文章编号: 1001- 2486(2010) 03- 0144- 05

一类完全非线性函数的证明与计数*

李 平, 周 悦, 李 超
(国防科技大学 理学院, 湖南 长沙 410073)

摘 要: Helleseth 等最近给出了一类二项式形式的完全非线性函数, 这是至今为止所发现的第一类由两个互不等价的单项式组成的二项式形式的完全非线性函数。本文利用 Frobinus 自同构将其变形为一个新的二项式, 给出了其完全非线性的简洁证明, 指出了这类函数与 x^2 是等价的, 最后讨论了该类完全非线性函数的计数性质。

关键词: 完全非线性函数; 扩展仿射等价; 计数
中图分类号: TN918.1 文献标识码: A

Proof and Count of a Family of Perfect Nonlinear Functions

LI Ping, ZHOU Yue, LI Chao
(College of Science, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: A new class of perfect nonlinear binomials was just found by Helleseth et al, which are the first perfect nonlinear binomials composed with two inequivalent monomials. We transformed the class of perfect nonlinear binomials to another form, and gave a concise proof for their perfect nonlineamess. It shows that this family of binomials is equivalent to . Furthermore, the calculation of the count of this family of functions is presented as well.

Key words: perfect nonlinear functions; extended affine equivalence; counting

1 预备知识和主要引理

设 $f: \mathrm{F}_q \to \mathrm{F}_q$, $q = p^n$, p 是奇素数, n 是正整数。函数 f 的差分均匀度[5] 定义为

$$\delta_f = \max_{a,\, b \in \mathrm{F}_q,\, a \neq 0} |\{x \in \mathrm{F}_q : f(x+a) - f(x) = b\}|$$

若映射 f 的差分均匀度为 k, 那么称 f 为 $k-$ 差分一致的[5]。在密码算法的设计中, 为抵抗差分密码攻击[3], 要使用 δ_f 尽可能小的函数。当 $\delta_f = 1$ 时, 函数 f 称为 F_q 上的完全非线性函数[4], 简称 PN 函数。PN 函数的构造、等价性和应用等问题, 是近年来密码函数研究的热点。2008 年, Helleseth 和 Kyureghyan 等利用有限几何的方法, 提出了一类二项式形式的 PN 函数[13], 并给出了计数以及等价性证明。这是至今发现的第一类由两个互不等价的单项式所组成的二项式形式的 PN 函数。

定义 1[15] 设 $L(x) = \sum_{i=0}^{n-1} a_i x^{p^i} \in \mathrm{F}_q[x]$, 其中 $q = p^n$, $a_i \in \mathrm{F}_q$, 则称 L 为线性化多项式。

线性化多项式给出了线性空间 F_p^n 到自身的线性变换[15]。线性化多项式和一个常数的和称为仿射多项式[15]。仿射多项式所对应的映射若是置换, 则称它为仿射置换。

定义 2[5] 设 f 和 g 是 F_q 上的两个函数, 如果存在 F_q 上两个仿射置换 l_1 和 l_2, 以及仿射映射 l_3, 使得 $f = l_1 \circ g \circ l_2 + l_3$, 其中 $\circ$ 表示函数的复合, 则称 f 和 g 是扩展仿射等价, 简称 EA 等价。

根据 PN 函数的定义, 容易证明与 PN 函数 EA 等价的函数仍然是 PN 函数[5]。另一方面, 如果将有限域 F_{p^n} 看作 F_p 上的 n 维线性空间 F_p^n, 则 F_{p^n} 中每一个元素可以认为是一个 n 维向量, 函数 $f: \mathrm{F}_p^n \to \mathrm{F}_p^n$ 的

* 收稿日期: 2009- 09- 10
基金项目: 国家自然科学基金资助项目(60803156); 信息安全国家重点实验室开放基金资助项目(01- 07)
作者简介: 李平(1981—), 男, 博士生。

图G_f 定义为: $G_f=\{(x,f(x))\mid x\in \mathrm{F}_p^n\}\subseteq \mathrm{F}_p^{2n}$。

定义 3[7]　设f 和g 是F_{p^n} 上的两个函数, 如果存在F_p^{2n} 上的仿射置换L, 使得 $G_g=L(G_f)$, 那么称f 和g 是 Carlet-Charpin-Zinoviev 等价的, 简称 CCZ 等价。

