一阶相关免疫布尔函数的计数 [1]

田海建 杨义先 王建宇 *

(北京邮电大学信息工程系 北京 100088)
*(加拿大 carleton 大学)

摘 要 本文研究线性结构布尔函数的相关免疫性，得到了一大类满足一阶相关免疫的线性结构函数，并大大改进了一阶相关免疫函数的计数结果，得到了目前为止的最好下界.

关键词 布尔函数，序列密码，相关免疫函数

中图号 TN911.2

1 引 言

布尔函数是序列密码中生成密钥序列的重要手段，作为前馈网络函数布尔函数的性质直接关系到密码系统的安全性，人们对用于序列密码中的布尔函数提出了 5 个必要条件. 前人对满足这五个条件的布尔函数的计数已作了较多的讨论 [1-4]，其中对满足 C4 条件的精确计数是遗留很久的问题，1990 年 C. Mitchell[1] 得到的下界为 $2^{2^{n-1}}$,1992 年文献 [2] 进行了改进，得到了新的下界为：$[2^{2^{n-1}}+2^n-2n+(2^{2^{n-r-1}}-2^{n-r})(2^{r-1}-1)],(r\geq 3)$，后来文献 [3,4] 又得到了更好的下界为：$[2^{2^{n-1}}+2^n-2n+(2^{2^{n-2}}-2^{n-2}-2^{2^{n-3}})n(n-1)]$，本文将对此界再作改进，得到的最新下界：$[2^{2^{n-1}}+2^{n-3}(3^n-3.2^n+5)\cdot 2^{2^{n-2}}+(3^n-3.2^n+5)\cdot(2^{2^{n-3}+n-3}-2^{2n-3}+2^{n-1})2^{2^{n-3}}+2C_n^3\cdot(2^{2^{n-3}}-2^{2^{n-4}}-2^{n-3})+2^n-2n]$, 显然我们的新下界远远大于已知下界，是目前为止最好的结果.

2 线性结构函数和相关免疫函数

定义 1 $f(x)$ 是 n 元布尔函数, 记 $E_b=\{s\in \mathrm{GF}(2)^n$: 对任意 $x\in \mathrm{GF}(2)^n, f(x+s)+f(x)=b\}$, $b=0$ 或 1 称 $E=E_0\cup E_1$ 为布尔函数 $f(x)$ 的线性核.

易证 E_0、E 均是 $\mathrm{GF}(2)^n$ 的子空间，E_0 亦是 E 的子空间. E_1 可以为空集 ϕ，若 $E_1\neq\phi$，则 E_1 是 E_0 作为 E 的子空间的陪集.

定义 2 设 $f(x)$ 是线性核为 $E=E_0\cup E_1$ 的 n 元布尔函数. 若 E 的维数大于零，称 $f(x)$ 是线性结构函数，记为 $f\in \mathrm{LS}(n)$，否则称 $f(x)$ 为非线性结构函数，记为 $f\in \mathrm{NLS}(n)$; 若 E 的维数大于零，且 $E_1=\phi$ 则称 $f(x)$ 为第一型线性结构函数，记为 $f\in \mathrm{L}_1(n)$，否则称 $f(x)$ 为第二型线性结构函数，记为 $f\in \mathrm{L}_2(n)$.

定义 3 称 n 元布尔函数 $f(x_1,\cdots,x_n)$ 为 m 阶相关免疫的，如果 f 与任意 m 个分量 $x_{i_1},x_{i_2},\cdots,x_{i_m},(1\leq m\leq n)$ 统计独立. 若 m=1, 称 f 是一阶相关免疫函数.

[1] 1995-11-06 收到，1996-07-22 定稿
国家杰出青年基金和国家教委跨世纪优秀人才专项基金资助课题

引理 1 [2] n 元布尔函数 $f(x_1,\cdots,x_n)$ 为一阶相关免疫函数的充要条件是对任意 $i(1\le i\le n)$, $W_H(f(x_1,x_2,\cdots,x_n)+x_i)=2^{n-1}$，这里，$W_H(g)$ 表示布尔函数 g 的 Haming 重量.

