相关免疫置换的构造和计数 [1]

郑浩然 金晨辉 张海模 *

(解放军信息工程大学电子技术学院 郑州 450004)
*(中原职业技术学院 驻马店 463000)

摘 要 该文引入了相关免疫置换的概念，并给出了相关免疫置换的一个构造方法，解决了该方法构造的相关免疫置换的计数问题.

关键词 相关免疫，置换，计数
中图号 TN918.1

1 引 言

相关免疫函数 [1−6] 是密码学中的一个重要概念，它是衡量密码系统抵抗相关攻击的重要度量指标。置换是密码体制设计中广泛使用的一类密码变换，在一些特定情况下，我们需要要求置换的各坐标函数都是相关免疫的布尔函数。例如，对于 S-P 网络 (Substitution-Permutation Network)，如果某个 S 盒的单比特输入与单比特输出具有较大的相关优势，则就可能利用 P 盒是坐标移位这个特点，建立对该 S-P 网络的具有较大相关优势的线性逼近。因此，我们希望 S-P 网络的各 S 盒的单比特输入与单比特输出的相关优势都很小，最好各 S 盒的各坐标函数都是相关免疫函数，本文研究的就是这类置换的构造问题和计数问题。

2 相关免疫置换及其构造方法

为方便起见，本文将所有布尔函数都看作 0 阶相关免疫函数。

定义 1 设 $F:\{0,1\}^n \to \{0,1\}^n$ 是双射，则称 F 为 n 维置换。又若 F 的各坐标函数均是 t 阶相关免疫函数，则称 F 为 t 阶相关免疫置换。

从定义 1 可见，相关免疫置换的概念既不同于多维相关免疫函数 [6] 的概念，又不同于弹性函数 (resilient functions)[7] 的概念。弹性函数就是平衡的多维相关免疫函数。由于 t 阶多维相关免疫函数要求坐标函数的所有非零线性组合都是 t 阶相关免疫函数，因而它不可能构成 Boole 置换，故多维相关免疫函数和弹性函数的概念都不适于刻划 Boole 置换的性质。仅仅要求 Boole 置换的各坐标函数是相关免疫函数，既是可行的，又有实际的密码学意义。

由于 n 阶相关免疫的 n 元布尔函数是常值函数，因而 n 维置换至多是 $n-1$ 阶相关免疫置换。下面研究相关免疫置换的构造和计数问题。

引理 1[8,9] 设 $F:\{0,1\}^n \to \{0,1\}^n$，$f_1, f_2, \cdots, f_n$ 是 F 的 n 个坐标函数，则 F 是 n 维置换的充要条件是对所有不全为 0 的 $\alpha_1, \alpha_2, \cdots, \alpha_n \in \{0,1\}$，$\oplus_{i=1}^n \alpha_i f_i$ 均是平衡函数。

显然有：

引理 2 如果 $\forall b \in \{0,1\}^{n-m}$，$f(x,b):\{0,1\}^m \to \{0,1\}$ 都是 m 元平衡函数，则 $f(x,y)$ 是 n 元平衡函数。

引理 3 设 $f(y)$ 是 $n-m$ 元布尔函数，$0 \le t \le m-1$，如果 $\forall \delta \in \{0,1\}^{n-m}$，$\varphi_\delta(x):\{0,1\}^m \to \{0,1\}$ 都是 t 阶相关免疫的平衡函数，则 $g(x,y)=\varphi_y(x)\oplus f(y)$ 也是 t 阶相关免疫的平衡函数。又若 $\varphi_y(x)$ 的取值与 y 无关，且 $f(y)$ 是平衡函数，则 $g(x,y)=\varphi_y(x)\oplus f(y)$ 是 $t+1$ 阶相关免疫的平衡函数。

证明 给定 $b \in \{0,1\}^{n-m}$，因 $\varphi_b(x)$ 是平衡函数，故 $g(x,b)=\varphi_b(x)\oplus f(b)$ 也是平衡函数，从而由引理 2 知 $g(x,y)$ 是平衡函数。下证其它结论，不妨设 $t \ge 1$。

[1] 2001-11-20 收到，2002-08-22 改回
河南省杰出青年科学基金资助项目 (0312001800)

