均衡弹性函数的结构与弹性阶

胡予濮[1], 杨 波[1], 张玉清[2]

(1. 西安电子科技大学 ISN 国家重点实验室, 北京 710071; 2. 清华大学信息网络工程研究中心, 北京 100084)

摘 要: 弹性函数是相关免疫布尔函数的自然推广。本文讨论均衡弹性函数, 得到以下结果: 给出了均衡弹性函数的一种结构, 并因此得到了由均衡$(n, m, 2t)$弹性函数构造均衡$(n+1, m, 2t+1)$弹性函数的非线性方法; 证明了均衡线性函数的弹性阶等于对应线性分组码的码字最小重最减 1, 且弹性阶上确界常常能由非线性函数所达到。

关键词: 信息泄露; 布尔函数; 相关免疫; 弹性函数

中图分类号: TN918.4 文献标识码: A 文章编号: 0372-2112 (2002) 07-1035-03

Structures and Resilient Orders of Balanced Resilient Functions

HU Yu-pu[1], YANG Bo[1], ZHANG Yu-qing[2]

(1. *Information Security & Privacy Institute, ISN National Key Lab., Xidian University, Xi'an, Shaanxi 710071, China;*
2. *Tsinghua University, Beijing 100084, China*)

Abstract: Resilient function is a natural generalization of correlation immunity Boolean function. This paper discusses balanced resilient functions, with following results: a kind of structure of balanced resilient functions is presented, and therefore a method is given which constructs balanced $(n+1, m, 2t+1)$ resilient functions from balanced $(n, m, 2t)$ resilient functions; a proposition is given and proved that the resilient order of the balanced linear function equals the minimum weight of corresponding block code minus one, and the supremum of this order can often be reached by non-linear functions.

Key words: information leakage; boolean function; correlation immunity; resilient function

1 介绍: 均衡相关免疫函数与均衡弹性函数

相关免疫函数和弹性函数在信息安全领域扮演着重要的角色. 相关免疫性和弹性是良好的密码学性能, 它们用来防止信息泄露, 抵抗对密码体制的相关攻击.

定义 1[1,2] 设均衡布尔函数 $F: GF(2)^n \to GF(2)$. 称 F 为均衡 t 阶相关免疫函数, 如果对任意 $\{j_1, j_2, \cdots, j_t\} \subset \{1, 2, \cdots, n\}$, 任意 $a=(a_1, a_2, \cdots, a_t) \in GF(2)^t$, 任意 $b \in GF(2)$, 有

$$|\{x \mid x=(x_1, x_2, \cdots, x_n) \in GF(2)^n, (x_{j_1}, x_{j_2}, \cdots, x_{j_t})=a, F(x)=b\}| = 2^{n-1-t}$$

称 F 的相关免疫阶为 t, 如果 F 是 t 阶相关免疫的, 但不是 $t+1$ 阶相关免疫的.

已知的结果[3]: ①n 个自变量的均衡布尔函数的相关免疫阶上确界为 $t(n)=n-1$, 且被 n 个自变量的线性函数达到; ②n 个自变量的 k 次均衡布尔函数的相关免疫阶上确界为 $n-k$, 这一性质称为均衡布尔函数相关免疫阶与代数次数的"此消彼长性" (trade off).

定义 2[4,5] 设有(n, m)均衡函数(均衡函数, 即当自变量的值均匀分布时, 函数值也均匀分布) $F: GF(2)^n \to GF(2)^m$, 其中 $1 \leqslant m \leqslant n$. 取定下标集 $\{j_1, j_2, \cdots, j_t\} \subset \{1, 2, \cdots, n\}$. 称 F 为均衡$(n, m, \{j_1, j_2, \cdots, j_t\})$弹性函数, 如果对任意 $a=(a_1, a_2, \cdots, a_t) \in GF(2)^t$, 任意 $b \in GF(2)^m$, 有

$$|\{x \mid x=(x_1, x_2, \cdots, x_n) \in GF(2)^n, (x_{j_1}, x_{j_2}, \cdots, x_{j_t})=a, F(x)=b\}| = 2^{n-m-t}$$

称 F 为均衡(n, m, t)弹性函数, 如果对任意 $\{j_1, j_2, \cdots, j_t\} \subset \{1, 2, \cdots, n\}$, F 都是均衡$(n, m, \{j_1, j_2, \cdots, j_t\})$弹性函数. 称 F 的弹性阶为 t, 如果 F 是(n, m, t)弹性函数, 但不是$(n, m, t+1)$弹性函数.