定理 1 (1) 若 $f\in \mathrm{LS}(n)$, f 的线性核为 $E=E_0\cup E_1$，如果 $(1\ 1\ \cdots\ 1)\in E_0$ 则 f 为一阶相关免疫函数. (2) 若 $f\in \mathrm{L}_2(n)$, E 是 f 的线性核，$E=E_0\cup E_1$, 若存在 $C_1,C_2\in E_1$, 且 C_1,C_2 的不为 0 的分量下标集不交，则 f 必是一阶相关免疫函数.

证明 (1) 的证明可见文献 [1]，下证 (2). 首先若 $f\in \mathrm{L}_2(n)$ 则 $E_1\neq\phi$ 有 $W_H(f)=2^{n-1}$，现在设 f 满足 (2) 中条件，对任意 $i(1\le i\le n)$, 由于 C_1,C_2 的不为 0 的分量下标集不交，则 C_1,C_2 中必有一个其第 i 个分量为 0, 不妨设之为 C_1，令 $g_i(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)+x_i$, 则有

$$g_i(x)+g_i(x+c_1)=f(x)+f(x+c_1)=1,$$

于是 $g_i\in \mathrm{L}_2(n)$, 从而 $W_H(g_i)=2^{n-1}$, 因此 $W_H(f(x_1,x_2,\cdots,x_n)+x_i)=2^{n-1}$，又由于 i 是任取的，由引理 1 知 f 是一阶相关免疫函数. 证毕

此定理在线性结构函数类中找到了一大类相关免疫函数，下面通过对这些函数的个数进行估计，来给出一阶相关免疫函数个数的下界.

设 $\sigma: Z_2^n\to Z_2^n$ 是可逆线性变换，若 f 是 n 元布尔函数，我们定义 σ^* 如下:

$$\sigma^*(f(x_1,x_2,\cdots,x_n))=f(\sigma(x_1,x_2,\cdots,x_n)).$$

引理 2 设 $f\in \mathrm{L}_2(n)$, $E=E_0\cup E_1$ 是 f 的线性核，且 E 的维数为 k, 则必存在可逆线性变换 $\sigma: Z_2^n\to Z_2^n$ 使得 $\sigma^*(f(x_1,x_2,\cdots,x_n))=g(x_1,x_2,\cdots,x_{n-k})+x_{n-k+1}$, 其中 $g\in \mathrm{NLS}(n-k)$.

证明 因为 $f\in \mathrm{L}_2(n)$, 且线性核 $E=E_0\cup E_1$ 的维数为 k, 那么线性空间 E_0 的维数为 $k-1$, 选择空间 E' 以致于使得它们的直和 $E'\oplus E=Z_2^n$, 让 $\{\alpha_1,\alpha_2,\cdots,\alpha_{n-k}\}$ 是线性空间 E' 的基，$\{\alpha_{n-k+2},\cdots,\alpha_n\}$ 是线性空间 E_0 的基，那么对任意的 $\alpha_{n-k+1}\in E_1$, $\{\alpha_{n-k+1},\cdots,\alpha_n\}$ 是 E 的基. 定义: $\sigma: Z_2^n\to Z_2^n$ 如下: $\sigma(x_1,x_2,\cdots,x_n)=\sigma(\sum_{i=1}^n x_i\varepsilon_i)=\sum_{i=1}^n x_i\alpha_i$，显然 σ 是可逆的，$\sigma^* f(x_1,x_2,\cdots,x_n)=f(\sigma(x_1,x_2,\cdots,x_n))=f(\sum_{i=1}^n x_i\alpha_i)=f(\sum_{i=1}^{n-k+1}x_i\alpha_i)=x_{n-k+1}+f(\sum_{i=1}^{n-k}x_i\alpha_i)=g(x_1,\cdots,x_{n-k})+x_{n-k+1}$.

