高非线性布尔函数的构造*

孙林红 叶顶锋 吕述望 冯登国

(中国科学院研究生院信息安全国家重点实验室, 北京 100039)

(2002年8月26日收稿; 2002年11月21日收修改稿)

摘 要 给出一种构造具有高非线性程度和整体非线性度布尔函数的方法, 具体构造了 Bent 函数以及高非线性的平衡布尔函数。

关键词 布尔函数, Bent 函数, 非线性程度, 整体非线性度

中图分类号 TN913.24

1 引言

在构造密钥流生成器时, 传统的方法一般是采用线性移位寄存器和非线性的布尔函数, 而布尔函数 $f(x)$, $f: F_2^n \to F_2$ 必须满足一定的密码准则, 才能提高抵抗各种密码攻击的能力. 常用的攻击方法有 Siegenthaler 的相关攻击[1]、Berlekamp-Massey 的线性综合[2], 以及其他的线性逼近方法[3]。目前关于布尔函数的密码准则主要有平衡性、非线性程度、代数次数、整体非线性度以及相关免役等。非线性程度主要是衡量函数的线性逼近程度[4,5], 而整体非线性度则是衡量函数的扩散程度[6]。

2 预备知识

本节介绍一些相关的定义、定理和记号。

布尔函数 $f(x): F_2^n \to F_2$ 可以表示成代数正规表达式, 存在唯一的常数 $a_1, a_2, \cdots, a_{12}, \cdots, a_{12\cdots n} \in F_2$,

$$f(x_1, x_2, \cdots, x_n) = a_0 + a_1x_1 + \cdots + a_nx_n + a_{12}x_1x_2 + a_{13}x_1x_2 + \cdots + a_{12\cdots n}x_1x_2\cdots x_n,$$

这里的加法和乘法都是 F_2 上的运算。

定义 1 $f(x)$ 的代数次数, 记为 $\deg(f)$, 指其代数正规表达式中最大的次数。

对于布尔函数的许多密码性质, 都是通过 Walsh 谱来进行研究的。

定义 2 一个布尔函数 $f(x)$ 的 Walsh 谱 $F(\omega)$ 定义为

$$F(\omega) = \sum_{x} (-1)^{f(x)} (-1)^{x \cdot \omega}$$

这里 $x \cdot \omega = x_1\omega_1 + \cdots + x_n\omega_n$.

如果 $P(f(x)=1) = P(f(x)=0) = 0.5$, 则称 $f(x)$ 为平衡函数, 也即 $F(0) = 0$.

记 F_n 为所有具有 n 个输入变量的布尔函数的集合, 对于任意两个函数 $f(x), g(x) \in F_n$, 则它们的 Hamming 距离定义为:

$$d_H(f, g) = |\{x | f(x) \neq g(x), x \in F_2^n\}|.$$

定义 3 一个布尔函数 $f(x)$ 的非线性程度, 记为 N_f, 表示为:

$$N_f = \min_{g \in A_n} d_H(f, g),$$

这里 $A_n = \{a_0 + a_1x_1 + \cdots + a_nx_n | a_i \in F_2, 0 \leqslant i \leqslant n\}$ 为所有 n 个变量的仿射函数的集合。

由 $f(x)$ 的 Walsh 谱可知:

*973 项目(19970309)课题和中国科学院百人计划资助

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n,\ \omega \neq 0} |F(\omega)|.$$

设计具有高非线性程度的布尔函数是密码设计中的一个重要而又值得研究的问题. 对于 n 为偶数, Bent 函数可获得最大非线性程度; 对于 n 为奇数, 则设计具有最大非线性程度的布尔函数是很困难的。由于 Bent 函数不平衡, 所以另一个困难的问题就是当 n 为偶数时, 设计具有最大非线性程度的平衡布尔函数。

非线性程度是衡量一个函数的线性逼近程度, 而整体非线性度则是衡量一个函数的扩散程度, 下面介绍整体非线性度.

设 $\alpha \in F_2^n$, 记 $\Delta(\alpha) = \sum_x (-1)^{f(x)+f(x+\alpha)}$.