设 $r \le t$，任取 $1 \le i_1 < \cdots < i_r \le m$, $1 \le j_1 < \cdots < j_{t-r} \le n-m$, 则对固定 δ，由 $\varphi_\delta(x)$ 是 t 阶相关免疫函数知

$$c_{(a_1,\cdots,a_r)} = \#\{x : \varphi_\delta(x) = 1 \text{且} x_{i_1} = a_1, \cdots, x_{i_r} = a_r\}$$

与 $a_1, a_2, \cdots, a_r$ 无关，由 $\varphi_\delta(x)$ 平衡知 $2^{m-1} = \sum_{(a_1,\cdots,a_r)\in\{0,1\}^r} c_{(a_1,\cdots,a_r)}$，从而 $c_{(a_1,\cdots,a_r)} = 2^{m-r-1}$。于是，对满足 $y_{j_1} = b_1, \cdots, y_{j_{t-r}} = b_{t-r}$ 的给定 $y \in \{0,1\}^{n-m}$，$\varphi_y(x)$ 在限定 $x_{i_1} = a_1, \cdots, x_{i_r} = a_r$ 时是平衡函数，故由引理 2 知，在限定 $x_{i_1} = a_1, \cdots, x_{i_r} = a_r$；$y_{j_1} = b_1, \cdots, y_{j_{t-r}} = b_{t-r}$ 时，$g(x,y) = \varphi_y(x) \oplus f(y)$ 也是平衡函数，从而 $g(x,y)$ 与 $x_{i_1}, \cdots, x_{i_r}$；$y_{j_1}, \cdots, y_{j_{t-r}}$ 独立，这说明 $g(x,y)$ 是 t 阶相关免疫函数。

如果 $\varphi_y(x)$ 的取值与 y 无关 (此时记 $\varphi_y(x) = \varphi(x)$) 且 $f(y)$ 是平衡函数，那么在限定 (x,y) 中 $t+1$ 个变元 $x_{i_1} = a_1, \cdots, x_{i_r} = a_r$；$y_{j_1} = b_1, \cdots, y_{j_{t+1-r}} = b_{t+1-r}$ 时，若 $r \le t$，则同上可证 $g(x,y)$ 与 $x_{i_1}, \cdots, x_{i_r}$；$y_{j_1}, \cdots, y_{j_{t+1-r}}$ 独立；若 $r = t+1$，则此时对 $y_1, \cdots, y_{n-m}$ 中变量没有限定，从而对满足 $x_{i_1} = a_1, \cdots, x_{i_{t+1}} = a_{t+1}$ 的给定 x，$g(x,y) = \varphi(x) \oplus f(y)$ 关于变量 y 是平衡函数，故由引理 2 知，在限定 $x_{i_1} = a_1, \cdots, x_{i_{t+1}} = a_{t+1}$ 时，$g(x,y)$ 是平衡函数，从而 $g(x,y)$ 与 $x_{i_1}, \cdots, x_{i_{t+1}}$ 独立，这说明 $g(x,y)$ 是 $t+1$ 阶相关免疫函数。 证毕

定义 2 设 $z = (z_1, \cdots, z_n)$，$m < n$，$1 \le i_1 < \cdots < i_m \le n$，令

$$z' = (z_{i_1}, z_{i_2}, \cdots, z_{i_m})$$
$$z'' = (z_1, \cdots, z_{i_1-1}, z_{i_1+1}, \cdots, z_{i_2-1}, z_{i_2+1}, \cdots, z_{i_m-1}, z_{i_m+1}, \cdots, z_n)$$

则称 z'，z'' 为对 z 的变元的一个有序 m 二分。

定理 1 设 $2 \le m < n$，$(f_1, \cdots, f_{n-m})$ 是 $n-m$ 维置换，$x = (x_1, \cdots, x_m)$，$y = (y_1, \cdots, y_{n-m})$ 为对 $z = (z_1, \cdots, z_n) \in \{0,1\}^n$ 的变元的一个有序 m 二分，记 $\varphi(x) = \oplus_{j=1}^m x_j$，且 $\forall i \in \{1, \cdots, m\}$，$\forall j \in \{1, \cdots, n-m\}$，令

$$\varphi_i(x) = \varphi(x) \oplus x_i, \quad b_j(z) = \varphi(x) \oplus f_j(y), \quad g_{i,j}(z) = \varphi_i(x) \oplus f_j(y),$$