下面证明 $g=f(\sum_{i=1}^{n-k}x_i\alpha_i)\in \mathrm{NLS}(n-k)$. 假设 $g\in \mathrm{LS}(n-k)$, 那么存在 $s=(s_1,s_2,\cdots,s_{n-k})\in Z_2^{n-k}$, $s\neq 0$. 对任意的 $(x_1,x_2,\cdots,x_{n-k})\in Z_2^{n-k}$, $b=0,1$, $g(x_1+s_1,x_2+s_2,\cdots,x_{n-k}+s_{n-k})+g(x_1,x_2,\cdots,x_{n-k})=b$. 所以 $f(\sum_{i=1}^{n-k}(x_i+s_i)\alpha_i)+f(\sum_{i=1}^{n-k}x_i\alpha_i)=b$. 让 $\alpha=\sum_{i=1}^{n-k}s_i\alpha_i$，对任意 $x=\sum_{i=1}^n x_i\alpha_i\in Z_2^n$, 我们有 $f(x+\alpha)+f(x)=f(\sum_{i=1}^{n-k}(x_i+s_i)\alpha_i+\sum_{i=n-k+1}^n x_i\alpha_i)+f(\sum_{i=1}^n x_i\alpha_i)=b$. 所以 $\alpha\in E$. 但是 $\alpha=\sum_{i=1}^{n-k}s_i\alpha_i\in E', \alpha\neq 0$. 矛盾！所以 $g\in \mathrm{NLS}(n-k)$.

证毕

引理 3 f 是 n 元布尔函数，$\sigma: Z_2^n\to Z_2^n$ 是可逆线性变换，如果 f 的线性核为 E，则 $\sigma^*(f)$ 的线性核为 $\sigma^{-1}(E)$.

证明 由 $\sigma^*(f)$ 和线性核的定义易证. 证毕

引理 4 用 $|\mathrm{LS}(n)|$ 表示 n 元线性结构布尔函数的个数，则

$$|\mathrm{LS}(n)|=\sum_{k=1}^{n}2^{2^{n-k}+[k(k+1)/2]}\cdot\frac{\Pi_{i=0}^{k-1}(2^n-2^i)}{\Pi_{i=0}^{k-1}(2^k-2^i)}<(2^n-1)\cdot 2^{2^{n-1}+1}$$

证明　见文献 [5] 第 225 页。　　证毕

3　一阶相关免疫函数的计数

设 f 是 n 元布尔函数，$E=E_0\cup E_1$ 是 f 的线性核，令

$I_n=\{f:Z_2^n\to Z_2, f$是一阶相关免疫函数$\}$，$S_1=\{f:Z_2^n\to Z_2,(1\ 1\ \cdots\ 1)\in E_0\}$，$P_n=\{f\in L_2(n)$, 线性核空间 E 的维数为 2，且存在两个不同的线性核 $c_1,c_2\in E_1$, c_1,c_2 的为 1 的分量下标集不交，$(1\ 1\ \cdots\ 1)\notin E\}$, 易知 $E=\{0,c_1,c_2,c_1+c_2\}$, 且 $c_1+c_2\neq(1\ 1\cdots\ 1)$, $E_1=\{c_1,c_2\}$, $P_n\subseteq I_n$. 为了得到 $|I_n|$ 的一个界，我们首先来估计 $|P_n|$.

