# 关于 Tu-Deng 函数的一个注记*

杜育松[1,2],张方国[1,3]
(1. 中山大学 信息科学与技术学院,广东 广州 510006;
2. 福建师范大学 网络安全与密码技术重点实验室,福建 福州 350007;
3. 中国科学院 软件研究所,北京 100190)

**摘 要**:2009年,Tu和Deng在一个组合猜想成立的基础上,构造了同时具有最优代数免疫性、最优代数次数和高非线性度的一类偶数元布尔函数。这类函数被称为Tu-Deng函数。基于同一猜想,Tu和Deng又构造了同时具有次最优代数免疫性、最优代数次数和较高非线性度的一类偶数元的1-阶弹性函数。通过研究由Tu-Deng函数导出的两个布尔函数的级联的密码学性质,在Tu-Deng猜想成立的基础上,给出一类奇数元的1-阶弹性布尔函数。这类函数同时具有次最优代数免疫性、最优代数次数和较高非线性度。

**关键词**:流密码;布尔函数;代数免疫度;非线性度;弹性函数
**中图分类号**:TP918.1 **文献标志码**:A **文章编号**:1001-2486(2012)02-0018-03

# A note on the Tu-Deng function

*DU Yusong*[1,2], *ZHANG Fangguo*[1,3]
(1. School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China;
2. Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China;
3. Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

**Abstract**: In 2009, based on a combinatorial conjecture, Tu and Deng constructed a class of Boolean functions in even variables with optimal algebraic immunity, optimal algebraic degree and good nonlinearity. This class of functions is called the Tu-Deng function. Based on the same conjecture, they also proposed a class of resilient functions in even variables with suboptimal algebraic immunity, optimal algebraic degree and good nonlinearity. By studying the cryptographic properties of the concatenation of two Boolean functions derived from the Tu-Deng function, based on Tu-Deng's conjecture, a class of resilient Boolean functions in odd variables is proposed. This class of functions has suboptimal algebraic immunity, optimal algebraic degree and good nonlinearity.

**Key words**: stream cipher; Boolean function; algebraic immunity; nonlinearity; resiliency

为了抵御代数攻击,使用在流密码中的布尔函数应该具有较大的代数免疫性[1-2]。近几年来,构造具有最优代数免疫性的布尔函数受到了较多关注[3-10]。

在2009年,Tu和Deng通过研究Dillon引入的所谓"部分扩散"(Partial Spread)函数[11]的一类子函数的代数免疫性,在一个组合猜想成立的基础上,构造了同时具有最优代数免疫性、最优代数次数和高非线性度的一类偶数元布尔函数[7-8]。这一类函数被称为Tu-Deng函数。这一猜想被称为Tu-Deng猜想。基于这一猜想,他们还给出了一类偶数元的1-阶弹性函数,并且同时具有次最优代数免疫性、最优代数次数和较高非线性度[9]。

考虑由Tu-Deng函数导出的两个布尔函数的级联的密码学性质,希望以此得到一类奇数元的1-阶弹性函数,并且具有最优的代数次数、好的非线性度和最优的代数免疫性。因为目前还没有这样一类布尔函数,以这样的方式可能无法得到一类具有最优代数免疫性的1-阶弹性函数。但是,如果Tu-Deng猜想成立,可以得到一类奇数元的具有次最优代数免疫性、最优代数次数和较高非线性度的1-阶弹性函数。

## 1 预备知识

设$n$是一个正整数。用$B_n$表示所有$n$元布

* **收稿日期**:2011-07-28
**基金项目**:国家自然科学基金资助项目(61070168, 10971246, 61003244, 60803135);网络安全与密码技术福建省高校重点实验室开放课题资助项目(2011008)
**作者简介**:杜育松(1982—),男,河北容城人,博士后,E-mail:ydu80h@163.com;
张方国(通信作者),男,教授,博士,博士生导师,E-mail:isszhfg@mail.sysu.edu.cn