则 $\forall i \in \{1, \cdots, m\}$，$\forall l, j \in \{1, \cdots, n-m\}$，

$$G(z) = (g_{i,1}, \cdots, g_{i,n-m}, g_{1,j}, \cdots, g_{i-1,j}, g_{i+1,j}, \cdots, g_{m,j}, b_l)$$

都是 $m-1$ 阶相关免疫置换。

证明 易证 $\varphi(x)$ 和 $\varphi_i(x)$ 都是 $m-2$ 阶相关免疫的平衡函数，又由 $(f_1, \cdots, f_{n-m})$ 是 $n-m$ 维置换知，$f_1(y), \cdots, f_{n-m}(y)$ 都是平衡函数，故由引理 3 知诸 $g_{i,j}(z)$，$b_l(z)$ 都是 $m-1$ 阶相关免疫函数，因而 G 的各坐标函数均是 $m-1$ 阶相关免疫函数。下证 G 是置换。详细证明略。

设 $G = (G_1, \cdots, G_n)$，$\alpha_1, \cdots, \alpha_n \in \{0,1\}$ 不全为 0，则容易验证

$$\oplus_{k=1}^n \alpha_k G_k = [\oplus_{s=1}^{i-1}(\oplus_{k=1}^n \alpha_k \oplus \alpha_{n-m+s})x_s \oplus \oplus_{k=n-m+1}^n \alpha_k x_i \oplus \oplus_{s=i+1}^m (\oplus_{k=1}^n \alpha_k \oplus \alpha_{n-m+s-1})x_s]$$
$$\oplus [\oplus_{k=1}^{j-1} \alpha_k f_k(y) \oplus (\alpha_j \oplus \oplus_{k=n-m+1}^{n-1} \alpha_k) f_j(y) \oplus \oplus_{k=j+1}^{n-m} \alpha_k f_k(y) \oplus \alpha_n f_l(y)]$$

记 $\oplus_{k=1}^n \alpha_k G_k = \oplus_{k=1}^m \beta_k x_k \oplus \oplus_{k=m+1}^n \beta_k f_{k-m}(y)$，则容易证明 $\beta_1, \cdots, \beta_n$ 不全为 0，从而 $\oplus_{k=1}^n \alpha_k G_k$ 是平衡函数，再由引理 1 知 G 是置换，因而 G 是 $m-1$ 阶相关免疫置换。 证毕

3 相关免疫置换的计数

下面考察由定理 1 构造的相关免疫置换的计数问题。

引理 4　对给定的 $2 \le m < n$，由定理 1 构造的 $m-1$ 阶相关免疫置换两两相异。

证明　记 $G_{(i,j,l,f,x,y)} = (g_{i,1}, \cdots, g_{i,n-m}, g_{1,j}, \cdots, g_{i-1,j}, g_{i+1,j}, \cdots, g_{m,j}, b_l)$ 是由 z 的变元的一个有序 m 二分 x, y, $n-m$ 维置换 $f = (f_1, \cdots, f_{n-m})$ 以及 i, j, l 利用定理 1 构造的 $m-1$ 阶相关免疫置换；$G'(i', j', l', f', x', y')$ 是由另一组 (i', j', l', f', x', y') 利用定理 1 构造的 $m-1$ 阶相关免疫置换。

如果 $G_{(i,j,l,f,x,y)} = G'_{(i',j',l',f',x',y')}$，则 $G_{(i,j,l,f,x,y)}$ 与 $G'_{(i',j',l',f',x',y')}$ 的对应分量函数相等。