由引理 2, 对任意的 $f\in P_n$, 均存在可逆线性变换 $\sigma:Z_2^n\to Z_2^n$ 使得 $\sigma^*(f(x_1,x_2,\cdots,x_n))=g(x_1,x_2,\cdots,x_{n-2})+x_{n-1}$，这里 $g\in$NLS$(n-2)$. 我们称 $g(x_1,x_2,\cdots,x_{n-2})+x_{n-1}$，　$g\in$NLS$(n-2)$ 为线性核空间维数为 2 的函数的标准形，显然标准形函数的个数为 $|\mathrm{NLS}(n-2)|$, 标准形函数的线性核 $E=\{0,\varepsilon_{n-1},\varepsilon_{n-1}+\varepsilon_n,\varepsilon_n\}$，　$E_1=\{\varepsilon_{n-1},\varepsilon_{n-1}+\varepsilon_n\}$ 。以下我们用 ε_i 表示第 i 个分量为 1 的 n 元单位向量，由同一标准型作不同的可逆线性变换将得到 $L_2(n)$ 中不同的函数 (由引理 3 易知)，为了使经可逆线性变换 σ 后得到的函数在 P_n 中，只需而且必须使得 $\sigma^{-1}(\varepsilon_{n-1})$, $\sigma^{-1}(\varepsilon_{n-1}+\varepsilon_n)$ 的分量为 1 的下标集不交，于是 $\sigma^{-1}(\varepsilon_{n-1})$, $\sigma^{-1}(\varepsilon_{n-1}+\varepsilon_n)$ 的选取种类为 $\sum_{j=1}^{n-2}(C_n^j\sum_{i=1}^{n-j-1}C_{n-j}^i)$, 因为 $\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-1},\varepsilon_{n-1}+\varepsilon_n$ 线性无关，故若使 σ 是可逆的线性变换，必须使 $\sigma^{-1}(\varepsilon_1),\sigma^{-1}(\varepsilon_2),\cdots,\sigma^{-1}(\varepsilon_{n-1}),\sigma^{-1}(\varepsilon_{n-1}+\varepsilon_n)$ 线性无关，故 $\sigma^{-1}(\varepsilon_1),\sigma^{-1}(\varepsilon_2),\cdots,\sigma^{-1}(\varepsilon_{n-1}),\sigma^{-1}(\varepsilon_{n-1}+\varepsilon_n)$ 的选取种类为 $(2^n-2^2)(2^n-2^3)\cdots(2^n-2^{n-1})$, 因此，满足将标准型函数变成 P_n 中函数的可逆线性变换的个数为 $\sum_{j=1}^{n-2}(C_n^j\sum_{i=1}^{n-j-1}C_{n-j}^i)(2^n-2^2)(2^n-2^3)\cdots(2^n-2^{n-1})$.

定义 4　设标准型 g_1,g_2，若存在可逆线性变换 σ 使得 $g_2=\sigma^*g_1$, 则称 g_1 与 g_2 等价，否则为不等价。

记标准形 g_1 经不同的可逆线性变换得到的 $\mathrm{L}_2(n)$ 中的函数集为 S_1，标准形 g_2 经不同的可逆线性变换得到的 $\mathrm{L}_2(n)$ 中的函数集为 S_2.

引理 5　若标准型 g_1 与标准型 g_2 等价，那么将有 $S_1=S_2$.

证明　设任意的 $f\in S_1$，那么存在可逆线性变换 σ_1 使 $\sigma_1^*g_1=f$. 又 $g_2=\sigma^*g_1$，　$g_1=(\sigma^*)^{-1}g_2$, 所以 $\sigma_1^*\cdot(\sigma^*)^{-1}g_2=f$, 所以 $f\in S_2$, $S_1\subseteq S_2$. 同理 $S_1\supseteq S_2$, 所以 $S_1=S_2$。　证毕

引理 6　若 $S_1\cap S_2\neq\phi$, 那么将有 g_1 与 g_2 等价。

证明　设 $f\in S_1\cap S_2$, 则有 $f\in S_1$, $f\in S_2$ 由 $f\in S_1$ 得存在可逆线性变换 σ_1 使 $\sigma_1^*g_1=f$, 由 $f\in S_2$ 得存在可逆线性变换 σ_2 使 $\sigma_2^*g_2=f$, 所以 $\sigma_1^*g_1=\sigma_2^*g_2$, 故 $g_2=((\sigma_2^*)^{-1}\sigma_1^*)g_1$。取 $\sigma^*=(\sigma_2^*)^{-1}\sigma_1^*$, 则 $g_2=\sigma^*g_1$。　证毕

由此引理知，若 g_1 与 g_2 不等价，$S_1\cap S_2=\phi$

定理 2　$|P_n|\geq 2^{n-2}(3^n-3\cdot 2^n+5)\cdot|\mathrm{NLS}(n-2)|$.

证明　首先我们求出把一标准形仍化成另一标准形的可逆线性变换的个数，即满足 $\sigma^*(g(x_1,\cdots,x_{n-2})+x_{n-1})=g'(x_1,\cdots,x_{n-2})+x_{n-1}$ 的 σ 的个数，其中 $g'\in$NLS$(n-2)$. 要想使上式成立，必须有 $\sigma(\sum_{i=1}^{n-2}x_i\varepsilon_i)\subset\mathrm{L}(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2})$. 这里 $\mathrm{L}(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2})$ 表示由 $\varepsilon_1,\cdots,\varepsilon_{n-2}$ 形成的线性空间 $\sigma(\varepsilon_{n-1})\in\mathrm{L}(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-2},\varepsilon_{n-1})-\mathrm{L}(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_{n-1})$, 易知满足这一要求 σ 的个数