EA 等价的函数一定是 CCZ 等价的, 但 CCZ 等价的函数未必 EA 等价。2008 年, Kyureghyan 等证明了对于 PN 函数来说, EA 等价与 CCZ 等价是同一个概念[9,12], 因此下文证明等价性只需证明 EA 等价即可。2008 年, 密码学者发现了三类新的 PN 函数[9-10], 连同以前的 PN 函数[1,6,8]一起构成了至今为止全部互不等价的 PN 函数类。

定义 4　F_{p^n} 上形如 $\Pi(x)=\sum_{i,j=0}^{n-1}a_{ij}x^{p^i+p^j}$ $(a_{ij}\in \mathrm{F}_{p^n})$ 的多项式称为 Dembowski-Ostrom 多项式, 具有这种形式的 PN 函数就称为 Dembowski-Ostrom 型的 PN 函数, 简称 DO 型 PN 函数。

在已知的 PN 函数中, 除 1997 年发现的第二类以外[6], 其余五类均为 DO 型的 PN 函数。文献[13]中提出的 PN 函数也是 DO 型的二项式函数。

定义 5　设 q 是奇素数的幂, F_q 上的二次特征 η 定义为 $\eta(x)=\begin{cases}0 & x=0\\ 1 & x=\omega^{2l}\\ -1 & x=\omega^{2l+1}\end{cases}$, 这里 ω 是F_q 中的本原元。

引理 1[14]　设p 为奇素数, k 为正整数, $a_1,a_2\in \mathrm{F}_{p^k}^*$, $\eta(\cdot)$ 是F_{p^k} 上的二次特征, $v(b)=-1$ 当 $b\in \mathrm{F}_{p^k}^*$, $v(0)=p^k-1$。那么方程 $a_1x_1^2+a_2x_2^2=b$ 的解是: $N(a_1x_1^2+a_2x_2^2=b)=p^k+v(b)\eta(-a_1a_2)$。

2　完全非线性的证明及等价性

引理 2[13]　设p 为奇素数, k 为正整数, $n=2k$。定义F_{p^n} 的子集 $G=\{g\in \mathrm{F}_{p^n}\mid g^{p^k+1}=1\}$、$\Gamma=\{\gamma\in \mathrm{F}_{p^n}\mid \gamma^{p^k-1}=-1\}$ 和 $H=\{g(1-\gamma)\mid g^{p^k+1}=1,\ \gamma^{p^k-1}=-1\}=G(1-\Gamma)$。$\mathrm{F}_{p^n}$ 上的函数f 定义为$f(x)=ux^{p^k+1}+x^2$, 那么f 是F_{p^n} 上的 PN 函数当且仅当 $u\notin H\cup G$。

引理 2 中给出的函数由 x^{p^k+1} 和 x^2 两个互不等价[14]的单项式组成, 这是第一类具有这种二项式形式的 PN 函数。文献[13]中利用有限几何的方法证明了其完全非线性并讨论了计数问题。本文对其做如下变形: 先做自同构 $\delta: x\to x^{p^k}$, 然后对系数做适当变换, 得到$f(x)=\frac{1}{2}x^{2p^k}+ux^{p^k+1}$。下面对这类变形之后的函数讨论其 PN 性质, 等价性以及计数问题。

定理 1　设p 为奇素数, k 为正整数, $n=2k$, F_{p^n} 上的函数f 定义为$f(x)=\frac{1}{2}x^{2p^k}+ux^{p^k+1}$, 其中 $u\in \mathrm{F}_{p^n}$ 使得多项式 $u^{p^k}x^{2(p^k-1)}+x^{p^k-1}+u$ 没有零点。那么f 就是F_{p^n} 上的 PN 函数。

证明　设 $a,b\in \mathrm{F}_{p^n}$, $a\neq 0$, $D_f(x,a)=f(x+a)-f(x)$, 则f 是 PN 函数当且仅当 $D_f(x,a)=b$ 在 F_{p^n} 中仅有一个根。注意到

$$D_f(x,a)=\frac{1}{2}(x+a)^{2p^k}+u(x+a)^{p^k+1}-\frac{1}{2}x^{2p^k}-ux^{p^k+1}=a^{p^k}x^{p^k}+u(a^{p^k}x+x^{p^k}a)+ua^{p^k+1}+\frac{1}{2}a^{2p^k}$$