先考察前 $n-m$ 个分量函数。则 $\forall k \in \{1, \cdots, n-m\}$，有 $g_{i,k}(x,y) = g'_{i',k}(x',y')$，即 $\varphi_i(x) \oplus f_k(y) = \varphi_{i'}(x') \oplus f'_k(y')$，故 $f_k(y) \oplus \varphi(x) \oplus x_i \oplus f'_k(y') \oplus \varphi_{i'}(x') \equiv 0$，则有 $x'_{i'} = x_i$，从而

$$\varphi(x) \oplus f_k(y) = \varphi(x') \oplus f'_k(y') \tag{1}$$

事实上，如果 $x'_{i'}$ 不是 x 的分量，则 $x'_{i'}$ 必为 y 的分量，此时等式 $f_k(y) = \varphi(x) \oplus x_i \oplus \varphi_{i'}(x') \oplus f'_k(y')$ 的右端各函数都不含变元 $x'_{i'}$，故 $\forall k \in \{1, \cdots, n-m\}$，$f_k(y)$ 的取值都与 $x'_{i'}$ 无关，因而 $f(y)$ 的取值均与 $x'_{i'}$ 无关，故由 $x'_{i'}$ 是 y 的分量知 f 不可能是双射，这与题设矛盾，该矛盾说明 $x'_{i'}$ 是 x 的分量；假若 $x'_{i'} \ne x_i$，则由 $\varphi(x) \oplus \varphi(x')$ 和 $f_k(y) \oplus f'_k(y')$ 的取值与 $x'_{i'}$ 无关知，等式 $x'_{i'} = \varphi(x) \oplus \varphi(x') \oplus x_i \oplus f_k(y) \oplus f'_k(y')$ 右端取值与 $x'_{i'}$ 无关，得出矛盾，该矛盾说明 $x'_{i'} = x_i$，由此即得 (1) 式。

再考察中间 $m-1$ 个分量函数。则可证 $i = i'$，进而有 $x'_{i'} = x'_i = x_i$。

事实上，如果 $i \ne i'$，不失一般性，不妨设 $i < i'$，则由两个置换的第 $n-m+i$ 个分量相同知，$g_{i+1,j}(x,y) = g'_{i,j'}(x',y')$，即 $\varphi_{i+1}(x) \oplus f_j(y) = \varphi_i(x') \oplus f'_{j'}(y')$，亦即 $\varphi(x) \oplus x_{i+1} \oplus f_j(y) = \varphi(x') \oplus x'_i \oplus f'_{j'}(y')$，故由 (1) 式得 $x'_i = \varphi(x) \oplus x_{i+1} \oplus f_j(y) \oplus \varphi(x') \oplus f'_{j'}(y') = x_{i+1} \oplus f'_j(y') \oplus f'_{j'}(y')$；如果 $x'_i \ne x_{i+1}$，则等式 $x'_i = x_{i+1} \oplus f'_j(y') \oplus f'_{j'}(y')$ 的右端不含变元 x'_i，此与 x'_i 可取 0,1 值矛盾，该矛盾说明 $x'_i = x_{i+1}$。现记 $x_i = z_{j_1}$，$x_{i+1} = z_{j_2}$，则由有序 m 二分的定义知 $j_1 < j_2$，但由 $x'_{i'} = x_i$ 和 $x'_i = x_{i+1}$ 知 $x'_{i'} = z_{j_1}$，$x'_i = z_{j_2}$，从而由有序 m 二分的定义知 $i' < i$，这与 $i < i'$ 矛盾，该矛盾说明 $i = i'$，因而 $x'_{i'} = x'_i = x_i$。

于是 $\forall k \in \{1, \cdots, i-1, i+1, \cdots, m\}$，有 $g_{k,j}(x,y) = g'_{k,j'}(x',y')$，即 $\varphi_k(x) \oplus f_j(y) = \varphi_k(x') \oplus f'_{j'}(y')$，故由 (1) 式知 $x'_k = \varphi(x) \oplus x_k \oplus f_j(y) \oplus \varphi(x') \oplus f'_{j'}(y') = x_k \oplus f'_j(y') \oplus f'_{j'}(y')$，故由 x'_k 不是 y' 的分量知必有 $x'_k = x_k$，进而得到 $f'_j(y') = f'_{j'}(y')$，故由 f' 是双射知 $j = j'$。

由 $x'_i = x_i$ 及 $x'_k = x_k$ 对 $\forall k \in \{1, \cdots, i-1, i+1, \cdots, m\}$ 成立知 $x = x'$，进而由有序 m 二分的定义得 $y = y'$。

