On the Construction and Enumeration of Correlation-Immune Boolean Functions of 2-order

Dajian LIAO
College of Science,Huaihai Institute of Technology, Jiangsu China
Email: 1006268675@qq.com

Abstract: Construction and enumeration of Correlation-Immune Boolean Functions of 2-order are discussed in this paper. Beside the constructed correlation-Immune Boolean Functions for the cases of weight 2r, a lot of new correlation-Immune Boolean Functions for the cases of weight 2r are constructed as supplement. Therefore a new formula of lower bounds on the number of Correlation-Immune Boolean Functions of 2-order is derived.

Keywords: correlation-immune, stream ciphers, orthogonal array, boolean functions

2 阶相关免疫函数的构造与计数

廖大见
淮海工学院理学院，连云港，中国，222005
Email: 1006268675@qq.com

摘　要：本文进一步讨论 2 阶相关免疫函数的构造与计数问题，补充构造出了大量重量为 2 的方幂的 2 阶相关免疫函数，给出了关于 2 阶相关免疫函数个数的新下界。

关键词：相关免疫；流密码；正交矩阵；布尔函数

1 引言

相关免疫函数是密码学中的一个重要概念，它是为抵抗 DC 攻击而提出的。自 1984 年 Seigenthaler T. 提出以来，国内外学者对此进行了大量研究，取得了丰富的结果［1-8］，同时还有许多有待研究的问题，计数问题便是其中之一。关于计数问题研究的意义文献［5］、［8］中都有论述。m 阶相关免疫函数和正交矩阵是等价的，而正交矩阵是研究认证码的重要工具［9］。给出一种好的正交矩阵的构造方法，就可拥有更多的正交阵列，设计出好的认证码。因此 m 阶相关免疫函数的构造与计数是一个值得研究的问题[10]。2 阶是研究高阶的基础，温巧燕等人 1998 年得到的一类正交矩阵的下界一直沿用至今未有突破。本文在原来研究成果的基础上进一步讨论 2 阶相关免疫函数个数的构造与计数问题，得到更优的结果。

2 定义及几个预备定理

相关免疫函数有多种等价定义，本文采取如下形式。

定义 1[7]

设 $f(x)=f(x_1,x_2\cdots x_n)$ 是布尔函数，$x_1,x_2\cdots x_n\in GF(2)$，称 $f(x_1,x_2\cdots x_n)$ 为 m 阶相关免疫的当且仅当对任意 m 个随机变量 $(x_{i_1},x_{i_2},x_{i_m})$ 和 $(a_1,a_2,a_m)\in GF(2)^m$，$\sum_{x\in x(m)} f(x)=\frac{w(f)}{2^m}$。$w(f)$ 是 $z=f(x_1,x_2\cdots x_n)$ 的汉明重量，

$$x(m)=\left\{x\mid x\in GF(2)^n,x_{i_j}=a_j,j=1,2\cdots m\right\}。$$

定义 2[5]

设 $f(x)=f(x_1,x_2\cdots x_n)$ 是布尔函数，$w=w(f)$ 是其汉明重量，

$$D=\left\{d\mid d=(d_1,d_2\cdots d_n)\in GF(2)^n;f(d)=1\right\}$$

将 D 中元素按字典式顺序从大到小排列为

$$C_i=(C_{i,1},C_{i,2}\cdots C_{i,n})$$

则称 0-1 矩阵

资助项目：国家自然科学基金（60473018）；教育部科学技术研究重点项目(208045)；东南大学移动通信国家重点实验室开放课题。

978-1-935068-10-5

$$C=\begin{vmatrix} C_{1,1} & \cdots & C_{1,n} \\ \vdots & \vdots & \vdots \\ C_{w,1} & \cdots & C_{w,n} \end{vmatrix}$$ 为 $f(x)$ 的特征阵 C_f。

为讨论方便，以下将不确定特征矩阵行向量的顺序，即视只有顺序不同的两个特征矩阵为相同特征矩阵。布尔函数与其特征阵是相互唯一确定的，亦称 $f(x)$ 是 C_f 的特征函数，又记为 f_C。

定义 3 [1]

设 A 是一个 w 行 n 列的矩阵，称 A 是一个 $(w,n,2,m)$ 正交阵，是指 A 的任 m 列构成的矩阵的行向量中，$GF(2)^m$ 中每个向量都出现且出现的次数相同。

引理 2.1 [1]