为 $(2^{n-2}-2^0)(2^{n-2}-2^1)\cdots(2^{n-2}-2^{n-3})(2^{n-1}-2^{n-2})$ 此数也是互相等价的标准形的个数. 然后我们再将 $|\mathrm{NLS}(n-2)|$ 个标准形按等价进行分类, 这样 $|\mathrm{NLS}(n-2)|$ 个标准形可分成

$$\frac{|\mathrm{NLS}(n-2)|}{(2^{n-2}-2^0)(2^{n-2}-2^1)\cdots(2^{n-2}-2^{n-3})(2^{n-2}-2^{n-2})}$$

个互相等价的集合. 再由引理 6 知由 $\sum_{j=1}^{n-2}(C_n^j\sum_{i=1}^{n-j-1}C_{n-j}^i)(2^n-2^2)(2^n-2^3)\cdots(2^n-2^{n-1})$ 个可逆线性变换至少得到

$$\frac{|\mathrm{NLS}(n-2)|\,(2^n-2^2)(2^n-2^3)\cdots(2^n-2^{n-1})}{(2^{n-2}-2^0)(2^{n-2}-2^1)\cdots(2^{n-2}-2^{n-3})(2^{n-1}-2^{n-2})}\sum_{j=1}^{n-2}(C_n^j\sum_{i=1}^{n-j-1}C_{n-j}^i)$$

个不同的 P_n 中的元素, 故

$$\begin{aligned}|P_n| &\geq \frac{|\mathrm{NLS}(n-2)|(2^n-2^2)(2^n-2^3)\cdots(2^n-2^{n-1})}{(2^{n-2}-2^0)(2^{n-2}-2^1)\cdots(2^{n-2}-2^{n-3})(2^{n-1}-2^{n-2})}\sum_{j=1}^{n-2}(C_n^j\sum_{i=1}^{n-j-1}C_{n-j}^i)\\ &= 2^{n-2}(3^n-3\cdot 2^n+5)\cdot|\mathrm{NLS}(n-2)|.\end{aligned}$$

这是因为 $\sum_{j=1}^{n-2}(C_n^j\sum_{i=1}^{n-j-1}C_{n-j}^i)=3^n-3\cdot 2^n+5$. 证毕

引理 7 [3] 设 $g(x)$ 为 $n-1$ 布尔函数, 那么 n 元布尔函数 $f(x_1,\cdots,x_n)=x_{i_0}+g(x_1,\cdots,x_{i_0-1},x_{i_0+1},\cdots,x_n)$ 是平衡的, 即 $W(f(x))=2^{n-1}$.

引理 8 n 元布尔函数 $f(x)=a+\sum_{i=1}^n x_i+g(x_{i_1},\cdots,x_{i_{n-3}})$ 为一阶相关免疫函数.

证明 这是因为对任意的 i 函数 $x_i+f(x)$ 均可表示为引理 7 的形式, 所以 $W(x_i+f(x))=2^{n-1}$, 故 $f(x)$ 为一阶相关免疫函数.

引理 9 如果 $f(x)$ 是 n 元布尔函数, 则 E 的维数大于等于 $n-1$ 的充要条件为 $f(x)$ 为仿射函数.

证明 充分性显然, 下证必要性. 因 E 的维数大于等于 $n-1$, 必存在无关向量 $c_1,c_2,\cdots,c_{n-1}\in E$, 将 $c_1,c_2,\cdots,c_{n-1}\in E$ 扩充成 $\mathrm{GF}(2)^n$ 上一组基 $c_1,c_2,\cdots,c_n$, 且使 $c_1,c_2,\cdots,c_{n-1}$ 对应 $b_1,b_2,\cdots,b_{n-1}$ 使得 $f(x)+f(x+c_i)=b_i$ 恒成立 $(1\leq i\leq n-1)$, 对任意 $x,y\in\mathrm{GF}(2)^n$ 必有 $e_1,e_2,\cdots,e_n\cdot a_1,a_2,\cdots,a_n$ 使 $y=a_1c_1+a_2c_2+\cdots+a_nc_n$, $x=e_1c_1+e_2c_2+\cdots+c_ne_n$, 易得到

$$\begin{aligned}f(x+y) &= f(\sum_{i=1}^n(e_i+a_i)c_i)\\ &= f((e_n+a_n)c_n)+\sum_{i=1}^{n-1}(e_i+a_i)b_i = f(0)+f(e_nc_n)+f(a_nc_n)+\sum_{i=1}^{n-1}(e_i+a_i)b_i\\ &= f(0)+f(x)+f(y),\end{aligned}$$