故 $\forall k \in \{1, \cdots, n-m\}$，有 $\varphi(x) \oplus f_k(y) = \varphi(x) \oplus f'_k(y)$，于是 $f_k(y) = f'_k(y)$，即 $f = f'$。

再考察最后一个分量。则有 $b_l(x,y) = b'_{l'}(x',y')$，即 $\varphi(x) \oplus f_l(y) = \varphi(x') \oplus f'_{l'}(y')$，故由 $x = x'$，$y = y'$，$f = f'$ 得 $f_l(y) = f_{l'}(y)$，从而由 f 是双射知 $l = l'$。

综上所述，有 $(i,j,l,f,x,y) = (i',j',l',f',x',y')$，即由定理 1 构造出来的 $m-1$ 阶相关免疫置换两两相异。　　证毕

定理 2　对给定的 $2 \le m < n$，由定理 1 构造出来的 $m-1$ 阶相关免疫置换的个数为

$$C_n^m m(n-m)^2 \times 2^{n-m}!$$

证明 在定理 1 构造 $m-1$ 阶相关免疫置换 $G(z)$ 时，对 z 的 n 个变元进行有序 m 二分共有 C_n^m 种方法，置换 f 有 $2^{n-m}!$ 种取法，i 有 m 种取法，j 有 $n-m$ 种取法，l 有 $n-m$ 种取法，故由引理 4 知由定理 1 构造出的 $m-1$ 阶相关免疫置换的个数为

$$C_n^m m(n-m)^2 \times 2^{n-m}! \qquad \text{证毕}$$

引理 5 对给定 n，由不同 m 按定理 1 构造的相关免疫置换互不相同。

证明 设 $G_{(m,i,j,l,f,x,y)}=(g_{i,1},\cdots,g_{i,n-m},g_{1,j},\cdots,g_{i-1,j},g_{i+1,j},\cdots,g_{m,j},b_l)$ 是由对 z 的变元的有序 m 二分 $x,y,n-m$ 维置换 $f=(f_1,\cdots,f_{n-m})$ 以及 m,i,j,l 利用定理 1 构造的相关免疫置换，$G'_{(m',i',j',l',f',x',y')}=(g'_{i',1},\cdots,g'_{i',n-m'},g'_{1,j'},\cdots,g'_{i'-1,j'},g'_{i'+1,j'},\cdots,g'_{m',j'},b'_{l'})$ 是由另一组 (m',i',j',l',f',x',y') 利用定理 1 构造的相关免疫置换，且 $m\neq m'$。不失一般性，不妨设 $m>m'$。

假设 $G_{(m,i,j,l,f,x,y)}=G'_{(m',i',j',l',f',x',y')}$，则 $G_{(m,i,j,l,f,x,y)}$ 与 $G'_{(m',i',j',l',f',x',y')}$ 的对应分量函数相等。

先考察前 $n-m$ 个分量函数。由于 $n-m<n-m'$，故 $\forall k\in\{1,\cdots,n-m\}$，有 $g_{i,k}(x,y)=g'_{i',k}(x',y')$，即 $\varphi_i(x)\oplus f_k(y)=\varphi_{i'}(x')\oplus f'_k(y')$，则按与引理 4 相同的方法可证明 $x'_{i'}=x_i$，且 $\forall k\in\{1,\cdots,n-m\}$，有

$$\varphi(x)\oplus f_k(y)=\varphi(x')\oplus f'_k(y') \tag{2}$$

再考察第 $n-m+1$ 个分量函数。如果 $i\neq 1$，则 $g_{1,j}=g'_{i',n-m+1}$，即 $\varphi_1(x)\oplus f_j(y)=\varphi_{i'}(x')\oplus f'_{n-m+1}(y')$，亦即 $\varphi(x)\oplus x_1\oplus f_j(y)=\varphi(x')\oplus x'_{i'}\oplus f'_{n-m+1}(y')$，故由 $j\in\{1,\cdots,n-m\}$ 和 (2) 式知

$$x'_{i'}=\varphi(x)\oplus f_j(y)\oplus\varphi(x')\oplus x_1\oplus f'_{n-m+1}(y')=x_1\oplus f'_j(y')\oplus f'_{n-m+1}(y')$$