定义 **4** 一个布尔函数 $f(x)$ 的整体非线性度, 记为 λ_f, 表示为:

$$\lambda_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in F_2^n,\ \alpha \neq 0} |\Delta(\alpha)|.$$

同样对于 n 为偶数, Bent 函数可获得最大整体非线性度; 对于 n 为奇数, 则设计具有最大整体非线性度的布尔函数是很困难的。由于 Bent 函数不平衡, 所以另一个困难的问题就是当 n 为偶数时, 设计具有最大整体非线性度的平衡布尔函数。

本文的目的在于构造高非线性布尔函数, 这里的高非线性指不仅具有较高的非线性程度, 而且具有较高的整体非线性度. 目前对函数的构造, 方法很多, 角度也不同, 如直接构造高阶扩散函数、高阶相关免役函数、高非线性程度的函数等; 但同时要求函数满足多个密码性质的方法不多, Thomas Johansson 构造了同时具有高阶相关免役和高非线性程度的函数. 本文的重点是构造同时具有高非线性程度和高整体非线性度的函数。

3 函数的构造

在函数的构造上, 有一种较常用的思想, 利用小变量的函数来构造大变量的函数, 我们的构造也是基于这样的思想。

定理 **1** 设 n, m, t 和 d 为正整数, $n \geqslant 4$, $1 \leqslant t \leqslant n-3$, $1 \leqslant d \leqslant n-t$, $m \leqslant n-d$. 对于每一对 (y, i), $y \in F_2^d$, $i = 1, \cdots, m$, $A_y^i \in F_2^{n-d}$ 满足 $w_H(A_y^i) \geqslant t+1$, 对于每一 $a \in F_2^{n-d}$, $c = (c_1, \cdots, c_m) \in F_2^m$, 记

$$s_{a,c}^* = \left| \left\{ y \in F_2^d \mid \sum_{i=1}^m c_i A_y^i = a \right\} \right|, \text{ 又记 } s^* = \max_{c \in F_2^m} \max_{a \in F_2^{n-d}} s_{a,c}^*.$$

定义函数 F: $F_2^n \to F_2^m$, $F(y, x) = (A_y^1 \cdot x, A_y^2 \cdot x, \cdots, A_y^m \cdot x)$, 这里 $y = (y_1, \cdots, y_d) \in F_2^d$, $x = (x_1, \cdots, x_{n-d}) \in F_2^{n-d}$, 则有下述结论成立:

(1)如果对任一 $c \in F_2^m$, $c \neq 0$, $\sum_{i=1}^m c_i A_y^i \neq 0$, 则 F 平衡;

(2)如果对任一 $a \in F_2^{n-d}$, $0 \leqslant wt(a) \leqslant t$, 任一 $c \in F_2^m$, $c \neq 0$, 满足 $\sum_{i=1}^m c_i A_y^i \neq a$, 则 F 满足 t 阶相关免役;

(3) $N_f = 2^{n-1} - s^* 2^{n-d-1}$.

在文献[7], [8]中, Thomas Johnson 利用距离大于等于 $t+1$ 的线性码, 来构造函数 F, 这样构造的函数满足 t 阶相关免役, 同时具有较高的非线性程度. 而本文侧重于构造具有较高整体非线性度和非线性程度的布尔函数, 基于这样的出发点来设计向量 A_y^i, 由于我们只针对单输出的布尔函数, 所以仅考虑 $m=1$。

设 $1 \leqslant d \leqslant n$, $y \in F_2^d$, $x \in F_2^{n-d}$, $F(y, x) = \boldsymbol{A}_y \cdot \boldsymbol{x}$, $\boldsymbol{A}_y \in F_2^{n-d}$, 那么对于所有的 $\boldsymbol{A}_y \in F_2^{n-d}$, 构成一个 $2^d \times (n-d)$ 矩阵 $\boldsymbol{A}$ 如下:

$$\boldsymbol{A} = \begin{pmatrix} A_{00\cdots0} \\ \vdots \\ A_{11\cdots1} \end{pmatrix} = \begin{pmatrix} A_{00\cdots0}^{(1)} & \cdots & A_{00\cdots0}^{(n-d)} \\ \vdots & & \vdots \\ A_{11\cdots1}^{(1)} & \cdots & A_{11\cdots1}^{(n-d)} \end{pmatrix}$$

其中 $\boldsymbol{A}_y^{(j)}$ 表示向量 $\boldsymbol{A}_y^{(j)}$ 的第 j 个比特。

记函数 f_i: $F_2^d \to F_2$, $f_i(x) = A_x^{(i)}$, $1 \leqslant i \leqslant n-d$, 所以 $f_i(x)$ 的真值表就是 $(A_{00\cdots0}{}^{(i)}, A_{00\cdots1}{}^{(i)},$

…, $A_{11\cdots1}{}^{(i)}$), 记函数 G: $F_2^d \to F_2^{n-d}$, $G(x)=(f_1(x), \cdots, f_{n-d}(x))$, 则有构造 Bent 函数的定理 2.

