非线性 Resilient 函数的构造

张串绒[1,2]，肖国镇[2]，刘卫江[1]，齐君宜[1]
(1. 空军工程大学 电讯工程学院，陕西 西安 710077；2. 西安电子科技大学 信息保密研究所，陕西 西安 710071)

摘　要：研究了非线性 Resilient 函数的构造问题。分别给出了利用 Resilient 函数与其分量函数之间的关系构造 Resilient 函数和由线性纠错码构造非线性 Resilient 函数，以及通过置换由线性 Resilient 函数得到非线性 Resilient 函数的方法。

关键词：密码学；非线性 Resilient 函数；无偏性；线性码
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-3516(2002)06-0082-04

Resilient 函数这一概念最早在文献[1]和文献[2]中分别被 Chor, B. 和 Bennet, C. H. 各自独立的提出来，经过近几年的深入研究，已被广泛用于流密码、密钥分配、秘密共享、容错技术、量子密码学等许多领域。而在这类函数的实际应用中，遇到的一个重要的问题就是如何构造出具有良好性能的 Resilient 函数。关于该问题，目前已经取得了一定的成果。比如怎样构造线性 Resilient 函数的问题已经完全解决（有关结果见文献[3]），文献[4]证明了文献[1]中的猜想“存在非线性 Resilient 函数就一定存在同参数的线性 Resilient 函数”是错误的，同时给出了“存在线性 Resilient 函数就一定存在大量同参数的非线性 resilient 函数”的结论。这些都是关于 Resilient 函数构造所取得的重大成果。然而，比线性 Resilient 函数更具密码学价值的非线性 Resilient 函数的构造问题到目前为止还远远没有解决。本文研究非线性 Resilient 函数的构造问题，给出利用 Resilient 函数与其分量函数之间的关系构造 Resilient 函数和由线性纠错码构造非线性 Resilient 函数，以及通过置换由线性 Resilient 函数得到非线性 Resilient 函数的方法。

1 基本概念

设 $F_2^n = GF(2)^n$ 是二元域上的 n 维向量，F 是由 F_2^n 到 F_2^m 上的多输出布尔函数，简称 (m,n) 布尔函数。F 可表示成 $F=(f_1,f_2,\cdots,f_m)$，其中每个分量函数 f_i 都是 F_2^n 到 F_2 的布尔函数(要求 $n\geqslant m\geqslant 1$)。F 的代数次数定义为 F 的分量函数的所有非零线性组合的代数次数的最小值，即

$$\deg(F)=\min_{g\in NLC_F}\{\deg(g)\mid g=\bigoplus_{j=1}^{m}c_jf_j\}$$

其中 NLC_F 表示 F 的分量函数的所有非零线性组合的集合。如果 F 的所有分量函数都是线性的，称 $F=(f_1,f_2,\cdots,f_m)$ 是线性(n,m) 布尔函数；否则，称为非线性(n,m) 布尔函数。

定义1　设 F 是(n,m) 布尔函数，如果对任意的 $\alpha\in F_2^m$，有

$$|\{x\in F_2^n\mid F(x)=\alpha\}|=2^{n-m}$$

则称 f 是无偏的。在 F_2^n 上的无偏函数通常又称为平衡函数。

(n,m) 布尔函数 F 是无偏的，其实就是说 F 的输出等可能的取遍 F_2^m 中的每一个向量，即

$$P\{F(x)=\alpha\mid\alpha\in F_2^m\}=\frac{1}{2^m}$$

收稿日期：2002-01-10
基金项目：陕西省自然科学基金项目，(2001-X32).
作者简介：张串绒(1965-)，女，陕西眉县人，讲师，硕士，主要从事应用数学和网络与信息安全的教学与研究；
肖国镇(1934-)，男，吉林四平人，教授，博导，主要从事密码学、信息安全等方面的教学与研究.

