一阶相关免疫函数的新构造方法与计数

吕继强, 韩锦荣, 韦宝典, 王新梅
(西安电子科技大学综合业务网国家重点实验室, 陕西西安 710071)

摘 要: 本文研究了一阶相关免疫函数构造、计数问题, 提出了一种新的一阶相关免疫函数的构造方法, 由此得到了大量的一阶相关免疫函数; 并通过这种构造方法给出了一个目前最好的一阶相关免疫函数个数下界, 此下界比现有的结果至少改进了$(2^{2^{n-1}+2n})/(2^{n+8}-2^{10})$.

关键词: 布尔函数; 相关免疫函数; 列平衡矩阵
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2003) 08-1269-03

New Construction Method and Numeration of 1st-Order Correlation-Immune Functions

LV Ji-qiang, HAN Jin-rong, WEI Bao-dian, WANG Xin-mei
(National Key Lab of Integrated Service Networks, Xidian Univ., Xi'an, Shaanxi 710071, China)

Abstract: Construction and numeration of 1st-order correlation-immune functions were studied. A new method to construct the 1st-order correlation-immune functions was proposed, through which a number of 1st-order correlation-immune functions were got and the best lower bound of 1st-order correlation-immune functions so far was gained. The lower bound is at least $(2^{2^{n-1}+2n})/(2^{n+8}-2^{10})$ more than the present.

Key words: boolean function; correlation-immune functions; column-balanced matrix

1 引言

相关免疫布尔函数最早是由 Siegenthaler 在研究流密码系统的安全性时提出的, 在抗相关攻击时发挥着巨大的作用; 而在密码学中具有实际应用价值的是高阶相关免疫函数, 高阶相关免疫函数个数必须足够大, 否则由此设计出的密码系统容易遭受攻击, 又由于高阶相关免疫函数必定是一阶相关免疫函数, 所以研究一阶相关免疫函数计数具有重要意义.

Mitchell 于 1990 年首先讨论了一阶相关免疫函数的计数问题, 给出了一阶相关免疫函数个数的下界[2] $2^{2^{n-1}}$, 文献[3]改进了此下限为 $2^{2^{n-1}}+\frac{2^{2^{n-1}}}{2^{n-2}+1}-2^{2^{n-2}}$. 本文设计了一种一阶相关免疫函数的新构造方法, 改进了 $2^{2^{n-1}}$ 项的系数, 得到了目前最好的下界, 第二节证明了构造方法的正确性; 第三节计算了个数下界; 第四节给出了结论.

2 构造

约定: $V_m^i=\{A=(A_1,\cdots,A_m)^T \mid A\in F_2^m, X(A)=i, (0\le i\le m)\}$, T 表示转置, X(A) 为 A 的汉明重量. $\overline{1}=V_{2k}^{2k}$, $\overline{0}=V_{2k}^{0}$.

定义 1[1] 设 $z=f(x_1,\cdots,x_n)$ 为 n 元布尔函数, 称 f(x) 是 m 阶相关免疫的当且仅当 z 与 $x_1,\cdots,x_n$ 中的任 m 个变量 $x_{i_1},\cdots,x_{i_m}$ 统计独立, 或者当且仅当互信息量 $I(z,x_{i_1},\cdots,x_{i_m})=0$ 对任一组 $1\le i_1<\cdots<i_m\le n$ 成立.

显然, 高阶相关免疫函数必定是一阶相关免疫函数.

定义 2[3] 设 $f(x_1,\cdots,x_n)$ 是 F_2 上的 n 元布尔函数, $S=\{(a_1,\cdots,a_n)\in F_2^n \mid f(a_1,\cdots,a_n)=1\}$, 称以 S 中所有向量为行向量按字典排序组成的矩阵 c_f 为 f 的特征矩阵.

定义 3 称矩阵 C 是列平衡矩阵, 如果 C 中行互不相同, 每列 0、1 各半.

定义 4 设 $A_{m\times n}=\begin{bmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{bmatrix}$ 是 m 行 n 列的矩阵, 则定义其共轭矩阵为 $\begin{bmatrix} a_{1,1}\oplus 1 & \cdots & a_{1,n}\oplus 1 \\ \vdots & & \vdots \\ a_{m,1}\oplus 1 & \cdots & a_{m,n}\oplus 1 \end{bmatrix}$, 简记为 $A_{m\times n}$, $\oplus$ 表示 F_2 上模 2 加.