显然"F 为均衡(n, m, t)弹性函数"的一个等价叙述为: 对任意 $\{j_1, j_2, \cdots, j_t\} \subset \{1, 2, \cdots, n\}$, 任意 $a=(a_1, a_2, \cdots, a_t) \in GF(2)^t$, 在 $(x_{j_1}, x_{j_2}, \cdots, x_{j_t})=a$ 前提下, $F: GF(2)^{n-t} \to GF(2)^m$ 是$(n-t, m)$均衡函数. 以下总记 $P(\cdot)$ 为概率, $P(\cdot \mid \cdot)$ 为条件概率. 则"F 为均衡(n, m, t)弹性函数"有等价叙述为 $P(F(x)=b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t})=a)=2^{-m}$.

由相关免疫函数的性质容易推出弹性函数的某些性质, 比如由文献[3]可得(n, m)均衡函数弹性阶的一个上界为 $n-m$. 文献[4]给出了弹性函数在容错分布式计算中的应用. 文献[6]给出了弹性函数的一种线性构造方法, 其基本思想仍然是: 若 F 为均衡(n_1, m, t_1)弹性函数, G 为均衡(n_2, m, t_2)弹性函数, 则 $F(x_1, x_2, \cdots, x_{n_1})+G(y_1, y_2, \cdots, y_{n_2})$ 为均衡(n_1+n_2, m, t_1+t_2+1)弹性函数. 此构造方法用大量提高自变量的维数 n 来提高弹性阶 t, 这是不经济的. 本文得到以下结果: (1) 给出了均衡弹性函数的一种结构, 并因此得到了由均衡$(n, m, 2t)$弹性函数构造均衡$(n+1, m, 2t+1)$弹性函数的非线性方法; (2) 证明了(n, m)均衡线性函数的弹性阶等于对应线性分组码的码字最小重量减 1, 因此其弹性阶上确界常常小于 $n-m$; (3) 实例说明当 $m>1$ 时, 均衡线性函数的弹性阶上确界常常能由均衡非线性函数所达到.

收稿日期: 2000-11-06; 修回日期: 2002-03-09

基金项目: 国家自然科学基金(No. 69972034); 陕西省自然科学基金(No. 99x06)

2 均衡弹性函数的结构

定义 **3** 设有两个函数 $F: GF(2)^n \to GF(2)^m$; $G: GF(2)^n \to GF(2)^m$. 设自变量 $x \in GF(2)^n$ 均匀分布. 称 F 和 G 是 t 阶对偶分布的, 若对任意 $\{j_1, j_2, \cdots, j_t\} \subset \{1, 2, \cdots, n\}$, 任意 $a = (a_1, a_2, \cdots a_t) \in GF(2)^t$, 任意 $b \in GF(2)^m$, 有

$$P(F(x) = b \mid (x_{j1}, x_{j2}, \cdots, x_{jt}) = a) = 2^{-m+1} - P(G(x) = b \mid (x_{j1}, x_{j2}, \cdots, x_{jt}) = a)$$

定理 **1** $H: GF(2)^{n+1} \to GF(2)^m$ 为均衡$(n+1, m, t+1)$弹性函数的充要件是:

$$H(x_1, x_2, \cdots, x_n, x_{n+1}) = F(x_1, x_2, \cdots, x_n) + x_{n+1}(F(x_1, x_2, \cdots, x_n) + G(x_1, x_2, \cdots x_n))$$

其中 F 和 G 都是均衡(n, m, t)弹性函数, 且 F 和 G 是$t+1$阶对偶分布的.