是一个仿射多项式, 因此仅需考虑线性化多项式 $\Delta_f(x,a)=a^{p^k}x^{p^k}+u(a^{p^k}x+x^{p^k}a)$ 的根数, 用 xa 替换 $\Delta_f(x,a)$ 中的 x, 得到 $\Delta_f(xa,a)=a^{2p^k}x^{p^k}+ua^{p^k+1}(x^{p^k}+x)=(a^{2p^k}+ua^{p^k+1})x^{p^k}+ua^{p^k+1}x$, 则若 x 为 $\Delta_f(x,a)$ 的一个根, 必有 $\Delta_f(xa,a)^{p^k}=u^{p^k}a^{p^k+1}x^{p^k}+(a^2+u^{p^k}a^{p^k+1})x=0$, 于是

$$(a^{p^k}+ua)\Delta_f(xa,a)^{p^k}-u^{p^k}a\Delta_f(xa,a)=a^3(u^{p^k}a^{2(p^k-1)}+a^{p^k-1}+u)x=0$$

由条件, $u^{p^k}a^{2(p^k-1)}+a^{p^k-1}+u\neq 0$, 故 $\Delta_f(x,a)=0$ 当且仅当 $x=0$, 于是f 是F_{p^n} 上的 PN 函数。　□

下面将证明上述定理中定义的 PN 函数与 x^2 的等价性。

定理2 设 p 为奇素数, k 为正整数, 并且 $n=2k$, F_{p^n} 上的函数 f 定义为 $f(x)=\frac{1}{2}x^{2p^k}+ux^{p^k+1}$, 其中 $u\in\mathrm{F}_{p^n}$ 使得多项式 $u^{p^k}x^{2(p^k-1)}+x^{p^k-1}+u$ 没有零点。那么 f 等价于 x^2。

证明 设 $L_1(x)=a_0x+a_kx^{p^k}$, $L_2(x)=x+c_kx^{p^k}$。假设 $L_1(f(x))=(L_2(x))^2$, 即

$$\frac{1}{2}a_0x^{2p^k}+(a_ku^{p^k}+a_0u)x^{p^k+1}+\frac{1}{2}a_kx^2=c_k^2x^{2p^k}+2c_0c_kx^{p^k+1}+x^2$$

故 $a_k=2, 2c_k=a_ku^{p^k}+a_0u, c_k^2=\frac{1}{2}a_0$。于是 $uc_k^2-c_k+u^{p^k}=0$, 它的根为 $(1\pm\sqrt{1-4u^{p^k+1}})/2u$, 这是因为 $1-4u^{p^k+1}\in\mathrm{F}_{p^k}$ 在 $\mathrm{F}_{p^{2k}}$ 里总有平方根。下面证明 $L_1(x)$ 和 $L_2(x)$ 均为置换, 根据定义就可以推出 x^2 和 f 是 EA 等价。

事实上, 线性化二项式 $L_2(x)=x+cx^{p^k}$ 是一个置换当且仅当 $c^{p^k+1}\neq1$, 这表明 $c_k\notin G$, 其中 $G=\{x\in\mathrm{F}_{p^{2k}}^*\mid x^{p^k+1}=1\}$, 而 $u+y+u^{p^k}y^2=0$ 在 G 中无根, 即 $y_0=(1\pm\sqrt{1-4u^{p^k+1}})/2u^{p^k}\notin G$。由 $c_k=u^{p^k-1}(-y_0)$, 有 $c_k^{p^k+1}=y_0^{p^k+1}\neq1$。因此 $c_k\notin G$, 于是 $L_2(x)$ 是一个置换。

由于 $c_k=(1\pm\alpha)/2u$, 其中 $\alpha=\sqrt{1-4u^{p^k+1}}$, 于是又有 $c_u^{p^k+1}=\frac{(1\pm\alpha)^{p^k+1}}{4u^{p^k+1}}=\frac{(1\pm\alpha)^2}{1-\alpha^2}$, 因为 $(1+\alpha)=\pm(1-\alpha)$ 不可能成立, 所以可推出 $c_k^{-2(p^k+1)}\neq1$, 即 $L_1(x)=2(c_k^2+x^{p^k})$ 是一个置换。