定义 2　设 F 是 (n,m) 布尔函数,$0 \leqslant t \leqslant n-m$, $T=\{j_1,j_2,\cdots,j_t\} \subseteq \{1,2,\cdots,n\}$。如果对于任意的 $(a_1,a_2,\cdots,a_t) \in F_2^t$ 以及任意的 $\alpha \in F_2^m$

$|\{x \mid x=(x_1,x_2,\cdots,x_n) \in F_2^n, x_{j1}=a_1, x_{j2}=a_2,\cdots,x_{jt}=a_t, F(x)=\alpha\}|=2^{n-m-t}$ 称 F 为关于一个固定子集 $T=\{j_1,j_2,\cdots,j_t\}$ 是无偏的。

定义 3　设 F 是 (n,m) 布尔函数,如果 F 关于 $\{1,2,\cdots,n\}$ 的任意子集 T 是无偏的,这里 $|T|=t$,则称 F 是 (n,m,t) Resilient 函数。

由定义知,如果 $F=(f_1,f_2,\cdots,f_m)$ 是 (n,m) Resilient 函数,那么对于任意的 s,$0 \leqslant s \leqslant t$,$F=(f_1,f_2,\cdots,f_m)$ 是 (n,m,s) Resilient 函数;反之依然。

定义 4　设 F 是 (n,m) 布尔函数,$T=\{j_1,j_2,\cdots,j_t\}$。如果任意固定 F 的对应于子集 F 的 t 个变量的输入,F 的输出向量的概率分布不变,称 F 关于 T 是相关免疫的。如果 F 关于 $\{1,2,\cdots,n\}$ 的任意子集 T 是相关免疫的,$\max|T|=t$,则称 F 是 t 阶相关免疫的。

由上定义可见,平衡的 t 阶相关免疫 (n,m) 布尔函数就是 (n,m,t) Resilient 函数。

文中用 $[n,kd]$ 表示极小距离为 d,长为 n 的 k 维线性码 C,它是 F_2^n 的一个 k 维子空间,一个 $[n,kd]$ 线性码的生成矩阵 A 是 F_2 上的 $n \times k$ 阶矩阵,$\mathrm{Rank}(A)=k$,其行向量是 C 的一组基。

2　非线性 Resilient 函数的构造

2.1　由 Resilient 函数与其分量函数之间的关系构造 Resilient 函数

引理 1　$F=(f_1,f_2,\cdots,f_m)$ 是 (n,m,t) Resilient 函数的的充要条件是 $f_1,f_2,\cdots,f_m$ 的每一个非零线性组合 $f(x)=\bigoplus_{j=1}^{m} c_j f_j(x)$ 都是 $(n,1,t)$ Resilient 函数。

引理 2　设 f_i 是 $(n_i,1,t_i)$ Resilient 函数,$i=1,2,\cdots,s$,那末,$f_1(x) \oplus \cdots \oplus f_s(y)$ 是 $(\sum_{i=1}^{s} n_i, 1, s-1+\sum_{i=1}^{s} t_i)$ Resilient 函数。其中,$x \in F_2^{n_1},\cdots,y \in F_2^{n_s}$。

引理反映了 Resilient 函数与其分量函数之间的关系,为我们构造 Resilient 函数提供了理论依据。

定理 1　设 $F=(f_1,f_2,\cdots,f_m)$ 是 (n,m,t) Resilient 函数,那末

$$G(x,y,z)=(F(x) \oplus F(y), F(x) \oplus F(z))$$

是 $(3n,2m,2t+1)$ Resilient 函数。

证明:首先,我们知道

$f_1(x) \oplus f_1(y),\cdots,f_m(x) \oplus f_m(y), f_1(y) \oplus f_1(z),\cdots,f_m(y) \oplus f_m(z)$ 包含了 G 的所有 $2m$ 个分量函数。现在我们来考虑这 $2m$ 个分量的非零线性组合

$$f(x,y,z)=\bigoplus_{j=1}^{m} c_j(f_j(x) \oplus f_j(y)) \oplus \bigoplus_{j=1}^{m} d_j(f_j(y) \oplus f_j(z))$$