证明 若 H 为均衡$(n+1, m, t+1)$弹性函数, 则 $H(x_1, x_2, \cdots, x_n, 0)$和 $H(x_1, x_2, \cdots, x_n, 1)$都是均衡$(n, m, t)$弹性函数, 且对任意$\{j_1, j_2, \cdots, j_t, j_{t+1}\} \subset \{1, 2, \cdots, n\}$, 任意 $a = (a_1, a_2, \cdots, a_t, a_{t+1}) \in GF(2)^{t+1}$, 任意 $b \in GF(2)^m$, 有:

$$\begin{aligned}
&P(H(x_1, x_2, \cdots, x_n, 0) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&\quad + P(H(x_1, x_2, \cdots, x_n, 1) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&= 2P(H(x_1, x_2, \cdots, x_n, 0) = b, x_{n+1} = 0 \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&\quad + 2P(H(x_1, x_2, \cdots, x_n, 1) = b, x_{n+1} = 1 \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&= 2P(H(x_1, x_2, \cdots, x_n, x_{n+1}) = b, x_{n+1} = 0 \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&\quad + 2P(H(x_1, x_2, \cdots, x_n, x_{n+1}) = b, x_{n+1} = 1 \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&= 2P(H(x_1, x_2, \cdots, x_n, x_{n+1}) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) = 2^{-m+1}
\end{aligned}$$

又 $H(x_1, x_2, \cdots, x_n, x_{n+1}) = H(x_1, x_2, \cdots, x_n, 0) + x_{n+1}(H(x_1, x_2, \cdots, x_n, 0) + H(x_1, x_2, \cdots, x_n, 1))$ 必要性得证. 下面证明充分性, 只须证明: 对任意$\{j_1, j_2, \cdots, j_t, j_{t+1}\} \subset \{1, 2, \cdots, n, n+1\}$, 任意 $a = (a_1, a_2, \cdots, a_t, a_{t+1}) \in GF(2)^{t+1}$, 任意 $b \in GF(2)^m$, $P(H(x_1, x_2, \cdots, x_n, x_{n+1}) = b \mid (x_{j_1}, x_{x_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) = 2^{-m}$. 当 $n+1 \in \{j_1, j_2, \cdots, j_t, j_{t+1}\}$ 时显然成立; 当 $n+1$ 不属于$\{j_1, j_2, \cdots, j_t, j_{t+1}\}$ 时有

$$\begin{aligned}
&P(H(x_1, x_2, \cdots, x_n, x_{n+1}) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&= P(F(x_1, x_2, \cdots, x_n) = b, x_{n+1} = 0 \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&\quad + P(G(x_1, x_2, \cdots, x_n) = b, x_{n+1} = 1 \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&= 2^{-1}(P(F(x_1, x_2, \cdots, x_n) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) \\
&\quad + P(G(x_1, x_2, \cdots, x_n) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a)) = 2^{-m}
\end{aligned}$$

定理 1 得证

引理 **1** 设 $F: GF(2)^n \to GF(2)^m$ 为均衡(n, m, t)弹性函数. 取$\{j_1, j_2, \cdots, j_t, j_{t+1}\} \subset \{1, 2, \cdots, n\}$, $a \in GF(2)^{t+1}$, $c \in GF(2)^{t+1}$, $b \in GF(2)^m$, 设 a 与 c 的Hamming距离为 h. 则 h 为奇数时

$$P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{jt+1}) = c) = 2^{-m+1};$$

当 h 为偶数时 $P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{jt+1}) = c)$

证明 只须证明当 a 与 c 的Hamming距离为1时有 $P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{jt+1}) = c) = 2^{-m+1}$. 不妨设 a 与 c 仅有最后一位不相同, a 的前 t 位构成子向量 a'. 故

$$\begin{aligned}
&P(F = b, (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + P(F = b, (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{jt+1}) = c) \\
&= 2^{t+1}P(F = b, (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + a^{t+1}P(F = b, (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = c) \\
&= 2^{t+1}P(F = b, (x_{j_1}, x_{j_2}, \cdots, x_{j_t}) = a') = 2P(F = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}) = a') = 2^{-m+1}
\end{aligned}$$

引理 1 得证.