定理 2　设 n 为偶数, $d=n/2$, $G(x)$为 $F_2^{n/2}\to F_2^{n/2}$ 的置换, 则由上述定义的函数 $F(y, x)=\boldsymbol{A}_y \cdot \boldsymbol{x}$ 为 Bent 函数。

证明

由差分的定义有, 对于任意向量$(y_0, x_0)\neq 0$,

$$\begin{aligned}\Delta(y_0, x_0)&=\sum_{y, x}(-1)^{F(y, x)+F(y+y_0, x+x_0)}\\&=\sum_y\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}+\boldsymbol{A}_{y+y_0}\cdot(\boldsymbol{x}+\boldsymbol{x}_0)}=\sum_y\sum_x(-1)^{(\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0})\cdot\boldsymbol{x}}(-1)^{\boldsymbol{A}_{y+y_0}\cdot\boldsymbol{x}_0}\\&=\sum_y(-1)^{\boldsymbol{A}_{y+y_0}\cdot\boldsymbol{x}_0}\sum_x(-1)^{(\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0})\cdot\boldsymbol{x}}。\end{aligned}$$

若 $y_0\neq 0$, 由于 $G(x)$为置换, 所以有 $\boldsymbol{A}_y\neq\boldsymbol{A}_{y+y_0}$, 即 $\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0}\neq 0$, 因此$\sum_x(-1)^{(\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0})\cdot\boldsymbol{x}}=0$, 从而 $\Delta(y_0, x_0)=0$.

若 $y_0=0$, 由于$(y_0, x_0)\neq 0$, 所以 $x_0\neq 0$,

$$\Delta(y_0, x_0)=\sum_y(-1)^{\boldsymbol{A}_{y+y_0}\cdot\boldsymbol{x}_0}\sum_x(-1)^{(\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0})\cdot\boldsymbol{x}}=2^{\frac{n}{2}}\sum_y(-1)^{\boldsymbol{A}_{y+y_0}\cdot\boldsymbol{x}_0}=2^{\frac{n}{2}}\sum_y(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}_0}。$$

由于 $G(x)$为置换, 所以 $\boldsymbol{A}_y$ 取遍$F_2^{n/2}$, 且每个向量只取一次, 所以有 $2^{\frac{n}{2}}\sum_y(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}_0}=0$, 所以$\Delta(y_0, x_0)=0$, 即 $F(y, x)$为 Bent 函数。

相应的 Bent 函数构造方法如下:

↴确定 n, $d=n/2$

↴随机产生 $F_2^{n/2}\to F_2^{n/2}$ 的置换 $G(x)=(f_1(x), \cdots, f_{n/2}(x))$

↴构造 F_2上 $2^{n/2}\times(n/2)$矩阵 $\boldsymbol{A}$, $f_i(x)$的真值表作为 $\boldsymbol{A}$ 的第 i 列, $i=1, \cdots, n/2$

↴设矩阵 $\boldsymbol{A}$ 第y 行为 $\boldsymbol{A}_y$, 则函数 $F(y, x)=\boldsymbol{A}_y\cdot\boldsymbol{x}$ 为 Bent 函数

我们知道, Bent 函数具有最大的非线性程度, $N_f=2^{n-1}-2^{n/2-1}$, 具有最大的整体非线性度 $\lambda_f=2^{n-1}$, 但是 Bent 函数不平衡, 而函数的平衡性是设计函数最基本的性质. 所以我们对上面的构造方法做一点改进, 即可获得具有较高非线性程度和整体非线性度的平衡函数。先分析上述构造法造成函数不平衡的原因.

$$\sum_{y, x}(-1)^{F(y, x)}=\sum_{y, x}(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_{y, x}(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_y\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}},$$

由于 $\boldsymbol{A}_y$ 取遍$F_2^{n/2}$, 所以

$$\sum_y\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_{\boldsymbol{A}_y\neq 0}\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}+\sum_{\boldsymbol{A}_y=0}\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_{\boldsymbol{A}_y=0}\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=2^{\frac{n}{2}},$$