引理 1[4] 设 $f(x_1,\cdots,x_n)$ 是 F_2 上的 n 元布尔函数, 则 f(x) 是 m 阶相关免疫的当且仅当其特征矩阵 c_f 是列平衡矩阵.

收稿日期: 2001-12-04; 修回日期: 2002-02-27
基金项目: 国家 973 项目基金(No.G1999035803)

显然, 若 f(x) 是一阶相关免疫的, 则 c_f 的行数必为偶数 2k, (0[k[2^{n-1}) ; 并且, 一阶相关免疫函数 f(x) 与定序列平衡特征矩阵 c_f 是一一对应的, 如果两个矩 A、B 按字典排序后的矩阵不同, 则记为 A WB.

引理 2[5] 若 $c_{2k@n}$ 是由 k 个互异共轭向量对构成的矩阵, 则 $c_{2k@n}$ 是列平衡矩阵.

因此, 由引理 1 可知: 以 $c_{2k@n}$ 为特征矩的 f(x) 是一阶相关免疫的.

定理 1 若 a_{m,i_m} I $V_{2k}^{i_m}$, $b_{m,2k-i_m}$ I $V_{2k}^{2k-i_m}$, (1[m[j, 0[j[n- 2), A、B 是 2k @(n- 1- j) 列平衡矩阵, 则 C= $\begin{bmatrix} 1 & a_{1,i_1}, & a_{j,i_j} & A \\ 0 & b_{1,2k-i_1}, & b_{j,2k-i_j} & B \end{bmatrix}$ 是 4k @n 列平衡矩阵, 且以 C 为特征矩阵的 f(x) 是一阶相关免疫的. 当 j= 0 时, m= 5 表示矩阵 $\begin{bmatrix} 1 & A \\ 0 & B \end{bmatrix}_{4k@n}$.

证明 因为 A、B 是 2k@(n- 1- j) 列平衡矩阵, 且由 C 中第一列, 所以 C 是行互异的; 而由于 X(a_{m,i_m}) = i_mX($b_{m,2k-i_m}$) = 2k- i_m, 则 4k 维列向量[a_{m,i_m}, $b_{m,2k-i_m}$] ^{T} 中 0、1 各半; 对 C 中其它列由条件可知 0、1 各半, 所以 C 是 4k @n 列平衡矩阵; 由引理 1 知结论成立. #

推论 1 若 a I V_{2k}^{i}, b I V_{2k}^{2k-i}, A、B 是 2k @(n- 2) 列平衡矩阵, 则 C= $\begin{bmatrix} 1 & a & A \\ 0 & b & B \end{bmatrix}$ 是 4k @n 列平衡矩阵, 且以 C 为特征矩阵的 f(x) 是一阶相关免疫的.

定理 2 设 A、B 是 2k @(n- 1- j) 定序列平衡矩阵(0[j[n- 2), 如果 $\begin{bmatrix} a_{1,i_1}, & a_{j,i_j} \\ b_{1,2k-i_1}, & b_{j,2k-i_j} \end{bmatrix}_{4k@j}$ X $\begin{bmatrix} a^*_{1,i_1}, & a^*_{j,i_j} \\ b^*_{1,2k-i_1}, & b^*_{j,2k-i_j} \end{bmatrix}_{4k@j}$, 则 $\begin{bmatrix} 1 & a_{1,i_1}, & a_{j,i_j} & A \\ 0 & b_{1,2k-i_1}, & b_{j,2k-i_j} & B \end{bmatrix}_{4k@n}$ W $\begin{bmatrix} 1 & a^*_{1,i_1}, & a^*_{j,i_j} & A \\ 0 & b^*_{1,2k-i_1}, & b^*_{j,2k-i_j} & B \end{bmatrix}_{4k@n}$ 其中 a_{m,i_m}、$b_{m,2k-i_m}$、a^*_{m,i_m}、$b^*_{m,2k-i_m}$ I $\bigcup_{i=0}^{2k} V_{2k}^{i}$ 且 X(a_{m,i_m}) + X(b_{m,i_m}) = X(a^*_{m,i_m}) + X(b^*_{m,i_m}) = 2k, 1[m[j; 当 j= 0 时, m= 5 表示矩阵 $\begin{bmatrix} 1 & A \\ 0 & B \end{bmatrix}_{4k@n}$.