尔函数组成的集合。对于布尔函数 $f \in B_n$,用 $\deg(f)$ 表示 $f$ 的代数次数,而用 $AI_n(f)$ 表示 $f$ 的代数免疫度。如果 $AI_n(f) = n/2p$,则称函数 $f$ 具有最优代数免疫性。如果 $AI_n(f) = n/2p - 1$,则称函数 $f$ 具有次最优代数免疫性。

对于 $f \in B_n$, 使得 $f(x) = 1$(相应地 $f(x) = 0$)的所有 $x = (x_1, x_2, \cdots, x_n) \in F_2^n$ 组成的集合称为上集(相应地称为下集),用 $1_f$(相应地用 $0_f$)表示。函数 $f$ 的 Hamming 重量即为 $1_f$ 的元素个数,用 $wt(f)$ 表示。

设 $n = 2k$,那么 $F_{2^n} \cong F_{2^k} \times F_{2^k}$,并且一个 $n$ 元布尔函数 $f$ 可以看成是 $F_{2^k}$ 上的一个双变量多项式 $f(x,y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j$,这里 $h_{i,j} \in F_{2^k}$。在双变量多项式表示下,布尔函数 $f \in B_{2k}$ 的代数次数由满足 $h_{i,j} \neq 0$ 的最大整数 $s = wt_2(i) + wt_2(j)$ 给出,这里 $wt_2(i)$ 是 $i$ 的二进制表示中非零系数的个数。布尔函数 $f(x,y) \in B_{2k}$ 的 Walsh 变换则由 $W_f(a,b) = \sum_{(x,y) \in F_{2^k} \times F_{2^k}} (-1)^{f(x,y) + \mathrm{tr}(ax+by)}$ 给出,其中 $a, b \in F_{2^k}$,而 tr 是绝对迹函数。此外, $W_f(a,b) = -2 \sum_{(x,y) \in 1_f} (-1)^{\mathrm{tr}(ax+by)}$ 对于所有 $(a,b) \neq 0$ 都成立。

总是设 $k$ 是一个正整数,$\alpha$ 是有限域 $F_{2^k}$ 的一个本原元,并且 $n = 2k$。$k$ 元布尔函数 $f: F_{2^k} \to F_2$ 在本文中总是定义成为 $\mathrm{supp}(f) = \{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+2^k-1-1}\}$,其中 $0 \leqslant s < 2^k - 1$。Tu-Deng 函数可以看成一个 $n$ 元布尔函数 $F: F_{2^k} \times F_{2^k} \to F_2$,即 $F_{2^k}$ 上的一个双变量多项式,定义为

$$F(x,y) = \begin{cases} f(x/y) & x \cdot y \neq 0 \\ 1 & x = 0, y \in \Delta, \\ 0 & \text{其他} \end{cases}$$

这里 $\Delta = \{\alpha^i : i = 2^{k-1} - 1, 2^{k-1}, \cdots, 2^k - 2\}$。如果 Tu-Deng 猜想成立,Tu-Deng 函数被证明具有最优代数免疫性[7-8]。根据定义为

$$F'(x,y) = \begin{cases} f(x/y) & x \cdot y \neq 0 \\ 0 & \text{其他} \end{cases}$$

的 $n$ 元布尔函数 $F': F_{2^k} \times F_{2^k} \to F_2$ 是 bent 函数的事实,同样在文献[7-8]中,Tu-Deng 函数被证明其非线性度大于或等于 $2^{n-1} - 2^{n/2-1} - 2^{k/2} k \ln 2 - 1$。

## 2　主要结果

在 Tu-Deng 函数的定义中,适当改变集合 $\Delta$ 不会影响 Tu-Deng 函数的密码学性质。

**引理 1**　对于任意整数 $t$ 满足 $0 \leqslant t < 2^k - 1$,在 Tu-Deng 函数的定义中,令 $\Delta = A = \{\alpha^{i+t} : i = 0, 1, \cdots, 2^{k-1} - 1\}$。于是 $\deg(f) = n - 1$,并且如果 Tu-Deng 猜想成立,则 $AI_n(F) = k$。