函数不平衡的原因在于存在 y, 使得 $\boldsymbol{A}_y=0$, 因此只需替换$(0, \cdots, 0)$, 就可以使上述构造的函数达到平衡。不过, 替换$(0, \cdots, 0)$后函数的非线性程度和整体非线性度会有所降低, 但仍然很高。

定理 3　设 n 为偶数, 设 $d=n/2$, $\boldsymbol{G}(x)$为 $F_2^{n/2}\to F_2^{n/2}$ 的置换, $\boldsymbol{H}(x)$为 $F_2^{n/2}\to F_2^{n/2}$ 的映射, 当 $\boldsymbol{G}(y)\neq 0$时, $\boldsymbol{H}(y)=\boldsymbol{G}(y)$, 当 $\boldsymbol{G}(y)=0$ 时, $\boldsymbol{H}(y)=\boldsymbol{C}$, $\boldsymbol{C}$ 为$F_2^{n/2}$ 中的非零向量, $\boldsymbol{A}_y=\boldsymbol{H}(y)$, $F(y, x)=\boldsymbol{A}_y\cdot\boldsymbol{x}$, 则函数 $F(y, x)$具有如下性质:

ⅰ, $F(y, x)$为平衡函数;

ⅱ, $N_f=2^{n-1}-2^{n/2}$;

ⅲ, $\lambda_f=2^{n-1}-2^{n/2}$.

证明

ⅰ,
$$\begin{aligned}\sum_{y, x}(-1)^{F(y, x)}&=\sum_{y, x}(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_{y, x}(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_y\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}\\&=\sum_{\boldsymbol{A}_y\neq 0}\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}+\sum_{\boldsymbol{A}_y=0}\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=\sum_{\boldsymbol{A}_y\neq 0}\sum_x(-1)^{\boldsymbol{A}_y\cdot\boldsymbol{x}}=2^{n/2},\end{aligned}$$

所以 $F(y, x)$为平衡函数。

ⅱ, 因为 $s_a^*=|\{y\in F_2^{n/2}\mid \boldsymbol{A}_y=a\}|$, 当 $a\neq c$ 时, $s_a^*=1$, 当 $a=c$ 时, $s_a^*=2$, 所以 $s^*=2$,

$$N_f=2^{n-1}-s^*2^{n-d-1}=2^{n-1}-2*2^{n/2-1}=2^{n-1}-2^{n/2}.$$

ⅲ, 由差分的定义有, 对于任意向量$(y_0, x_0)\neq 0$,

$$\Delta(y_0, x_0)=\sum_{y,x}(-1)^{F(y,x)+F(y+y_0,x+x_0)}$$
$$=\sum_{y}(-1)^{A_{y+y_0}\cdot x_0}\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}.$$

设 $H(y_1)=H(y_2)=c, y_1\neq y_2$,

当 $y_0\neq 0$ 时,

(1)若 $y_0\neq y_1+y_2$, 由 H 的定义, 对任一 y, 有 $A_y\neq A_{y+y_0}$, 即 $A_y+A_{y+y_0}\neq 0$, 则 $\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}=0$, 从而 $\Delta(y_0, x_0)=0$;

(2)若 $y_0=y_1+y_2$, 由 H 的定义, 对于 $y\neq y_1, y_2$, $A_y\neq A_{y+y_0}$, 即 $A_y+A_{y+y_0}\neq 0$, 则 $\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}=0$;

对于 $y=y_1, y_2$, 有 $A_y=A_{y+y_0}$, 即 $A_y+A_{y+y_0}=0$, 则 $\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}=2^{n/2}$. 所以

$$\Delta(y_0, x_0)=\sum_{y}(-1)^{A_{y+y_0}\cdot x}\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}$$
$$=2^{n/2}\sum_{y=y_1,y_2}(-1)^{A_{y+y_0}\cdot x_0}=2^{n/2+1}(-1)^{c\cdot x_0}。$$