其中,$(c_1,c_2,\cdots,c_m) \neq (0,0,\cdots,0)$ $(d_1,d_2,\cdots,d_m) \neq (0,0,\cdots,0)$

注意到

$$f(x,y,z)=\bigoplus_{j=1}^{m} c_j f_j(x) \oplus \bigoplus_{j=1}^{m} (c_j \oplus d_j) f_j(y) \oplus \bigoplus_{j=1}^{m} d_j f_j(z)$$

由引理 1 知,当 $(c_1,c_2,\cdots,c_m) \neq (0,0,\cdots,0)$ 时,$\bigoplus_{j=1}^{m} c_j f_j(x)$ 是 $(n,1,t)$ Resilient 函数,同理 $\bigoplus_{j=1}^{m} d_j f_j(z)$ 当 $(d_1,d_2,\cdots,d_m) \neq (0,0,\cdots,0)$ 时是 $(n,1,t)$ Resilient 函数。

由于

$$(c_1,c_2,\cdots,c_m) \neq (0,0,\cdots,0),$$
$$(d_1,d_2,\cdots,d_m) \neq (0,0,\cdots,0),$$
$$(c_1 \oplus d_1, c_2 \oplus d_2,\cdots,c_m \oplus d_m) \neq (0,0,\cdots,0)$$

中至少两个成立。由引理 2,当其中 2 个成立时,$f(x,y,z)$ 是 $(3n,1,2t+1)$ Resilient 函数,当 3 个都成立时,$f(x,y,z)$ 是 $(3n,1,2t+2)$ Resilient 函数。再利用引理 1,就得到 $G(x,y,z)$ 是 $(3n,2m,2t+1)$ Resilient 函数。

与上定理类似可得

$$G(x,y,z,u)=(F(x) \oplus F(y), F(y) \oplus F(z), F(z) \oplus F(u))$$

是$(4n,3m,2t+1)$Resilient 函数。

定理2 $F(f_1,f_2,\cdots,f_m)$ 是(n_1,m,t_1) Resilient 函数, $G=(g_1,g_2,\cdots,g_m)$是(n_2,m,t_2)Resilient 函数,那末 $P(z)=F(x)+G(y)=(f_1(x)+g_1(y),\cdots,f_m(x)+g_m(y))$ 是(n_1+n_2,m,t_1+t_2+1)Resilient 函数。其中 $z=(x,y)$,$x\in F_2^{n_1}$,$y\in F_2^{n_2}$。

证明:考虑 $P(z)$ 的分量函数的任意非零线性组合

$$p(z)=\bigoplus_{j=1}^{m}c_j[f_j(x)\oplus g_i(y)]=\bigoplus_{j=1}^{m}c_jf_j(x)\oplus\bigoplus_{j=1}^{m}c_jg_j(y)$$

由引理1,$\bigoplus_{j=1}^{m}c_jf_j(x)$ 是t_1Resilient 函数,$\bigoplus_{j=1}^{m}c_jg_j(y)$ 是t_2Resilient 函数,由引理2,$p(z)$ 是(t_1+t_2+1)Resilient 函数。

定理3 设 $F=(f_1,f_2,\cdots,f_{m1})$ 是(n_1,m_1,t_1)Resilient 函数,$G=(g_1,g_2,\cdots,g_{m2})$ 是(n_2,m_2,t_2)Resilient 函数,那末,$P(z)=(f_1(x),\cdots,f_{m1}(x),g_1(y),\cdots,g_{m2}(y))$ 是(n_1+n_2,m_1+m_2,ρ)Resilient 函数,其中 $z=(x,y)$,$x\in F_2^{n_1}$,$y\in F_2^{n_2}$,$\rho=\min\{t_1,t_2\}$。