**引理 2**　设 $k$ 元布尔函数 $g: F_{2^k} \to F_2$ 定义为 $\mathrm{supp}(g) = \{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+2^{k-1}-2}\}$,其中 $0 \leqslant s < 2^k - 1$。在 $g$ 的基础上,$n$ 元布尔函数 $G: F_{2^k} \times F_{2^k} \to F_2$ 定义为

$$G(x,y) = \begin{cases} g(x/y) & x \cdot y \neq 0 \\ 1 & x = 0, y \in B \\ 1 & x \in F_{2^k}^*, y = 0 \\ 0 & \text{其他} \end{cases},$$

这里 $B \subset F_{2^k}$ 且 $|B| = 2^{k-1}$。于是 $G$ 是平衡的,并且如果 Tu-Deng 猜想成立,则 $AI_n(G) \geqslant k - 1$。

**证明**　证明过程与文献[9]中命题 3.11 类似。只写出证明概要。设 $\tilde{G}(x,y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j$ 是函数 $G$ 的一个代数次数不超过 $k-2$ 的零化子。因为 $\tilde{G}$ 零化 $G$ 并且 $\deg(\tilde{G}) \leqslant k - 2$,所以对于 $wt_2(i) + wt_2(t-i) \leqslant k - 2, 1 \leqslant t \leqslant 2^k - 2$ 和 $\gamma \in \mathrm{supp}(g)$,有 $\tilde{G}_t(\gamma) = \sum_{i=0}^{2^k-2} h_{i,t-i} \gamma^i = 0$ 成立。这表明 $\tilde{G}_t(\gamma)$ 在 $F_{2^k}$ 上有 $2^{k-1} - 1$ 个连续的根。根据 BCH 阶,$\tilde{G}_t(\gamma)$ 的非零系数的个数应该大于等于 $2^{k-1}$。而根据 Tu-Deng 猜想和文献[9]中的引理 3.10 可知,$\tilde{G}_t(\gamma)$ 的非零系数的个数应该小于 $2^{k-1}$,矛盾,于是 $\tilde{G} = 0$。类似地,根据 BCH 阶,可以证明如果 $\tilde{G}(x,y)$ 是 $G+1$ 的一个代数次数不超过 $k-1$ 的零化子,则 $\tilde{G} = 0$。因此,如果 Tu-Deng 猜想成立,则 $AI_n(G) \geqslant k - 1$。

**构造 1**　设 $F \in B_n$ 是如引理 1 所定义的函数,而 $G \in B_n$ 是如引理 2 所定义的函数,满足 $B = F_{2^k} \backslash\backslash A$。把 $F$ 和 $G$ 当做 $F_2[x_1, x_2, \cdots, x_n]$ 中的两个 $n$ 变量多项式,定义 $(n+1)$ 元布尔函数 $H(x_1, x_2, \cdots, x_n, x_{n+1}) = (1 + x_{n+1})F + x_{n+1} G$,即 $H$ 是 $F$ 和 $G$ 的级联函数。

现在考虑如构造 1 所定义的函数 $H$ 的代数免疫性、弹性、代数次数和非线性度。

关于两个布尔函数的级联的代数免疫性,Dalai 等曾有一个著名的发现[12]。

**引理 3**　设 $f, g$ 是两个 $k$ 元布尔函数,满足 $AI_k(f) = d_1$ 和 $AI_k(g) = d_2$。设 $h \in B_{k+1}$ 并且 $h = (1 + x_{k+1})f + x_{k+1} g \in B_{k+1}$。那么,如果 $d_1 \neq d_2$,则 $AI_{k+1}(h) = \min\{d_1, d_2\} + 1$,如果 $d_1 = d_2$,则 $d_1 \leqslant AI_{k+1}(h) \leqslant d_1 + 1$。