当 $y_0=0$ 时, 由于 $(y_0, x_0)\neq 0$, 所以 $x_0\neq 0$, 则

$$\Delta(y_0, x_0)=\sum_{y}(-1)^{A_{y+y_0}\cdot x_0}\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}=2^{\frac{n}{2}}\sum_{y}(-1)^{A_y\cdot x}$$
$$=2^{\frac{n}{2}}\left(\sum_{y}(-1)^{G(y)\cdot x_0}+(-1)^{A_{y1}\cdot x_0}-(-1)^{G(y_1)\cdot x_0}\right)$$
$$=2^{\frac{n}{2}}\left((-1)^{A_{y_1}\cdot x_0}-(-1)^{G(y_1)\cdot x_0}\right).$$

综合上述情况, 可得 $\max_{(y_0,x_0)\neq 0}|\Delta(y_0, x_0)|=2^{n/2+1}$, 从而 $\lambda_f=2^{n-1}-\frac{1}{2}\max_{(y_0,x_0)\neq 0}|\Delta(y_0, x_0)|=2^{n-1}-2^{n/2}$.

相应的高非线性平衡函数构造方法如下:

ㄐ确定 n, $d=n/2$

ㄐ随机产生 $F_2^{n/2}\to F_2^{n/2}$ 的置换 $G(x)$

ㄐ构造 $F_2^{n/2}\to F_2^{n/2}$ 的映射 $H(x)=(f_1(x), \cdots, f_{n/2}(x))$, 当 $G(y)\neq 0$ 时, $H(y)=G(y)$; 当 $G(y)=0$ 时, $H(y)=C$, C 为 $F_2^{n/2}$ 中的非零向量

ㄐ构造 F_2 上 $2^{n/2}\times(n/2)$ 矩阵 A, $f_i(x)$ 的真值表作为 A 的第 i 列, $i=1, \cdots, n/2$

ㄐ设矩阵 A 第 y 行为 A_y, 则函数 $F(y, x)=A_y\cdot x$ 为高非线性平衡函数

定理 2 和定理 3 主要是构造了 n 为偶数的函数, 对于 n 为偶数, 构造密码性质高的函数易于 n 为奇数的情况。我们知道, 只有当 n 为偶数时, 才存在 Bent 函数. 下面构造 n 为奇数的函数.

定理 4 设 n 为奇数, 设 $d=(n+1)/2$, $G(x)$ 为 $F_2^{(n+1)/2}\to F_2^{(n-1)/2}$ 的平衡函数, $A_y=G(y)$, $F(y, x)=A_y\cdot x$, 记 $\beta=\max_{y_0\neq 0}|\{y|G(y)=G(y+y_0)\}|$, 则函数 $F(y, x)$ 具有如下性质:

ⅰ, $N_f=2^{n-1}-2^{\frac{n-1}{2}}$; ⅱ, $\lambda_f=2^{n-1}-\beta 2^{\frac{n-3}{2}}$.

证明

ⅰ, $N_f=2^{n-1}-s^*2^{n-d-1}=2^{n-1}-(2^{\frac{n+1}{2}}/2^{\frac{n-1}{2}})2^{n-\frac{n+1}{2}-1}=2^{n-1}-2^{\frac{n-1}{2}}$.

ⅱ, (1)$y_0=0$, $x_0\neq 0$,

$$\Delta(y_0, x_0)=\sum_{y,x}(-1)^{F(y,x)+F(y+y_0,x+x_0)}=\sum_{y}(-1)^{A_{y+y_0}\cdot x_0}\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}$$
$$=2^{\frac{n-1}{2}}\sum_{y}(-1)^{A_y\cdot x_0}=0;$$

(2)$y_0\neq 0$, $x_0=0$,

$$\Delta(y_0, x_0)=\sum_{y,x}(-1)^{F(y,x)+F(y+y_0,x+x_0)}=\sum_{y}(-1)^{A_{y+y_0}\cdot x_0}\sum_{x}(-1)^{(A_y+A_{y+y_0})\cdot x}$$

$$=\sum_{y}\sum_{x}(-1)^{(\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0})\cdot\boldsymbol{x}}=|\{y|\ \boldsymbol{A}_y=\boldsymbol{A}_{y+y_0}\}|\ *2^{\frac{n-1}{2}};$$