布尔函数 $f(x)$ 是 2 阶相关免疫的当且仅当 C_f 是 $(w(f),n,2,2)$ 正交矩阵，当且仅当 C_f 的任一列是平衡的且下述条件之一成立。

1) 任两列的和向量是平衡向量；2) 任两列逐项积后所得向量有 $\frac{w(f)}{4}$ 个 1。

3 构造与计数

定理 3.1 [1]

设 A，B 都是 $(w,n,2,2)$ 正交阵，则 $C=\begin{vmatrix} 1 & A \\ 0 & B \end{vmatrix}$ 是 $(2w,n+1,2,2)$ 正交矩阵。

定理 3.2 [1]

设 A，B 分别是 $(w_2,n,2,2)$、$(w_1,n,2,2)$ 正交阵，相互无相同行，则 $C=\left|A^T \quad B^T\right|^T$ 是 $(w_1+w_2,n,2,2)$ 正交矩阵。

定理 3.3 [1]

设 $k\le j-1$ 用 $GF(2)^j$ 表示由该空间全体向量为行的矩阵，将 $GF(2)^j$ 矩阵 2^{j-1} 个共轭对平均分成 2^k 快，每 2^{j-k-1} 个共轭对组成一个 $2^{j-k}\times j$ 阶分块矩阵 C_i，$i=1,2\cdots 2^k$，则矩阵

$$C=\begin{vmatrix} 1 & \cdots & 1 & C_1 \\ 1 & \cdots & 0 & C_2 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 1 & C_{2^k-1} \\ 0 & \cdots & 0 & C_{2^k} \end{vmatrix}$$

是 $(2^j,j+k,2,2)$ 正交阵，即 f_C 是二阶相关免疫的。其中 1 和 0 都是指 $2^{j-k}\times 1$ 阶矩阵。

以下为方便起见，记 C 为 $\phi(C_1,C_2,\cdots C_{2^k})$。

用 $N(4k,n)$ 记重量为 $4k$ 的 n 元 2 阶相关免疫函数的个数，亦即 $(4k,n,2,2)$ 定序正交矩阵的个数。用 $N(n)$ 记 n 元 2 阶相关免疫函数的个数，则 $N(n)=\sum_{k=1}^{2^{k-2}}N(4k,n)$，为确定 $N(n)$ 的下界，当 k 为 2 的方次时，根据以上定理来构造 $(4k,n,2,2)$ 正交阵，方法如下：

对任意 $k\le j-1$ 可将 $GF(2)^j$ 得 2^{k-1} 个共轭对分成平均分成行数相等的矩阵 $C_1,C_2\cdots C_{2^k}$，构造矩阵 $C=\phi(C_1,C_2,\cdots C_{2^k})$，相当于把 2^{j-1} 个共轭对分成平均分到 2^k 个空格中去。有 $\frac{(2^{j-1})!}{((2^{j-k-1})!)^{2^k}}$ 种不同的分法，根据定理 3.3，这意味着按这种方法可以得到 $\frac{(2^{j-1})!}{((2^{j-k-1})!)^{2^k}}$ 个不同的 $(2^j,j+k,2,2)$ 矩阵。这样就得到下面的结论

定理 3.4

任意 $1\le k\le j-1, j\ge 2$，有：

$$N(2^j,j+k)\ge\frac{(2^{j-1})!}{((2^{j-k-1})!)^{2^k}}。$$

为把该下界与原来文献 [1] 中 $N(2^{n-r},n)$ 下界比较，令 $j+k=n,k=r$，则上式变为：

$$N(2^{n-r},n)\ge\frac{(2^{n-r-1})!}{((2^{n-2r-1})!)^{2^r}}。$$

再引入下面的引理：

引理 3.1

设 m,n 为任意正整数，有:

$$\frac{(mn)!}{(m!)^n(n!)^m}\ge(\min\{m,n\}-1)!。$$

证明 不妨设 $n\le m$，则

$$\frac{(mn)!}{(m!)^n(n!)^m}=\prod_{j=0}^{m-1}\frac{(m-j)n\cdot((m-j)n-1)\cdots((m-j)n-n+1)}{(m-j)^n n!}$$

$$=\prod_{j=0}^{m-1}\frac{n\cdot(n-\frac{1}{m-j})\cdots(n-\frac{n-1}{m-j})}{n!}$$

$$=\prod_{j=0}^{m-1}\prod_{i=1}^{n-1}\frac{n-\frac{i}{m-j}}{n-i}\geq\prod_{j=0}^{m-1}(n-\frac{n-1}{m-j})\geq(n-1)!$$ 证毕。