由定理 1 和引理 1 即得

定理 **2** 设 $F: GF(2)^n \to GF(2)^m$ 为均衡$(n, m, 2t)$弹性函数, 令 $G(x_1, x_2, \cdots, x_n) = F(1+x, 1+x_2, \cdots, 1+x_n)$. 则 G 是均衡(n, m, t)弹性函数, 且 F 和 G 是 $t+1$ 阶对偶分布的; 因此

$$H(x_1, x_2, \cdots, x_n, x_{n+1}) = F(x_1, x_2, \cdots, x_n) + x_{n+1}(F(x_1, x_2, \cdots x_n) + F(1+x, 1+x_2, \cdots, 1+x_n))$$

是均衡$(n+1, m, t+1)$弹性函数.

注 定理 1 说明, 要想由均衡(n, m, t)弹性函数 F 构造均衡$(n+1, m, t+1)$弹性函数 H, 关键是寻找一个均衡(n, m, t)弹性函数 G, 使 F 和 G 是 $t+1$ 阶对偶分布. 这样的 G 是否存在? 定理 2 肯定了当 t 为偶数时 G 是存在的, 并具体给出了一个这样的 G. 但必须注意, 由定理 2 构造出的均衡$(n+1, m, t+1)$弹性函数 H 与均衡(n, m, t)弹性函数 F 相比, 其代数次数并没有增加, 即 H 与 F 的最高次项的次数相等. 因此为了构造非线性性质较好的均衡$(n+1, m, 2t+1)$弹性函数, 我们希望找到一个这样的 G, F 和 G 是 $2t+1$ 阶对偶分布的, 且 $G(x_1, x_2, \cdots, x_n) \neq F(1+x_1, 1+x_2, \cdots, 1+x_n)$. 对于弹性函数的构造, 我们还有以下特殊情形的结论.

命题 设 $F: GF(2)^n \to GF(2)^m$ 是一个均衡(n, m, t)弹性函数; 且有一个固定的下标 $j_0 \in \{1, 2, \cdots, n\}$, 使得对任意 $\{j_1, j_2, \cdots, j_t, j_{t+1}\} \subset \{1, 2, \cdots, n\}$, $j_0 \notin \{j_1, j_2, \cdots, j_t, j_{t+1}\}$, F 都是一个均衡$(n, m, \{j_1, j_2, \cdots, j_t, j_{t+1}\})$弹性函数. 取

$$F_1(x_1, x_2, \cdots, x_n) = F(x_1, x_2, \cdots, x_n); \quad F_2(x_1, x_2, \cdots, x_n) = F(x_1, \cdots, x_{j_0-1}, 1+x_{j_0}, x_{j_0+1}, \cdots, x_n);$$ 则

$$G(x_1, x_2, \cdots, x_n, x_{n+1}) = F_1 + x_{n+1}(F_1 + F_2)$$

是一个均衡$(n+1, m, t+1)$弹性函数.

证明 由定理 1, 只须证明 F_1 和 F_2 是 $t+1$ 阶对偶分布的, 取任意下标集 $\{j_1, j_2, \cdots, j_t, j_{t+1}\} \subset \{1, 2, \cdots, n\}$. 当 $j_0 \notin \{j_1, j_2, \cdots, j_t, j_{t+1}\}$ 时, 由命题假设有

$$P(F_1(x) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) = P(F_2(x) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) = 2^{-m}$$

当 $j_0 \in \{j_1, j_2, \cdots, j_t, j_{t+1}\}$ 时, 不妨设 $j_0 = j_{t+1}$, 由命题假设和定理 1 有

$$P(F_1(x) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + P(F_2(x) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a)$$

$= P(F(x) = b \mid (x_{j_1}, x_{t_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a) + P(F(x) = b \mid (x_{j_1}, x_{j_2}, \cdots, x_{j_t}, x_{j_{t+1}}) = a') = 2^{-m+1}$;

这里 $a = (a_1, a_2, \cdots, a_t, a_{t+1})$; $a' = (a_1, a_2, \cdots, a_t, 1 + a_{t+1})$. 命题得证.