故 $f(x)$ 为仿射函数, 引理成立. 证毕

为了估计一阶相关免疫函数的个数, 我们再引入两个函数集.

$$S_2=\{f: f(x_1,\cdots,x_n)=a+\sum_{i=1}^{n}b_ix_i;\sum_{i=1}^{n}b_i\text{为大于 1 的奇数}\},$$

$$S_3=\{f: f(x_1,\cdots,x_n)=a+\sum_{i=1}^{n}x_i+g(x_{i_1},x_{i_2},\cdots,x_{i_{n-3}}),\quad \text{其中}i_1,i_2,\cdots,i_{n-3}$$

取自集合$\{1,2,\cdots,n\}$且互不相同. $\}$

定理 3　$|I_n|\geq|P_n|+|S_1|+|S_2|+|S_3-(S_1\cup S_2)|,\ (n>3)$.

证明　因为由前述引理易知 $P_n,S_1,S_2,S_3,$ 均为一阶相关免疫函数，所以我们有 $I_n\supseteq P_n\cup S_1\cup S_2\cup S_3$.

$$\begin{aligned}|I_n|\geq{}&|P_n|+|S_1|+|S_2|+|S_3|-|P_n\cap S_1|-|P_n\cap S_2|-|P_n\cap S_3|-|S_1\cap S_2|\\&-|S_1\cap S_3|-|S_2\cap S_3|+|S_1\cap P_n\cap S_2|+|S_1\cap P_n\cap S_3|\\&+|S_1\cap S_2\cap S_3|+|P_n\cap S_2\cap S_3|-|P_n\cap S_1\cap S_2\cap S_3|.\end{aligned}$$

由文献 [2] 知 $S_1\cap S_2=\phi$, 所以 $|S_1\cap S_2|=|P_n\cap S_1\cap S_2|=|S_1\cap S_2\cap S_3|=|P_n\cap S_1\cap S_2\cap S_3|=0$. 又易知 $S_1\cap P_n=\phi$，所以 $|S_1\cap P_n|=|S_1\cap P_n\cap S_3|=0$.

下面讨论 $P_n\cap S_2$ 和 $P_n\cap S_3$. 因为 S_2 中的函数 $f(x)$ 均为仿射函数，由引理 9 知 S_2 中的 $f(x)$ 的线性核空间的维数大于等于 $n-1$ 大于 2, 而 P_n 中的线性核空间的维数等于 2, 所以 $S_2\cap P_n=\phi$, $|S_2\cap P_n|=|P_n\cap S_2\cap S_3|=|S_1\cap P_n\cap S_2|=0$；又 S_3 中的线性核空间的维数大于等于 3, 所以 $S_3\cap P_n=\phi$, $|S_3\cap P_n|=0$, 得

$$\begin{aligned}|I_n|&\geq|P_n|+|S_1|+|S_2|+|S_3|-|S_1\cap S_3|-|S_2\cap S_3|\\&=|P_n|+|S_1|+|S_2|+|S_3-(S_1\cup S_2)|,\quad (n>3).\end{aligned}$$

证毕

定理 4　一阶相关免疫函数的 n 元布尔函数的个数 $|I_n|$ 满足：$|I_n|\geq 2^{2^{n-1}}+2^{n-3}(3^n-3\cdot 2^n+5)\cdot 2^{2^{n-2}}+(3^n-3\cdot 2^n+5)\cdot(2^{2^{n-3}+n-3}-2^{2n-3}+2^{n-1})2^{2^{n-3}}+2C_n^3\cdot(2^{2^{n-3}}-2^{2^{n-4}}-2^{n-3})+2^n-2n$.