由引理 3.1，新下界 $\frac{\left(2^{n-r-1}\right)!}{\left(\left(2^{n-2r-1}\right)!\right)^{2^r}}$ 至少是原下界 $\left(\left(2^r\right)!\right)^{2^{n-2r-1}}$ 的 $(2^b-1)!$ 倍，其中 $b=\min\{r,n-2r-1\}$。

在所有用定理 3.4 的方法构造的 $\frac{\left(2^{j-1}\right)!}{\left(\left(2^{j-k-1}\right)!\right)^{2^k}}$ 个形如 $C=\phi(C_1,C_2,\cdots C_{2^k})$ 的 $(2^j,j+k,2,2)$ 正交矩阵集合中定义一个等价关系：$C'\square C$ 当且仅当存在 l，使 $C'=\phi(C_{1+l},C_{2+l},\cdots C_{2^k+l})$，其中的下标取模 2^k。把上述矩阵集合按该等价关系的等价类划分，每个等价类中含有 2^k 个矩阵，且同一个等价类中的矩阵之间无相同行，用定理 3.2 可构造 $C_{2^k}^t$ 个 $(2^j,j+k,2,2)$ 正交矩阵，$0\leq t\leq 2^k$。下面说明当 t 为奇数时由不同等价类中的矩阵构造出来的 $(2^j,j+k,2,2)$ 正交矩阵互相不同。

设 $E_l=\phi(C_{1+l},C_{2+l},\cdots C_{2^k+l})$，$0\leq l\leq 2^k-1$ 是 $C=\phi(C_1,C_2,\cdots C_{2^k})$ 所在等价类中一个元素。$F_l=\phi(D_{1+l},D_{2+l},\cdots D_{2^k+l})$，$0\leq l\leq 2^k-1$ 是

$$D=\phi(D_1,D_2,\cdots D_{2^k})$$

所在等价类中一个元素。这里及以下涉及的下标运算都模 2^k。如果：

$$\left|E^T{}_{l_1}\quad E^T{}_{l_2}\quad\cdots\quad E^T{}_{l_t}\right|^T=\left|F^T{}_{n_1}\quad F^T{}_{n_2}\quad\cdots\quad F^T{}_{n_t}\right|^T,$$

则对任意 $0\leq m\leq 2^k-1$，有

$$\left|C^T{}_{l_1+m}\quad C^T{}_{l_2+m}\quad\cdots\quad C^T{}_{l_t+m}\right|^T$$

$$=\left|D^T{}_{n_1+m}\quad D^T{}_{n_2+m}\quad\cdots\quad D^T{}_{n_t+m}\right|^T$$

成立。不妨设 $0\leq l_1<l_2<\cdots<l_t<2^k$，按如下方式定义 m_i：$l_i+m_i\equiv l_1,1\leq i\leq t$。若 x 是 C_{l_1} 中某一行向量，则对任意 $1\leq i\leq t$，x 是下面矩阵中的一个行向量。

$$\left|D^T{}_{n_1+m_i}\quad D^T{}_{n_2+m_i}\quad\cdots\quad D^T{}_{n_t+m_i}\right|^T\qquad(1)$$

由于 $D_1,D_2\cdots D_{2^k}$ 相互无相同行，所以存在唯一矩阵 D_j，使得 x 是 D_j 中一行向量，且任意 $1\leq i\leq t$，存在 $1\leq s_i\leq t$ 使得 $D_j=D_{n_{s_i}+m_i}$，根据 m_i 的定义知 $\{s_i\,|\,1\leq i\leq t\}=\{1,2\cdots t\}$。下面证明满足同样条件的矩阵是唯一的。若不然，即另有一矩阵 $D_p\neq D_j$，对任意 $1\leq i\leq t$ 存在 p_i，使

$$D_p=D_{n_{p_i}+m_i}\quad\text{那么}\quad\{p_i\,|\,1\leq i\leq t\}=\{1,2\cdots t\},$$

则对任意 $1\leq i\leq t$，有下式成立：$n_{p_i}-n_{s_i}\equiv(n_{p_i}+m_i)-(n_{s_i}+m_i)\equiv p-j$。设 $p-j=s$，则 $\{n_{p_i}\,|\,1\leq i\leq t\}=\{n_{s_i}+s\,|\,1\leq i\leq t\}$