如果 $x'_{i'}\neq x_1$，则函数 $x_1\oplus f'_j(y')\oplus f'_{n-m+1}(y')$ 的取值与 $x'_{i'}$ 无关，这与上述等式矛盾，从而 $x_1=x'_{i'}=x_i$，这与 $i\neq 1$ 矛盾；如果 $i=1$，则 $g_{2,j}=g'_{i',n-m+1}$，同理可证 $x_2=x'_{i'}=x_i=x_1$，也得出矛盾。

这些矛盾说明假设 $G_{(m,i,j,l,f,x,y)}=G'_{(m',i',j',l',f',x',y')}$ 不成立，因而不同 m 按定理 1 构造出不同的相关免疫置换。 证毕

定理 3 设 $t\geq 2$，则对给定 n，由定理 1 构造出来的 $t-1$ 阶相关免疫置换的个数为

$$\sum_{m=t}^{n-1} C_n^m m(n-m)^2\times 2^{n-m}!$$

证明 由定理 2 知，$\forall m\in\{t,t+1,\cdots,n-1\}$，利用该 m 由定理 1 构造的 $m-1$ 阶相关免疫置换的个数为 $C_n^m m(n-m)^2\times 2^{n-m}!$，它们都是 $t-1$ 阶相关免疫置换，且由引理 5 知，，不同 m 构造出不同的相关免疫置换，故利用定理 1 构造的 $t-1$ 阶相关免疫置换的个数为 $\sum_{m=t}^{n-1} C_n^m m(n-m)^2\times 2^{n-m}!$。 证毕

4 结 束 语

本文引入了相关免疫置换的概念，给出了相关免疫置换的一个构造方法，并解决了该方法构造的相关免疫置换的计数问题。但相关免疫置换的构造是个十分困难的问题，如何构造出更多的相关免疫置换，进而改进其计数公式的下界，有待于进一步研究和探讨。

参 考 文 献

[1] T. Siegenthaler, Correlation immunity of nonlinear combining function for cryptographic applications, IEEE Trans. on IT, 1984, 30(5), 776–780.

[2] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science, 1992, Springer-Verlag, vol.576, 86–100.

[3] J. Seberry, X. M. Zhang, Y. L. Zheng, Construction and nonlinearity of correlation-immune functions, Advances in Cryptology—EUROCRYPT'93 Lecture Notes in Computer Science, 1994, Springer-Verlag, vol.765, 181–199.

[4] Xiao Guo Zhen, J. L. Massey, A spectral characterization of correlation-immune combining functions, IEEE Trans. on IT, 1988, 34(3), 569–571.

[5] 杨义先，林须端，胡正名，编码密码学，北京，人民邮电出版社，1992.

[6] 单炜娟，相关免疫函数的结构与构造及其在流密码中的应用，[硕士学位论文]，西北电讯工程学院，1987，第三、四章.

[7] X. M. Zhang, Y. L. Zheng, On nonlinear resilent functions, Advances in Cryptology-EUROCRYPT'95, Lecture Notes in Computer Science, 1995, Springer-Verlag, vol.921, 274–288.

[8] C. Adams, S. Tavares, The structured design of cryptographically good S-boxes, Journal of Cryptology, 1990, 2(3), 27–41.

[9] 武传坤，王新梅，非线性置换的构造，科学通报，1992, 37(12), 1147–1150.

CONSTRUCTION AND ENUMERATION OF CORRELATION-IMMUNE PERMUTATIONS

Zheng Haoran Jin Chenhui Zhang Haimo*

(*Institute of Electron. Tech., the PLA Info. Eng. University, Zhengzhou* 450004, *China*)

*(*Zhongyuan Vocational Inst. of Tech., Zhumadian* 463000, *China*)

Abstract In this paper, the concept of correlation-immune permutations and a constructing method for these permutations are proposed, and the enumeration problem of correlation-immune permutations constructed by this method is solved.

Key words Correlation-immunity, Permutation, Enumeration

郑浩然： 男，1968 年生，讲师，主要研究方向为密码学.

金晨辉： 男，1965 年生，博士，教授，博士生导师，主要研究方向为密码学和信息安全.

张海模： 男，1966 年生，讲师，主要研究方向为应用数学.