证明 由于若 A、B 是 2k@(n- 1- j) 定序列平衡矩阵, A、B 行互不相同, 从而 4k @n 矩阵 $\begin{bmatrix} 1 & A \\ 0 & B \end{bmatrix}$ 的行互不相同; 又由于 $\begin{bmatrix} a_{1,i_1}, & a_{j,i_j} \\ b_{1,2k-i_1}, & b_{j,2k-i_j} \end{bmatrix}_{4k@j}$ X $\begin{bmatrix} a^*_{1,i_1}, & a^*_{j,i_j} \\ b^*_{1,2k-i_1}, & b^*_{j,2k-i_j} \end{bmatrix}_{4k@j}$, 故 $\begin{bmatrix} 1 & a_{1,i_1}, & a_{j,i_j} & A \\ 0 & b_{1,2k-i_1}, & b_{j,2k-i_j} & B \end{bmatrix}$ W $\begin{bmatrix} 1 & a^*_{1,i_1}, & a^*_{j,i_j} & A \\ 0 & b^*_{1,2k-i_1}, & b^*_{j,2k-i_j} & B \end{bmatrix}$. #

推论 2 若 a、a^* I V_{2k}^{i}, b、b^* I V_{2k}^{2k-i}, 且[a, b] ^{T} X[a^*, b^*] ^{T}(0[i[2k), A、B 是 2k @(n- 2) 列平衡矩阵, 则 $\begin{bmatrix} 1 & a & A \\ 0 & b & B \end{bmatrix}$ W $\begin{bmatrix} 1 & a^* & A \\ 0 & b^* & B \end{bmatrix}$.

3 计数

由引理 1 知一阶相关免疫布尔函数的计数问题可转化为列平衡特征矩阵的计数问题. 以下定理 3 和定理 4 是基于这一点得出的.

定理 3 一阶相关免疫函数个数 N(n) 满足:

$$N(n) \setminus 2^{2^{n-1}} + \sum_{k=1}^{2^{n-3}} (C_{4k}^{2k} \# C_{2^{n-3}}^{k} - 2^{2k}) \# C_{2^{n-3}}^{k}$$

证明 记 $S_{2l,n}$ 为 F_2^n 上全体由 1 个共轭向量对构成 2l @ n 定序列矩阵之集,

$$M_{4k,n} = \left\{ \begin{bmatrix} 1 & a & A \\ 0 & b & B \end{bmatrix} a \text{ I } \bigcup_{i=0}^{2k} V_{2k}^{i}, b \text{ I } \bigcup_{i=0}^{2k} V_{2k}^{i}, \text{ 且 } X(a) + X(b) = 2k, A、B \text{ I } S_{2k,n-2} \right\}$$

; 显然, 为使 A、B、$S_{2l,n}$、$M_{4k,n}$ 非空, 应有 0[l[2^{n-1}, 1[k[2^{n-3}.

令 $M_n = \bigcup_{k=1}^{2^{n-3}} M_{4k,n}$, $S_n = \bigcup_{k=0}^{2^{n-1}} S_{2l,n}$, 则| S_n| = $\sum_{i=0}^{2^{n-1}} C_{2^{n-1}}^{i} = 2^{2^{n-1}}$. 由推论 2 知| $M_{4k,n}$| = $\sum_{i=0}^{2k} (C_{2k}^{i})^2 \# (C_{2^{n-3}}^{k})^2 = C_{4k}^{2k} \# (C_{2^{n-3}}^{k})^2$, | M_n| = $\sum_{k=1}^{2^{n-3}} C_{4k}^{2k} \# (C_{2^{n-3}}^{k})^2$.