由 $\{s_i\,|\,1\leq i\leq t\}=\{p_i\,|\,1\leq i\leq t\}=\{1,2\cdots t\}$

得 $\{n_i\,|\,1\leq i\leq t\}\equiv\{n_i+s\,|\,1\leq i\leq t\}$，则任意 n，$n_1+ns\in\{n_i\,|\,1\leq i\leq t\}$。则可以在矩阵列 $D_{n_1},D_{n_2},\cdots D_{n_t}$ 中定义等价关系：$D_{n_i}\square D_{n_j}$ 当且仅当存在整数 n，使 $n_i-n_j=ns$。令 $d=\gcd\{2^k,s\}$，$n_0=\frac{2^k}{d}$，则 n_0 为偶数。那么按照该等价关系 $D_{n_1},D_{n_2},\cdots D_{n_t}$ 被划分成几个等价类，每个等价类中有 n_0 个元素，这与 t 为奇数矛盾。所以假设不成立。也就是说只有唯一的矩阵 $D_j=D_{n_{s_1}}$，满足对任意 $1\leq i\leq t$，$D_{n_{s_1}}$ 在矩阵 (1) 中。因此 C_{l_1} 中任意一行向量只能在 $D_{n_{s_1}}$ 中，所以 $C_{l_1}=D_{n_{s_1}}$。

根据 n_{s_i} 的定义知，$n_{s_1}=n_{s_i}+m_i,1\leq i\leq t$，则对任意 r，$D_{n_{s_1}+r}=D_{n_{s_i}+r+m_i},1\leq i\leq t$，同样

$$l_i+m_i\equiv l_1,1\leq i\leq t$$

则 $C_{l_{s_1}+r}=C_{l_{s_i}+r+m_i},1\leq i\leq t$，可由上面同样的方法可证只有一个矩阵 $D_{n_{s_1}+r}$ 满足：任意 $1\leq i\leq t$，$D_{n_{s_1}+r}$ 在矩阵

$$\left|D^T{}_{n_{s_1}+r+m_i}\quad D^T{}_{n_{s_2}+r+m_i}\quad\cdots\quad D^T{}_{n_{s_t}+r+m_i}\right|^T\text{ 中；}$$

有唯一矩阵 C_{l_1+r} 满足：任意 $1\leq i\leq t$，C_{l_1+r} 在矩阵

$$\left|C^T{}_{l_1+r+m_i}\quad C^T{}_{l_2+r+m_i}\quad\cdots\quad C^T{}_{l_t+r+m_i}\right|^T\text{ 中。}$$

又因为对任意 $0\leq m\leq 2^{k-1}$，下式：

$$\left|C^T{}_{l_1+m}\quad C^T{}_{l_2+m}\quad\cdots\quad C^T{}_{l_t+m}\right|^T$$

$$=\left|D^T{}_{n_1+m}\quad D^T{}_{n_2+m}\quad\cdots\quad D^T{}_{n_t+m}\right|^T$$

成立，可得 $C_{l_1+r}=D_{s_1+r}$ 对于任意 $0\leq r\leq 2^k-1$ 也都成立。因为 $\{n_{s_i}\,|\,1\leq i\leq t\}=\{n_i\,|\,1\leq i\leq t\}$，所以，存在 i，

978-1-935068-10-5 © 2010 SciRes.

$1 \le i \le t$,使$C_{l_i+r} = D_{n_i+r}$ 对于任意 $0 \le r \le 2^k - 1$ 也都成立，所以 C 与 D 在同一等价类中。

这样就有下面的结果：

引理 3.2

$$\text{对任意 } k \ge \frac{n+1}{2}, n \ge 3,$$

$$N(2^k t, n) \ge \frac{(2^{k-1})! C_{2^{n-k}}^{t}}{\left((2^{2k-n-1})!\right)^{2^{n-k}} 2^{n-k}}, t = 1,3,5\cdots 2^{n-k} - 1$$

最后，根据定理 3.4 和引理 3.2 得

定理 3.5

2 阶相关免疫函数的个数 $N(n)$ 至少为：

$$\sum_{k=[\frac{n+2}{2}]}^{n-1} \frac{(2^{k-1})! 2^{2^{n-k-1}}}{\left((2^{2k-n-1})!\right)^{2^{n-k}} 2^{n-k}} + 2 \text{。}$$