综上所述, x^2 和 f 是 EA 等价的。 □

3 函数类的计数

引理3 设 p 为奇素数, k 为正整数, 令 ω 为 $\mathrm{F}_{p^{2k}}$ 中的本原元, $G=\{x\in\mathrm{F}_{p^{2k}}^*\mid x^{p^k+1}=1\}$。那么

$$\mathrm{F}_{p^{2k}}^*=\{\alpha\beta\mid\alpha\in\mathrm{F}_{p^k}^*,\beta\in G\}\cup\{\alpha\beta\omega\mid\alpha\in\mathrm{F}_{p^k}^*,\beta\in G\}$$

事实上, 在 p 为奇素数时, 引理3中的表示并不唯一: 由于 $\alpha_1\beta_1=\alpha_2\beta_2$ 当且仅当 $\alpha_1\alpha_2^{-1}=\beta_2\beta_1^{-1}\in\mathrm{F}_{p^k}^*\cap G=\{1,-1\}$。因此 $\alpha_1=\alpha_2, \beta_1=\beta_2$, 或者 $\alpha_1=-\alpha_2, \beta_1=-\beta_2$, 即按照这种方式, $\mathrm{F}_{p^{2k}}^*$ 中的每个元素有且仅有两种表示形式。

定理3 设 p 为奇素数, k 为正整数, 并且 $n=2k$, 则存在 $u\in\mathrm{F}_{p^n}$, 使得

$$u^{p^k}(x^{p^k-1})^2+x^{p^k-1}+u=0 \tag{1}$$

在 $\mathrm{F}_{p^n}^*$ 中没有根, 并且这样的 u 的个数是 $\frac{(p^k-1)^2}{2}-1$。

证明 定义交换群: $G=\{x\in\mathrm{F}_{p^{2k}}^*\mid x^{p^k+1}=1\}$, G 上的乘法就是 $\mathrm{F}_{p^{2k}}^*$ 上的乘法。

当 $u=0$ 时, 命题显然成立, 下面考虑 $u\neq0$ 的情况, 根据引理3, 我们分成两部分讨论:

(1) 设 $u=\alpha\beta$, 其中 $\alpha\in\mathrm{F}_{p^k}^*$, $\beta\in G$。令 $y=x^{p^k-1}$ (显然 $y\in G$), 式(1)可以写为: $\alpha\beta+y+\alpha\beta^{-1}y^2=0$。用 βy 替换其中的 y, 就有 $\alpha\beta(1+\alpha^{-1}y+y^2)=0$。为方便, 将 $-\alpha^{-1}$ 记为 a, 进而考虑使得式

$$y^2-ay+1=0 \tag{2}$$

在 G 中没有解的 $a\in\mathrm{F}_{p^k}^*$ 的个数 N_k。

设 $t\in G$ 是式(2)的一个根, 那么另一个根就是 t^{-1}, 并且 $a=t+t^{-1}$。由于 $a\in\mathrm{F}_{p^k}^*$, 因此 t 满足 $(t+t^{-1})^{p^k-1}=1\Rightarrow t+t^{-1}\neq0\Rightarrow t^2\neq-1$。这样就可以定义映射 $h(t)=t+t^{-1}$, 从 $G\setminus\{t\mid t^2=-1\}$ 到 $\mathrm{F}_{p^k}^*$, 显然除了 $t=t^{-1}$ 之外, 它是一个2-1的映射, 因此

$$N_k=|\mathrm{F}_{p^k}^*|-\left(\frac{|G|-N(t\in G\mid t^2=-1)-N(t\in G\mid t^2=1)}{2}+N(t^2=1)\right)=\frac{p^k-5+N(t\in G\mid t^2=-1)}{2}$$

其中 $|\mathrm{F}_{p^k}^*|=p^k-1$, $|G|=p^k+1$, $N(t\in G\mid t^2=1)$ 表示 $t^2=1$ 在 $\mathrm{F}_{p^{2k}}$ 中根的个数, $N(t\in G\mid t^2=-1)$ 表示 $t^2=-1$ 在 G 中根的个数。