易知, 若 AI $S_{2l,n}$, 则 AI $S_{2l,n}$, 从而 $M_{4k,n}$ H $S_{4k,n}$ = $\left\{ \begin{bmatrix} 1 & a & A \\ 0 & a & A \end{bmatrix} a \text{ I } \bigcup_{i=0}^{2^{n-3}} V_{2k}^{i}, A \text{ I } S_{2k,n-2} \right\}$, | $M_{4k,n}$ H $S_{4k,n}$| = $\sum_{i=0}^{2k} C_{2k}^{i} \# C_{2^{n-3}}^{k} = 2^{2k} \# C_{2^{n-3}}^{k}$. 所以| M_n H S_n| = $\sum_{k=1}^{2^{n-3}}$ | $M_{4k,n}$ H $S_{4k,n}$| = $\sum_{k=1}^{2^{n-3}} 2^{2k} \# C_{2^{n-3}}^{k}$.

由引理 2 和推论 1 可知 S_n、M_n 是列平衡矩阵, 从而所确定的布尔函数为一阶相关免疫的. 最后由 N(n) \ | S_n G M_n| = | S_n| + | M_n| - | S_n H M_n| 即知结论成立.

推论 1 保证构造的 $M_{4k,n}$ 是列平衡矩阵, 推论 2 保证 $M_{4k,n}$ 中任意满足 X(a) + X(b) = 2k 的 a, b 构造出的矩阵不相交, 这为计数提供了方便; 同理, 应用定理 1 和定理 2 可得到定理 4, 由于从 1 列到 j 列的特殊性, 证明如下.

定理 4 一阶相关免疫函数的个数 N(n) 满足:

$$N(n)\setminus 2^{2^{n-1}}+(n-1)\#2^{2n-3}+\sum_{i=1}^{n-2}\sum_{k=2^{n-2-i}+1}^{2^{n-1-i}}[(C_{2^{n-1-i}}^{k})^2\#(C_{4k}^{2k})^{i-1}-C_{2^{n-1-i}}^{k}\#2^{2k(i-1)}]$$

证明　记 $M_{4k,j,n}=$

$$\left\{\begin{bmatrix}1 & a_{1,i_1},\ a_{j,i_j} & A\\ 0 & b_{1,2k-i_1},\ b_{j,2k-i_j} & B\end{bmatrix}\ \middle|\ a_{m,i_m}\in\bigcup_{i=0}^{2k}V_{2k}^{i},\ b_{m,2k-i_m}\in\bigcup_{i=0}^{2k}V_{2k}^{i}\right.$$

$$\left.\text{且 } X(a_{m,i_m})+X(b_{m,2k-i_m})=2k,A、B\in S_{2k,n-1-j},1\leqslant m\leqslant j\right\}.$$

显然, 为使 A、B、$M_{4k,j,n}$ 存在, 须 $0\leqslant j\leqslant n-2$, $1\leqslant k\leqslant 2^{n-2-j}$.

令 $M_{4k,n}=\bigcup_{j=0}^{i}M_{4k,i,n}$, $M_n=\bigcup_{j=0}^{n-2}\bigcup_{k=1}^{2^{n-2-j}}M_{4k,j,n}$, $l=\lfloor\log_{2^k}8\rfloor$, $\lfloor a\rfloor$ 表示大于 a 的最大整数. 给定 k, 对满足 $1\leqslant k\leqslant 2^{n-2-j^*}$ 的 j^*, 有 $M_{4k,j^*-1,n}\subset M_{4k,j^*,n}$; 因此 $M_n=M_{4,n-2,n}\cup\left(\bigcup_{i=1}^{n-2}\bigcup_{k=2^{n-2-i}+1}^{2^{n-2-i}}M_{4,i-1,n}\right)$; 从而 $|M_n|=|M_{4,n-2,n}|+\sum_{i=1}^{n-2}\sum_{k=2^{n-1-i}+1}^{2^{n-1-i}}|M_{4k,i-1,n}|=(C_2^1)^2\#\left(\sum_{m=0}^{2}(C_2^m)^2\right)^{n-2}+\sum_{i=1}^{n-2}\sum_{k=2^{n-1-i}+1}^{2^{n-1-i}}\#\left[(C_{2^{n-1-i}}^{k})^2\#\left(\sum_{m=0}^{2k}(C_{2k}^{m})^2\right)^{i-1}\right]$.