3 线性函数的弹性阶上确界

引理 **2** 记(n, m)均衡函数 $F(x) = (F_1(x), F_2(x), \cdots, F_m(x))$. 则 F 的弹性阶为 t 的充要条件是对任意 $c = (c_1, c_2, \cdots, c_m) \in GF(2)^m$, $c \neq 0$, $\sum_{j=1}^{m} c_j F_j(x)$ 是均衡 t 阶相关免疫函数.

设(n, m)均衡线性函数为 $F(x) = xG$, 其中 $x = (x_1, x_2, \cdots, x_n) \in GF(2)^n$, $G = [g_{ij}]_{n \times m}$ 为 $GF(2)$ 上的 $n \times m$ 的阶矩阵, 且 $rank(G) = m$. 又 $F(x) = (F_1(x), F_2(x), \cdots, F_m(x))$, 其中 $F_j(x) = \sum_{i=1}^{n} g_{ij} x_i$.

定理**3** 均衡线性函数 $F(x) = xG$ 的弹性阶等于以 G^{τ} 为生成矩阵的线性分组码的码字最小重量减小 1.

证明　由引理 2 知, 说 F 是均衡(n, m, t)弹性函数等价于说对任意 $c = (c_1, c_2, \cdots, c_m) \in GF(2)^m$, $c \neq 0$, $\sum_{i=1}^{n} (\sum_{j=1}^{n} c_j g_{ij}) x_i$ 是均衡 t 阶相关免疫函数; 即又等价于说对任意 $c = (c_1, c_2, \cdots, c_m) \in GF(2)^m$, $c \neq 0$, 向量 $(\sum_{j=1}^{m} c_j g_{1j}, \sum_{j=1}^{m} c_j g_{2j} \cdots, \sum_{j=1}^{m} c_j g_{nj})$的重量不小于 $t+1$; 即又等价于说以 G^{τ} 为生成矩阵的线性分组码的码字最小重量不小于 $t+1$. 定理 3 得证.

推论 **1** 设(n, m)均衡线性函数的弹性阶上确为 $t_1(n, m)$, 则

$$\max\left(\left\lfloor \frac{n}{m} \right\rfloor - 1, 2^{m-1}\left\lceil \frac{n}{2^m - 1} \right\rceil - 1\right) \leqslant t_1(n, m) \leqslant 2^{m-1}\left(\frac{n}{2^m - 1}\right) - 1$$

其中$\lfloor x \rfloor$ 表示不小于 x 的最小整数;$\lceil x \rceil$表示不超过 x 的最大整数.

证明　由定理 1 及 Plotkin 限(见文[7])得 $t_1(n, m) \leqslant 2^{m-1}\left(\frac{n}{2^m - 1}\right) - 1$. 另一方面, 可取 $n \times m$ 阶矩阵 $\boldsymbol{G}$ 如下: $\boldsymbol{G}$ 的第一列为某个最小周期为 $2^m - 1$ 的 m-序列的某个 n 工的串; G 的第二列为该序列的该串的一步右平移串; G 的第三列为该序列的该串的二步右平移串; …; G 的第 m 列为该序列的该串的 $m-1$ 步右平移串. 由 m-序列的性质即得 $F(x) = xG$ 的弹性阶 $t \geqslant 2^{m-1}\left\lceil \frac{n}{2^m - 1} \right\rceil - 1$. 又可取 $n \times m$ 阶矩阵 G 为: $G^l = [I, I, \cdots, I, P]$, 其中 I 为 m 阶单位阵, P 为 $m \times (n - m\lceil \frac{n}{m} \rceil)$阶全 1 矩阵. 容易看出此时 $F(x) = xG$ 的弹性阶 $t \geqslant \lfloor \frac{n}{m} \rfloor - 1$. 推论 1 得证.