$N(t\in G\mid t^2=1)=2$ 是显然的, 下证 $N(t\in G\mid t^2=-1)=2$。事实上, 若 $t_0^2=-1$, 则 $(-t_0)^2=-1$ 也成立, 即 t_0 和 $-t_0$ 为相应的两个根。若 $t_0\in F_{p^k}^*$, 则在 G 中没有根; 若 $t_0\notin F_{p^k}^*$, 则 $(t_0)^{p^k-1}\neq 1\Rightarrow (t_0)^{p^k-1}=-1$, 即 $t_0\in G$, 从而 $N(t\in G\mid t^2=-1)=2-(1+\eta(-1))=1-\eta(-1)$, 其中 $\eta(\cdot)$ 是 F_{p^k} 上的二次特征。从而得到 $N_k=\dfrac{p^k-4-\eta(-1)}{2}$。

考虑到 $u=\alpha\beta$, 注意引理 3 后面的注记, 对于每一个 α 就存在 $\dfrac{p^k+1}{2}$ 个 β 对应不同的 u。可知使得式 (1) 没有根的形如 $\alpha\beta$ 的 u 共有 $\dfrac{p^k+1}{2}N_k$ 个。

(2) 设 $u=\alpha\beta\omega$, 其中 ω 是 $F_{p^{2k}}$ 中的本原元, $\alpha\in F_{p^k}^*$, $\beta\in G$。同样令 $y=x^{p^k-1}$ (显然 $y\in G$), 式 (1) 可以写为

$$\alpha\beta^{-1}\omega^{p^k}y^2+y+\alpha\beta\omega=0 \tag{3}$$

用 βy 替换 y, 就有 $\alpha\beta\omega^{p^k}(y^2+\omega^{-p^k}\alpha^{-1}y+\omega^{1-p^k})=0$。由于 α 和 β 非零, 于是只需考虑 $y^2+\omega^{-p^k}\alpha^{-1}y+\omega^{1-p^k}=0$, 进一步 $(y+\alpha^{-1}\omega^{-p^k}/2)^2=\omega^{1-p^k}(\alpha^{-2}\omega^{-1-p^k}/4-1)$。注意到 α、ω^{-1-p^k}、1 和 4 都属于 $F_{p^k}^*$, 因此 $\alpha^{-2}\omega^{-1-p^k}/4-1$ 在 $F_{p^{2k}}$ 中有平方根。设 θ 是这两个平方根中的一个, 那么 $\theta^2=\alpha^{-2}\omega^{-1-p^k}/4-1\in F_{p^k}$, 并且 $y=-\alpha^{-1}\omega^{-p^k}/2\pm\omega^{\frac{1-p^k}{2}}\theta$。计算如下等式:

$$\begin{aligned}y^{p^k+1}&=(-\alpha^{-1}\omega^{-p^{2k}}/2\pm\omega^{\frac{p^k-p^{2k}}{2}}\theta^{p^k})(-\alpha^{-1}\omega^{-p^k}/2\pm\omega^{\frac{1-p^k}{2}}\theta)\\&=\alpha^{-2}\omega^{1-p^k}/4\mp\alpha^{-1}\omega^{\frac{-p^k-p^{2k}}{2}}\theta^{p^k}/2\mp\alpha^{-1}\omega^{\frac{-1-p^k}{2}}\theta/2+\omega^{\frac{1-p^{2k}}{2}}\theta^{p^k+1}\end{aligned}$$

其中 $(\omega^{\frac{-p^k-p^{2k}}{2}})^2=\omega^{-p^k-p^{2k}}=\omega^{-1-p^k}=(\omega^{\frac{-1-p^k}{2}})^2$。

因此 $\omega^{\frac{-p^k-p^{2k}}{2}}$ 等于 $\omega^{\frac{-1-p^k}{2}}$ 或 $-\omega^{\frac{-1-p^k}{2}}$, 又因为 $\omega^{\frac{-1-p^k}{2}}=(\omega^{-1})^{\frac{1+p^k}{2}}\notin F_{p^k}$, 则

$$\omega^{\frac{-1-p^k}{2}}=(\omega^{-1})^{\frac{1+p^k}{2}}\neq((\omega^{-1})^{\frac{1+p^k}{2}})^{p^k}=\omega^{\frac{-p^k-p^{2k}}{2}}$$