根据函数 $H$ 的定义和引理 3,可以直接得到

以下结论。

**定理 1** 设 $H \in B_{n+1}$ 是如构造 1 所定义的函数,那么 $H$ 是平衡的,并且如果 Tu-Deng 猜想成立,则 $AI_{n+1}(H) \geqslant k$。

**定理 2** 设 $H \in B_{n+1}$ 是如构造 1 所定义的函数,那么 $H$ 是 1 - 弹性的。

**证明** 容易证明布尔函数 $H$ 的 Walsh 变换满足 $W_H(a,b,c) = W_F(a,b) + (-1)^c \cdot W_G(a,b)$,其中 $a,b \in F_{2k}$ 而 $c \in F_2$。因为 $H$ 是平衡的,所以研究 $W_H(a,b,c)$ 在以下 3 种情况的取值就足够了。下面的讨论主要基于以下事实:

$$\sum_{x \in F_{2k}} (-1)^{\mathrm{tr}(\lambda x)} = \begin{cases} 2^k & \lambda = 0 \\ 0 & \text{其他} \end{cases}.$$

情况 1 $a = 0, b = 0, c = 1$

$$W_H(a,b,c) = W_F(0,0) - W_G(0,0) = 0 - 0 = 0$$

情况 2 $a \neq 0, b = 0, c = 0$

$$\begin{aligned} W_H(a,b,c) &= W_F(a,b) + W_G(a,b) \\ &= -2\sum_{(x,y) \in 1_F} (-1)^{\mathrm{tr}(ax+by)} - 2\sum_{(x,y) \in 1_G} (-1)^{\mathrm{tr}(ax+by)} \\ &= -2\sum_{\gamma \in \mathrm{supp}(f), y \in F_{2k}^*} (-1)^{\mathrm{tr}((a\gamma+b)y)} - 2\sum_{y \in A} (-1)^{\mathrm{tr}(by)} \\ &\quad -2\sum_{\gamma \in \mathrm{supp}(g), y \in F_{2k}^*} (-1)^{\mathrm{tr}((a\gamma+b)y)} - 2\sum_{x \in F_{2k}^*} (-1)^{\mathrm{tr}(ax)} \\ &\quad -2\sum_{y \in B} (-1)^{\mathrm{tr}(by)} \\ &= -2\sum_{\gamma \in \mathrm{supp}(f)} \Big( \sum_{y \in F_{2k}} (-1)^{\mathrm{tr}(a\gamma y)} - 1 \Big) - 2\sum_{y \in A \cup B} (-1)^{\mathrm{tr}(by)} \\ &\quad -2\sum_{\gamma \in \mathrm{supp}(g)} \Big( \sum_{y \in F_{2k}} (-1)^{\mathrm{tr}(a\gamma y)} - 1 \Big) - 2\sum_{x \in FF_{2k}^*} (-1)^{\mathrm{tr}(ax)} \\ &= 2wt(f) + 2wt(g) - 2 \times 2^k + 2 \\ &= 2(2^{k-1}) + 2(2^{k-1} - 1) - 2 \times 2^k + 2 \\ &= 0 \end{aligned}$$

情况 3 $a = 0, b \neq 0, c = 0$

$$\begin{aligned} &W_H(a,b,c) \\ &= -2\sum_{\gamma \in \mathrm{supp}(f)} \Big( \sum_{y \in F_{2k}} (-1)^{\mathrm{tr}(by)} - 1 \Big) - 2\sum_{y \in A \cup B} (-1)^{\mathrm{tr}(by)} \\ &\quad -2\sum_{\gamma \in \mathrm{supp}(g)} \Big( \sum_{y \in F_{2k}} (-1)^{\mathrm{tr}(by)} - 1 \Big) - 2\sum_{x \in F_{2k}^*} (-1)^{\mathrm{tr}(ax)} \\ &= 2(2^{k-1}) + 2(2^{k-1} - 1) - 2(2^k - 1) + 0 \\ &= 0 \end{aligned}$$