证明:考虑 $P(z)$ 的任意非零线性组合

$$p(z)=\bigoplus_{j=1}^{m_1}c_jf_j(x)\oplus\bigoplus_{j=1}^{m_2}d_jg_j(y)$$

因为$(c_1,\cdots,c_{m_1},d_1,\cdots,d_{m_2})\neq(0,0,\cdots,0)$,不失一般性,假设 $(c_1,\cdots,c_{m_1})\neq(0,0,\cdots,0)$。对于任意的子集$\{j_1,j_2,\cdots,j_{\lambda_1}\}\subseteq\{1,2,\cdots,n_1\}$ 和任意的子集$\{j_1,j_2,\cdots,j_{\lambda_2}\}\subseteq\{1,2,\cdots,n_2\}$,此处 $\lambda_1+\lambda_2=\rho$,任取 $a_1,\cdots,a_{\lambda_1},b_{\lambda_2}\in F_2$,由引理1 和无重复变元的两个函数之和平衡当且仅当两函数之一是平衡的结论及 $\bigoplus_{j=1}^{m_1}c_jf_j(x)\mid_{x_{j1}=a_1,\cdots,x_{j_{\lambda_1}}=a_{\lambda_1}}$平衡的事实,得到

$$\bigoplus_{j=1}^{m_1}c_jf_j(x)\mid_{x_{j1}=a_1,\cdots,x_{j_{\lambda_1}}=a_{\lambda_1}}\oplus\bigoplus_{j=1}^{m_2}d_jg_j(x)\mid_{y_{j1}=b_1,\cdots,y_{j_{\lambda_1}}=b_{\lambda_1}}$$

是平衡的。由引理1 我们就得到了 $P(x,y)=(f_1(x),\cdots,f_{m1}(x),g_1(y),\cdots,g_{m_2}(y))$ 是(n_1+n_2,m_1+m_2,ρ)Resilient 函数。

除了以上方法,我们还有其它构造 Resilient 函数的方法。如设 $F=(f_1,f_2,\cdots,f_m)$是(n,m,t)Resilient 函数、G 是(m,s) 无偏函数,则 $P(x)=G(F(x))$ 是(n,s,t)Resilient 函数[7]等。

2.2 由线性纠错码构造 Resilient 函数

由于 Resilient 函数和纠错码之间的密切联系,使我们可以借助纠错码理论来构造 Resilient 函数。

定理4[2] 设 $\boldsymbol{G}$ 是 F_2上的 $n\times m$ 矩阵,则当且仅当 $\boldsymbol{G}^{\mathrm{T}}$是某一$[n,m,d]$ 线性码的生成矩阵时,$F(x)=x\boldsymbol{G}$ 是$(n,m,d-1)$Resilient 函数,其中, $x\in F_2^n$。

定理4 指出了线性纠错码与线性 Resilient 函数之间的一一对应关系,同时给出了利用线性纠错码构造线性 Resilient 的方法。这些线性函数是构造非线性函数的基础(利用本文后面给出的由线性函数构造非线性函数的方法可知)。下面的定理指出了利用线性纠错码构造非线性 Resilient 的方法。

定理5[5] 设 $F=(f_1,f_2,\cdots,f_m)$是(n,m,t)Resilient 函数,$\boldsymbol{G}$ 是一个$[N,K,d]$ 线性码的生成矩阵,则$[F(x_1),F_2(x_2),\cdots,F(x_N)]\boldsymbol{G}^{\mathrm{T}}$是一个$(nN,mK,d(t+1)-1)$Resilient 函数。其中, $x_i\in F_2^n$。

将定理5 推广可得如下定理。

定理6 设 $F_i(x)$ 是(n,m,t)Resilient 函数,$i=1,2,\cdots,N$,$\boldsymbol{G}$ 是 $[N,K,d]$ 线性码的生成矩阵,则 $[F(x_1),F_2(x_2),\cdots,F(x_N)]\boldsymbol{G}^{\mathrm{T}}$ 是(n',m',t')Resilient 函数。

其中,$x_i\in F_2^{n_i}$, $n=\sum_{i=1}^{N}n_i$, $m=mK$, $t=\min\{t_{i1}+t_{i_2}+\cdots+t_{id}+d-1\cdot1\leqslant i_1<i_2<\cdots<i_d\leqslant N\}$