证明　由前面的推导有 $|P_n|\geq 2^{n-2}(3^n-3\cdot 2^n+5)\cdot|\mathrm{NLS}(n-2)|$; 又 $|\mathrm{NLS}(n-2)|=2^{2^{n-2}}-|\mathrm{LS}(n-2)|$, 再由引理 4 可知 $|\mathrm{LS}(n-2)|<(2^{n-2}-1)\cdot 2^{2^{n-3}+1}$, 于是 $|\mathrm{NLS}(n-2)|>2^{2^{n-2}}-(2^{n-2}-1)\cdot 2^{2^{n-3}+1}$, 则有

$$\begin{aligned}|P_n|&\geq 2^{n-2}(3^n-3\cdot 2^n+5)\cdot|\mathrm{NLS}(n-2)|\\&>2^{n-2}(3^n-3\cdot 2^n+5)\cdot(2^{2^{n-2}}-(2^{n-2}-1)\cdot 2^{2^{n-3}+1})\\&=(3^n-3\cdot 2^n+5)\cdot 2^{2^{n-2}+n-2}-(3^n-3\cdot 2^n+5)\cdot(2^{n-2}-1)\cdot 2^{2^{n-3}+n-1}).\end{aligned}$$

由文献 [1] 知 $|S_1|=2^{2^{n-1}}$, 由文献 [6] 知 $|S_2|=2(2^{n-1}-n)$, 由文献 [3] 知 $|S_3-(S_1\cup S_2)|\leq 2C_n^3(2^{2^{n-3}}-2^{n-3}-2^{2^{n-4}})$. 把以上结果代入定理 3，定理 4 获证.

4 结束语

由定理 4 中一阶相关免疫布尔函数个数 $|I_n|$ 的下界表达式可清楚地看到，我们的新下界大于 $2^{2^{n-1}}+2^{n-3}\cdot 2^{2^{n-2}}$ 而文献 [3,4] 中的下界则大约为 $2^{2^{n-1}}+2^{2^{n-2}}$，故新下界的改进是不小的。很明显，我们涉及到的一阶相关免疫函数类均属线性结构函数类。有资料表明，非线性结构的一阶相关免疫函数比线性结构的一阶相关免疫函数还要多，如何将它们归类找出，这还有待于进一步的研究和探讨。

致谢 感谢博士生邢育森同学的有益讨论，感谢信号理论与密码学实验室同学的大力支持。

参 考 文 献

[1] Mitchell C. Enumerating Boolean function of cryptographic significance. J. Cryptology,1990,2(3): 155–170.

[2] 杨义先，胡正名. 用于序列密码的布尔函数计数问题. 通信学报， 1992,13(4): 18–24.

[3] 郭宝安. 非线性序列的分析与综合：[博士论文]. 北京：北京邮电大学， 1993.6.

[4] Yang Yi Xian, Guo Bao An. Further enumeration of Boolean functions of cryptographic significance. J.Cryptology, 1996, 8(1):115–122.

[5] O'Connor L, Klapper A. Algebraic nonlinearity and it's applications to cryptography. J. Cryptology, 1994, 7(4): 213–227.

[6] 杨义先，林须端，胡正名. 编码密码学. 北京：人民邮电出版社， 1992 年，第 15 章， 538–549.

ENUMERATING CORRELATION-IMMUNE FUNCTIONS OF ORDER ONE

Tian Haijian Yang Yixian Wang Jianyu*

(*Department of Information Engineering, Beijing Univ. Posts and Telecom., Beijing* 100088)

*(*Carleton University, Canada*)

Abstract A large class of linear structure functions satisfying correlation immunity of order one is found by the studying of linear structural Boolean functions. The known enumeration bounds of correlation-immune Boolean functions are greatly improved. The best updated lower bounds are found.

Key words Boolean function, Stream ciphers, Correlation-immune function

田海建： 男， 1968 年生，硕士，专业为信号与信息处理，现于山东邮电管理局设计规划院工作.
杨义先： 男， 1961 年生，教授，博士生导师，从事专业：信号与信息处理、密码学和应用数学.
王建宇： 男， 1965 年生，博士，专业为组合数学.