基于以上 3 种情况,不难推出 $H$ 是 1 - 阶弹性的。

显然 $\deg(H) \geqslant \deg(F) = n - 1$。根据 Siegenthaler 不等式,可以确定 $H$ 的代数次数。

**定理 3** 设 $H \in B_{n+1}$ 是如构造 1 所定义的函数,那么 $\deg(H) = n - 1$。

**定理 4** 设 $H \in B_{n+1}$ 是如构造 1 所定义的函数,那么 $H$ 的非线性度满足

$$nl(H) \geqslant 2^{2k} - 2^{k+1} - c_k \cdot 2^{k/2+1}$$

这里,$c_k = \dfrac{\ln 2}{3}(k-1) + \dfrac{5}{6} + \dfrac{1}{3\sqrt{3}} + \dfrac{1}{6\sqrt{2}}$。

**证明** 因为 $nl(H) \geqslant nl(F) + nl(G)$,考虑 $nl(F)$ 和 $nl(G)$。利用类似文献[8]中命题 5.4 的一个处理技巧,结合 $F$ 和 $G$ 的定义,有

$$nl(F) \geqslant 2^{2k-1} - 2^{k-1} - \max_{b \in F_{2k}^*} \Big| \sum_{y \in A} (-1)^{\mathrm{tr}(by)} \Big|$$

和

$$nl(G) \geqslant 2^{2k-1} - 2^{k-1} - \max_{\substack{a,b \in F_{2k} \\ (a,b) \neq 0}} S_{a,b}$$

其中 $S_{a,b} = \Big| \sum_{\gamma, y \in F_{2k}^*} (-1)^{\mathrm{tr}((a\gamma+b)y)} + \sum_{x \in F_{2k}^*} (-1)^{\mathrm{tr}(ax)} + \sum_{y \in B} (-1)^{\mathrm{tr}(by)} \Big|$.

根据 Zeng 等在文献[10]中定理 2 给出的估计,对于任意 $0 \neq \lambda \in F_{2k}$ 有

$$\Big| \sum_{i=0}^{2^{k-1}-1} (-1)^{\mathrm{tr}(\lambda \alpha^i)} \Big| \leqslant c_k \cdot 2^{k/2} + 1$$

其中,$c_k = \dfrac{\ln 2}{3}(k-1) + \dfrac{5}{6} + \dfrac{1}{3\sqrt{3}} + \dfrac{1}{6\sqrt{2}}$。于是根据 $A$ 的定义和 $B = F_{2k} \backslash\backslash A$ 的事实,可以验证

$$\max_{\substack{a,b \in F_{2k} \\ (a,b) \neq 0}} S_{a,b} \leqslant 2^k + c_k \cdot 2^{k/2} - 1$$

最后有

$$\begin{aligned} nl(H) &\geqslant 2^{2k} - 2^k - c_k \cdot 2^{k/2} - 1 - \max_{a,b \in F_{2k}} S_{a,b} \\ &\geqslant 2^{2k} - 2^{k+1} - c_k \cdot 2^{k/2+1} \end{aligned}$$

证明完成。

可以看出定理 4 给出的非线性度下界比文献[4]中定理 3 和文献[6]中命题 6 给出的非线性度下界都要好。

## 3 结论

在 Tu-Deng 猜想成立的基础上,给出一类奇数元的 1 - 阶弹性布尔函数,并且同时具有最优的代数次数、较高的非线性度和次最优的代数免疫性。据了解,在这之前还没有一类这样的奇数元的布尔函数能同时满足这些密码学性质。

## 参考文献(References)

[1] Courtois N, Meier W. Algebraic attacks on stream ciphers with linear feedback [C] // Proc of Advances in Cryptology-EUROCRYPT 2003, LNCS 2729: 345 - 359.

[2] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions [C] // Proc of Advances in Cryptology-EUROCRYPT 2004, LNCS 3027: 474 - 491.