由上定理可见,如果存在(n,m,t)Resilient 函数和 $[N,K,d]$线性码,那末,就一定存在$(nN,mK,d(t+1)-1)$Resilient 函数。

推论1 设 $F=(f_1,f_2,\cdots,f_m)$是(n,m,t)Resilient 函数, $\boldsymbol{G}$ 是 F_2上的 $n\times k$ 矩阵,$k\leqslant m$,$\mathrm{Rank}(\boldsymbol{G})=k$,则 $P(x)=F(x)G=(f_1(x),f_2(x)\cdots f_m(x))\boldsymbol{G}$ 是(n,k,t)Resilient 函数。

推论2 设 $F=(f_1,f_2,\cdots,f_m)$是(n,m,t)Resilient 函数, $\boldsymbol{G}$ 是 F_2上的 $n\times k$ 矩阵,$k\leqslant m$,$\mathrm{Rank}(\boldsymbol{G})=k$,$D$ 是(k,s) 无偏函数,则 $P(x)=D(F(x)\boldsymbol{G}$ 是(n,s,t)Resilient 函数,$x\in F_2^n$。

2.3 由线性 Resilient 函数构造非线性 Resilient 函数的方法

定理 7　设 F 是(n,m,t) Resilient 函数，G 是 F_2^m 上的置换,记 $P=G\cdot F$,即 $P(x)=G(F(x))$是(n,m,t) Resilient 函数。

证明:由(n,m,t) Resilient 函数的定义易得。

定理 7 告诉我们,如果已知 F 是线性(n,m,t) Resilient 函数,那末由 F 可构造出 $2^m!$ 个非线性(n,m,t) Resilient 函数。举例说明如下。

设 $F(x_1,x_2,x_3,x_4,x_5,x_6)=(x_1\oplus x_2\oplus x_3,x_3\oplus x_4\oplus x_5,x_5\oplus x_6\oplus x_1)$,则 F 是$(6,2,3)$ 线性 Resilient 函数,取

$$G(u_1,u_2,u_3)=(u_1\oplus u_3\oplus u_2u_3,u_1\oplus u_2\oplus u_1u_3,u_2\oplus u_3\oplus u_1u_2)$$

则 $P=G\cdot F$ 是$(6,2,3)$ 非线性 Resilient 函数。

参考文献:

[1] Choi B, Goldreich O, Hastad J, el at;The bit extraction problem or t - resilient functions[J]. IEEE Symposium on foundations of computer science, 1985,26(2):396 - 407.

[2] Bnnett C H, Brassard G, Robert J M. Privacy amplication by public discussion[J]. SIAM J Comput,1988,17(1):210 - 229.

[3] WU Chuankun - kun, Dowson E d. On construction of resilient functions[J]. Information security and privacy springer,1996,12(3):79 - 86.

[4] Stinson D R, Massey J L. An infinite class of counterexamples to a conjecture concerining non - linear resilient functions[J]. J Of cryptology,1995,8(3):167 - 173.

[5] 王新梅,马文平,武传坤. 纠错密码理论[M]. 北京:人民邮电出版社,2001.

[6] ZHANG Xiao - mo,ZHENG Yu - liang. On nonlinear resilient functions[J]. Eurocrypt,1995,(4):32 - 38.

[7] 陈鲁生,符方伟. 复合多输出前馈函数的密码学性质[J]. 电子与信息学报,2001,23(1):60 - 67.

(编辑:门向生)

Constructions of Non - linear Resilient Functions

ZHANG Chuan - rong[1,2], XIAO Guo - zhen[2], LIU Wei - jing[1], QI Ju - yi[1]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China; 2. Institute of Information Security, Xidian University, Xi'an, Shaanxi 710071, China)

Abstract: The constructions of nonlinear Resilient functions are studied in this paper. By using the relationship between Resilient functions and their component functions, the theory of linear error - correcting code constructing non - linear Resilient function and the permutations, some methods of constructing nonlinear Resilient functions are given.

Key Words: cryptology; non - linear Resilient functions; unbiasedness; linear code

(本卷终)

空军工程大学学报(自然科学版)2002年总目次