又 $M_{4k,n}\cap S_{4k,n}=$

$$\left\{\begin{bmatrix}1 & a_1,\ a_j & A\\ 0 & a_1,\ a_j & A\end{bmatrix}\ \middle|\ a_i\in\bigcup_{i=0}^{2k}V_{2k}^{j},A\in S_{2k,n-1-j},1\leqslant i\leqslant j=\lfloor\log_{2^k}8\rfloor\right\},$$

因此 $|M_{4k,n}\cap S_{4k,n}|=\left(\sum_{m=0}^{2k}C_{2k}^{m}\right)^{j}\#C_{2^{n-2-j}}^{k}$. 由 $M_n\cap S_n=\left(M_{4,n-2,n}\cap S_{4,n}\right)\cup\left[\bigcup_{i=1}^{n-2}\bigcup_{k=2^{n-1-j}+1}^{2^{n-1-i}}\left(M_{4k,n}\cap S_{4k,n}\right)\right]$ 知, $|M_n\cap S_n|=|M_{4,n-2,n}\cap S_{4,n}|+\sum_{i=1}^{n-2}\sum_{k=2^{n-1-j}+1}^{2^{n-1-i}}|M_{4k,n}\cap S_{4k,n}|=C_2^1\#\left(\sum_{m=0}^{2}C_2^m\right)^{n-2}+\sum_{i=1}^{n-2}\sum_{k=2^{n-1-j}+1}^{2^{n-1-i}}\left[C_{2^{n-1-i}}^{k}\#\left(\sum_{m=0}^{2k}C_{2k}^{m}\right)^{i-1}\right]$.

由定理 1 可知 M_n 是列平衡矩阵, 从而所确定的布尔函数为一阶相关免疫的. 从而 $N(n)\setminus|S_n\cup M_n|=|S_n|+|M_n|-|S_n\cap M_n|=2^{2^{n-1}}+2^n\#3^{n-2}-2^{2n-3}+\sum_{i=1}^{n-2}\sum_{k=2^{n-1-i}+1}^{2^{n-1-i}}[(C_{2^{n-1-i}}^{k})^2\#(C_{4k}^{2k})^{i-1}-C_{2^{n-1-i}}^{k}\#2^{2k(i-1)}]\setminus 2^{2^{n-1}}+n\#2^{n-3}-2^{2n-3}+\sum_{i=1}^{n-2}\sum_{k=2^{n-1-j}+1}^{2^{n-1-j}}\left[(C_{2^{n-1-i}}^{k})^2\#(C_{4k}^{2k})^{i-1}-C_{2^{n-1-i}}^{k}\#2^{2k(i-1)}\right]$, 结论成立.

4　结论

本文给出了一种构造一阶相关免疫布尔函数的方法, 并得到了目前最好的计数下界. 对定理 3 分析可知 $2^{2^{n-1}}$ 项的系数至少被改进了 $2^{2n}/(2^{n+8}-2^{10})$, 定理 4 的结果更优于此值, 可见新的下界已远远大于已有的下界.

参考文献:

[1] T Siegenthaler, correlation2immunity of nonlinear combining functions for cryptographica applications [J]. IEEE Trans, 1984, IT230(5): 776-780.

[2] C Mitchell. Enumerating boolean functions of cryptographic signfi2cance, J of Cryptology [J]. 1990, 2(3): 155-170.

[3] 温巧燕、纽心忻、杨义先. 现代密码学中的布尔函数 [M]. 北京: 科学出版社, 2000. 46-94.

[4] 杨义先. 相关免疫布尔函数的计数 [J]. 电子科学学刊, 1993, 15(2): 140-146.

[5] 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.

作者简介:

吕继强　男, 1977 年 11 月生于山东省潍坊市, 2000 年毕业于烟台大学应用数学专业, 获学士学位, 现为西安电子科技大学通信与信息系统专业硕士研究生, 主要研究兴趣为网络与信息安全、密码学和应用数学. Email: lvjiqiang@sina.com

韩锦荣　女, 1978 年 4 月生于河南驻马店, 1999 年于郑州大学基础数学专业获学士学位, 现为西安电子科技大学硕士研究生, 主要研究方向为应用数学、信息安全和电子商务.