(3) $y_0\neq 0$, $x_0\neq 0$

$$\Delta(y_0,x_0)=\sum_{y,x}(-1)^{F(y,x)+F(y+y_0,x+x_0)}=\sum_{y}(-1)^{\boldsymbol{A}_{y+y_0}\cdot\boldsymbol{x}}\sum_{x}(-1)^{(\boldsymbol{A}_y+\boldsymbol{A}_{y+y_0})\cdot\boldsymbol{x}},$$

$$|\Delta(y_0,x_0)|\leqslant|\{y|\ \boldsymbol{A}_y=\boldsymbol{A}_{y+y_0}\}|\ *2^{\frac{n-1}{2}}.$$

综合上述情况, 可得 $\max_{(y_0,x_0)\neq 0}|\Delta(y_0,x_0)|\leqslant\beta 2^{\frac{n-1}{2}}$, 从而 $\lambda_f=2^{n-1}-\frac{1}{2}\max_{(y_0,x_0)\neq 0}|\Delta(y_0,x_0)|\geqslant 2^{n-1}-\frac{1}{2}\beta 2^{\frac{n-1}{2}}$. $\lambda_f\geqslant 2^{n-1}-\beta 2^{\frac{n-3}{2}}$.

相应的 n 为奇数的高非线性函数构造方法如下:

1) 确定 n, $d=(n+1)/2$

2) 随机产生 $F_2^{(n+1)/2}\rightarrow F_2^{(n-1)/2}$的平衡函数 $\boldsymbol{G}(x)$ ($f_1(x)$, …, $f_{(n-1)/2}(x)$)

3) 构造 F_2上 $2^{n/2}\times(n/2)$矩阵 $\boldsymbol{A}$, $f_i(x)$的真值表作为 $\boldsymbol{A}$ 的第 i 列, $i=1,\cdots,(n-1)/2$

4) 设矩阵 $\boldsymbol{A}$ 第 y 行为 $\boldsymbol{A}_y$, 则函数 $F(y,x)=\boldsymbol{A}_y\cdot\boldsymbol{x}$ 为高非线性函数

同样可以对定理 4 中的条件稍作修改, 即可构造出 n 为奇数、具有较高 N_f, λ_f的平衡函数。

4　讨论

由上述的构造方法可知, d 在[n /2] 附近取值可使 N_f, λ_f达到最大值; 如果 d 偏离[n/2] , 则 N_f, λ_f 有所降低, 但降低的程度和 d 的偏离的关系还需进一步研究。在本文中主要研究了单输出的布尔函数, 同样可以将布尔函数 $F(y,x)$: $F_2^n\rightarrow F_2$推广到多输出布尔函数 $F(y,x)$: $F_2^n\rightarrow F_2^m$ 的情况, $1\leqslant m\leqslant n$, 不过这时的情况会更难研究。

参　考　文　献

[1] T Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. Congressus Numerantium, 1993, 92: 105~110

[2] A Menezes, P van Oorschot, S Vanstone. Handbook of applied cryptography. CRC Press, 1997

[3] C Ding, G Xiao, W Shan. The stability theory of stream ciphers. Number 561, Lectures Notes in Computer Science. Springer-Verlag, 1991

[4] K Kurosawa, T Satoh, K Yamamoto. Highly nonlinear t-Resilient functions. Journal of Univer Computer Science, 1997, 3(6): 721~729

[5] X M Zhang, Y. Zheng. On nonlinear resilient functions. Advances in Cryptography-EUROCRYPT' 95. Lecture Notes in Computer Science, 1995, 921: 274~288

[6] B Preneel, W V Leekwijck, L V Linden, R Govaerts, J Vandewalle. Propagation characteristics of Boolean function. Advances in Cryptography-EUROCRYPT' 1990. Lecture Notes in Computer Science, 1991, 473: 161~173

[7] Thomas Johnsson, Enes Pasalic. A construction of resilient functions with high nonlinearity. Lectures Notes in Computer Science. Springer-Verlag, 2000

[8] E Pasalic, S maitra, T Johnsson, P Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity. Journal of Computing, 1999, 18: 197~207

Construction of Boolean Function with High Nonlinearity

SUN Lin-Hong　YE Ding-Feng　LÍ Shu-Wang　FENG Deng-Guo

(*State Key Laboratory of Information Security, Graduate School, Chinese Acadamy of Sciences, Beijing* 100039, *China*)

Abstract　A method for construction of Boolean function with high nonlinearity and differential uniformity is proposed, Bent functions and balanced functions with high nonlinearity are constructed in detail.

Key words　Boolean function, Bent function, nonlinearity, differential uniformity