即 $\omega^{\frac{-p^k-p^{2k}}{2}}=-\omega^{\frac{-1-p^k}{2}}$。注意到 $y\in G$, 于是

$$y^{p^k+1}=\alpha^{-2}\omega^{-1-p^k}/4\pm\alpha^{-1}\omega^{\frac{-1-p^k}{2}}\theta^{p^k}/2\mp\alpha^{-1}\omega^{\frac{-1-p^k}{2}}\theta/2-\theta^{p^k+1}=1$$

接下来, 将分三种情况分别进行讨论。由于 $\theta^2\in F_{p^k}$, 所以 θ 可能等于 0, $\theta^{p^k-1}=1$, 或 $\theta^{p^k-1}=-1$。

(1) 若 $\theta=0$, 那么 $y=-\alpha^{-1}\omega^{-p^k}/2$, $y^{p^k+1}=(-\alpha^{-1}\omega^{-p^k}/2)^{p^k+1}=\alpha^{-2}\omega^{-1-p^k}/4=1$, 所以 $\alpha=\pm\omega^{\frac{-p^k-1}{2}}/2$, 同时 $\alpha^{p^k-1}=\omega^{\frac{-(p^k+1)(p^k-1)}{2}}=-1$ 与 $\alpha\in F_{p^k}^*$ 矛盾, 所以不存在 $\alpha\in F_{p^k}^*$, 使得 $\theta=0$。

(2) 若 $\theta^{p^k-1}=1$, 即 $\theta^{p^k}=\theta$。那么 $y^{p^k+1}=\alpha^{-2}\omega^{-(p^k+1)}/4-\theta^2=1$, 这与 θ 的定义 $\theta^2=\alpha^{-2}\omega^{-1-p^k}/4-1$ 一致, 说明式 (3) 总有根。将 θ 的定义公式变形为

$$w^2+v^2=\omega^{-1-p^k} \tag{4}$$

其中 $w=2\theta\alpha$, $v=\alpha$。根据引理 1, 并考虑 θ 的正负号, 使得式 (4) 成立的解 α 的个数是 $N=(p^k-\eta(-1))/2$, 其中 $\eta(\cdot)$ 是 F_{p^k} 上的二次特征。

(3) 若 $\theta^{p^k-1}=-1$, 即 $\theta^{p^k}=-\theta$。那么就有 $y^{p^k+1}=\alpha^{-2}\omega^{-1-p^k}/4\mp\alpha^{-1}\omega^{-\frac{p^k+1}{2}}\theta+\theta^2$, 将 $\alpha^{-2}\omega^{-1-p^k}/4$ 替换为 θ^2+1, 就有 $y^{p^k+1}=2\theta^2\mp\alpha^{-1}\omega^{-\frac{p^k+1}{2}}\theta+1$, 若 $y^{p^k+1}=1$, 那么 $\theta^2=\alpha^{-2}\omega^{-1-p^k}/4$, 这与 $\theta^2=\alpha^{-2}\omega^{-1-p^k}/4-1$ 矛盾。注意到在 (2) 中, $N=(p^k-\eta(-1))/2$, 因此, 使得式 (1) 没有根的 α 的个数是 $p^k-1-N=(p^k-2+\eta(-1))/2$。

考虑表达式 $u=\alpha\beta\omega$, 可知对于每个 α, 存在 $(p^k+1)/2$ 个 β, 由引理 3, 可知使式 (1) 没有根的 $u=\alpha\beta\omega$

的总数共有$(p^k+1)N_k/2$个。综合前面(1)和(2)两部分讨论,并且加上$u=0$的情况,可知使式(1)没有根的u共有$(p^k+1)(p^k-3)/2+1=(p^k-1)^2/2-1$个。 □

参考文献:

[1] Dembowski P, Ostrom T G. Planes of Order n with Collineation Groups of Order n^2[J]. Math. Z., 1968, 193: 239-258.

[2] Hughes D R, Piper F C. Projective Planes[M]. Springer-verlag, New York, Graduate Texts in Mathematics, 1973, 6.

[3] Biham E, Shamir A. Differential Cryptanalysis of DES-like Cryptosystems[J]. Journal of Cryptology, 1991, 4: 3-72.

[4] Nyberg K. Perfect Nonlinear S-boxes[C]. Advances in Cryptology-EUROCRYPT'91, LNCS 547, Springer-verlag, 1992: 378-386.