证明 $N(n) = \sum_{s=0}^{2^{n-2}} N(4s, n, 2, 2) \ge$

$$\sum_{k=[\frac{n+2}{2}]}^{n-1} \left(\sum_{i=1}^{2^{n-k-1}} \frac{(2^{k-1})! C_{2^{n-k}}^{2i-1}}{\left((2^{2k-n-1})!\right)^{2^{n-k}} 2^{n-k}} \right) + 2$$

$$= \sum_{k=[\frac{n+2}{2}]}^{n-1} \frac{(2^{k-1})! 2^{2^{n-k-1}}}{\left((2^{2k-n-1})!\right)^{2^{n-k}} 2^{n-k}} + 2 \text{。}$$

4 结束语

相关免疫函数是密码学中的一个重要概念，它是为抵抗 DC 攻击而提出的。由于在密码学中有重要作用自 1984 年 Seigenthaler T.提出以来，国内外学者对此进行了大量研究，取得了丰富的结果。温巧燕等人 1998 年得到的一类正交矩阵的下界一直沿用至今未有突破。本文改进了文献[1]构造，在构造的 2 阶相关免疫函数中定义了等价关系，证明了一个等价类内的正交矩阵无相同行，可以用定理 3.2 构造新的正交矩阵，并证明了不同等价类矩阵构造的正交矩阵互不相同，从而改进了 $N^{(2)}(n)$ 的下界。本文中结果比文献[1]中的结果从形式上看要简单，但却大得多,是比较好的。

致 谢

作者对唐元生教授的有益讨论和帮助表示衷心的感谢。

References (参考文献)

[1] Wen Qiao-yan. Niu Xin-xin and Yang yi-xian. Boolean Founctions in Modern Cryptography [M]. Beijing:Science Press, 2000: 178-181.
温巧燕，钮心沂，杨义先. 现代密码学中的布尔函数[M]. 科学出版社 2000，P 74-80.

[2] Seigenthaler T. Correlation-Immunity of nonlinear combining functions for cryptographic applications [J] IEEE Trans on IT, 1984, 30(5) ，P 776-780.

[3] Xiao Guo-zhen. Massey J L. A Spectral Characterization of Correlation-immune Combining functions[J]IEEE Trans on IT, 1988, 34(3) ，P 569-571.

[4] Feng deng-guo. Xiao Guo-zhen. Dual distance and the order of correlation immune function[J]Journal of communication. 1994，15(1) ，P 15-16.
冯登国，肖国镇. 对偶距离和相关免疫阶[J]. 通信学报，1994，15(1) ，P 15-16.

[5] Yang Yi-xian. On the enumeration of correlation-immune function[J]Journal of electronic science, 1993，15(2) ，P 140-146
杨义先，相关免疫布尔函数的计数[J]. 电子科学学刊，1993，15(2) ，P 140-146.

[6] Ding chun-sheng. Xiao Guo-zhen. Stream cryptography and its implication [M] Industry of natural defense press.1994，P 161-173.
丁存生，肖国镇。流密码学及其应用[M]. 国防工业出版社，1994，P 161-173.

[7] Wang Yu-ming. He Da-ke. Basic and Implication of cryptography[M].Xi-an electric science university press, 1990，P 150-151.
王育民，何大可。保密学基础与应用[M]。西安电子科技大学.

[8] Yang Yi-xian,Lin Xv-rui. Codes and cryptography[M]Poste and telecom press, 1992，P 590-610.
杨义先，林须端。编码密码学 [M]。人民邮电出版社，1992，P 590-610.

[9] Stinson D R. The combinatorices of authentication and secrecy codes. [J].Cryptology, 1990, 2(1), P 23-49.

[10] Mu Jiao,Wen qiao yan. On the construction and numeration of Symmetric correlation immune function[J]. Journal of Beijin University of Posts and telecommunications, 2008，3,P59-62.
莫娇，温巧燕。对称相关免疫函数的构造[J]. 北京邮电大学学报，2008，3,P59-62.

[11] Zheng hao-ran, Jin cheng-hui. On construction and numeration of the correlation immune function of m-order[J]Journal of electronics science, 2008，4，P 804-808.
郑浩然，金辰辉. m 阶相关免疫函数的构造和计数[J]。电子学报，2008，4，P 804-808.