由文[7]知 $t_1(n, m)$ 的上限还有 Hamming 限和 V-G 限, 此处不再叙述.

4 均衡函数的弹性阶上确界的讨论

以下将(n, m)均衡仿射函数的弹性阶上确界记为 $t_1(n, m)$, (n, m)均衡非仿射函数的弹性阶上确界记为 $t_2(n, m)$. 当 $t_1(n, m) \leqslant t_2(n, m)$时, 我们称$(n, m)$是非线性可达的, 否则称$(n, m)$是非线性不可达的. 我们有

例 **1**　由相关免疫函数的结论(如文献[3])可知$(n, 1)$都是平线性不可达的.

例 **2**　$(2, 2)$和$(3, 2)$都是非线性不可达的, 这是因为: ① $GF(2)^2$ 上的置换都是仿射函数; ②不难证明 $t_1(3, 2) = 1$.

例 **3**　$(4, 2)$是非线性可达的, 这是因为: ①$(3, 2)$均衡函数的总数为 $8!/2^4 = 2520$, 而$(3, 2)$均衡一次函数的总数仅为 $7 \times 6 \times 4 = 168$; ②由定理 1, 任何一个$(3, 2)$均衡非线性函数都可以构造成一个均衡$(4, 2, 1)$弹性函数; ③不难证明 $t_1(4, 2) = 1$.

例 **4**　当 $m \geqslant 3$ 时, (m, m)和$(m+1, m)$都是非线性可达的, 这是由于定理 1 和定理 2.

对于其他情形的(n, m), (n, m)是否非线性可达尚不清楚.

5 结论与问题

本文给出了均衡弹性函数的一种结构, 并因此得到了由均衡$(n, m, 2t)$弹性函数构造均衡$(n+1, m, 2t+1)$弹性函数的一种方法, 该方法是非线性的, 使得自变量的维数和弹性阶同步增加. 本文用线性分组码的码字最小重量来描述均衡线性函数的弹性阶, 得出其弹性阶上确界一般小于 $n-m$; 本文以实例说明均衡线性函数的弹性阶上确界常常能由均衡非线性函数所达到, 因此弹性阶与代数次数已不具有明显的"此消彼长性"(trade off). 这些都说明弹性函数的结构要比相关免疫布尔函数的结构复杂得多. 还有下述问题尚待解决, 有些问题可能是困难的: ①由均衡$(n, m, 2t-1)$弹性函数构造均衡$(n+1, m, 2t)$弹性函数的实用方法; ②我们已经发现弹性阶与代数次数具有某种程度的相互制约作用, 但尚不清楚这种相互制约作用的细部结构是什么样的; ③(n, m)有没有可能 $t_1(n, m) < t_2(n, m)$.

参考文献:

[1] T Siegenthaler. Correlation immunity of nonlinear combining functions for cryptographic applications [J]. IEEE Trans Inform Theory, 1984, IT-30(9): 776-779.

[2] R A Rueppel. Analysis and Design of Stream Ciphers [M]. Berlin: Springer-Verlag, 1986.

[3] G Z Xiao, J L Massey. A spectral characterization of correlation immune combining functions [J]. IEEE Trans Inform Theory, 1988, IT-34(5): 569-571.

[4] B Chor, O Goldreich, J Hastad, J Friedman, S Rudich, R Solensky. The bit-extraction problem or t-resilient functions [A]. In Proc 26th IEEE Symp Foundations of Computer Science [C]. 1985.

[5] C H Bennett, G Brasard, J M Robert. Privacy amplification by public discussion [J]. SIAM J Comput, 1988, 17(2): 210-2129.

[6] Lusheng Chen, Fang-Wei Fu. On the construction of new resilient functions from old ones [J]. IEEE Trans Inform Teory, 1999, IT-45(9): 2077-2082.

[7] 王新梅, 肖国镇. 纠错码-原理与方法 [M]. 西安: 西安电子科技大学出版社, 1991.