(下转第 28 页)

法所需要的时间是 Galbraith 等[5]提出的二维 GLV 方法的 0.70 和 0.73。

## 参考文献(References)


[1] Gallant R P, Lambert R J, Vanstone S A. Faster point multiplication on elliptic curves with efficient endomorphisms, [C]// Proc of CRYPTO 2001, LNCS 2139, Springer, Heidelberg, 2001:190 – 200.

[2] Park Y H, Jeong S, Kim C H, et al. An alternate decomposition of an integer for faster ponit multiplication on certain elliptic curves[C]// Proc of PKC 2002, LNCS 2274, Springer, Heidelberg, 2001:323 – 334.

[3] Sica F, Ciet M, Quisquater J J. Analysis of gallant-lambert-vanstone method based on efficient endomophisms: elliptic and hyperelliptic curves. [C]// Proc of SAC 2002, LNCS 2595, Springer, Heidelberg, 2003:21 – 36.

[4] Iijma T, Matsuo K, Chao J, et al. Construction of frobenius maps of twist elliptic curves and its application to elliptic scalar multiplication. [C]// Proc of SCIS 2002, IEICE, Japan, 2002:699 – 702.

[5] Galbraith S D, Lin X B, Scott M. Endomorphisms for faster elliptic curve cryptogrpahy on a large class of curves. [C]// Proc of EUROCRYPT 2009, LNCS 5479, Springer, Heidelberg, 2009:518 – 535.

[6] Zhou Z H, Hu Z, Xu M Z, et al. Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves[J]. Information Processing Letters, 2010, 110: 1003 – 1006

[7] Cohen H. A course in computational algebraic number theory[M]. Springer-Verlag, 1996.

[8] Hankerson D, Menezes A J, Vanstone S. Guide to elliptic curve cryptography[M]. Springer, Heidelberg, 2004.

[9] Ireland K, Rosen M. A classical introduction to modern number theory [M]. 2nd ed. GTM, Springer, New York, 1990.

[10] Galbraith S D, Lin X B, Scott M. Endomorphisms for faster elliptic curve cryptogrpahy on a large class of curves[J]. J. Cryptol, 2010.


(上接第 20 页)


[3] Li N, Qi W. Construction and analysis of Boolean functions of 2t + 1 variables with maximum algebraic immunity[C] // Proc of Advances in Cryptology-ASIACRYPT 2006, LNCS 4284: 84 – 98.

[4] Carlet C, Feng K. An infinite class of balanced functions with optimal Algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity [C] // Proc of Advances in Cryptology-ASIACRYPT 2008, LNCS 5350: 425 – 440.

[5] Qu L, Feng K, Liu F, et al.. Constructing symmetric Boolean functions with maximum algebraic immunity [J]. IEEE Transactions on Information Theory, 2009, 55(5): 2406 – 2412.

[6] Wang Q, Peng J, Kan H, et al. Constructions of cryptographically significant Boolean functions using primitive polynomials [J]. IEEE Transactions on Information Theory, 2010, 56(6): 3048 – 3053.

[7] Tu Z R, Deng Y P. A conjecture on binary string and its applications on constructing Boolean functions of optimal algebraic Immunity [EB/OL]. [2011 – 05 – 12]. Cryptology ePrint Archive, Report 2009/272, http://eprint.iacr.org.

[8] Tu Z R, Deng Y P. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity [J]. Designs, Codes and Cryptography, 2011, 60(1): 1 – 14.

[9] Tu Z R, Deng Y P. Boolean functions with all main cryptographic properties [EB/OL]. [2011 – 06 – 05]. Cryptology ePrint Archive, Report 2010/518, http://eprint.iacr.org.

[10] Zeng X, Carlet C, Shan J, et al. More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks [J]. IEEE Transactions on Information Theory, 2011, 57(9): 6310 – 6320.

[11] Dillon J F. Elementary hadamard difference sets [D]. Baltimore University of Maryland, 1974.

[12] Carlet C, Dalai D K, Gupta K C, et al.. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction [J]. IEEE Transactions on Information Theory, 2006, 52(7): 3105 – 3121.