[5] Nyberg K. Differentially Uniform Mappings for Cryptography[C]. Advances in Cryptology-EUROCRYPT'93, LNCS 765, Springer-verlag, 1994: 55-64.

[6] Coulter R S, Matthews R W. Planar Functions and Planes of Lenz-barlotti Class Ⅱ[J]. Design, Coding and Cryptography, 1997, 10: 167-184.

[7] Carlet A, Charpin P, Zinoviev V. Codes, Bent Functions and Permutations Suitable for DESlike Cryptosystems[J]. Designs, Codes and Cryptography, 1998, 15(2): 125-156.

[8] Ding C, Yuan J. A Family of Skew Hadamard Difference sets[J]. Comb. Theory, Series A, 2006, 113: 1526-1535.

[9] Zha Z, Kyureghyan G M, Wang X. Perfect Nonlinear Binomials and Their Semifields[J]. Finite Fields and Their Applications, 2009, 15: 125-133.

[10] Budaghyan L, Helleseth T. New Perfect Nolinear Multinomials over $F_{p^{2k}}$ for Any Odd Prime p[C]. SETA 2008, LNCS 5203, 2008, 403-414.

[11] Coulter R S, Henderson M. Commutative Presemifields and Semifields[C]. Advances in Mathematics, 2008, 217: 282-304.

[12] Kyureghyan G M, Pott A. Some Theorems on Planar Mappings[C]. WAIFI 2008, LNCS 5130, 2008, 117-122.

[13] Helleseth T, Kyureghyan G, Ness G J, et al. On a Family of Perfect Nonlinear Binomials[J]. Boolean Functions in Cryptology and Information Security, B. Preenel and O. A. Logacher(Eds.) IOS Press 2008, 126-139.

[14] Budaghyan L, Carlet C, Leander G. On Inequivalence Between Known Power APN Functions[C]// Proceedings of the conference BFCA 2008, Copenhagen.

[15] Lidl R, Niederreiter H. Finite Fields[M]. Encyclopedia of Mathematics and Its Application, US: Addison-wesley, 1983.

(上接第143页)

6 结论

传统的积分攻击对于基于比特设计的密码不再有效,采用基于比特的分析方法能够取得较好的效果。本文从比特的层面寻找平衡性,分析了PUFFIN密码抵抗积分攻击的能力,给出了一个5轮积分区分器并利用高阶积分的思想将其扩展为6轮,在PC机上验证了PUFFIN区分器的存在性。利用6轮区分器,对8轮的PUFFIN进行了攻击。对于PUFFIN类的分组密码,通过统计活跃模式不同值重复的次数,证明了其至少存在3轮积分区分器,证明的过程同时也提供了寻找这类密码积分区分器的方法。

参考文献:

[1] Wheeler D, Needham R. TEA, a Tiny Encryption Algorithm[C]// FSE 1995, LNCS 1008: 363-366.

[2] Lim C, Korkishko T. mCrypto —A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors[C]// WISA 2005, LNCS, 2005, 3786: 243-258.

[3] Standaert F, Piret G, Gershenfeld N, et al. SEA: A Scalable Encryption Algorithm for Small Embedded Applications[C]// CARDIS 2006, LNCS, 2006, 3928: 222-236.

[4] Robshaw M. Searching for Compact Algorithms: CGEN[C]// VIETCRYPT 2006, LNCS, 2006, 4341: 37-49.

[5] Hong D, Sung J, Hong S, et al. HIGHT: A New Block Cipher Suitable for Low-resource Device[C]// CHES 2006, LNCS, 2006, 4249: 46-59.

[6] Cheng H, Heys H, Wang C. PUFFIN: A Novel Compact Block Cipher Targeted to Embedded Digital Systems[C]// 11th Euromicro Conference on Digital System Design: Architectures, Methods and Tools. DSD, 2008: 383-390.

[7] Knudsen L, Wagner D. Integral Cryptanalysis[C]// FSE 2002, LNCS, 2002, 2365: 112-127.

[8] Galice S, Minier M. Improving Integral Attacks Against Rijndael-256 Up to 9 Rounds[C]// AFRICACRYPT 2008, LNCS, 2008, 5023: 1-15.

[9] Duo L, Li C, Feng K Q. New Observation on Camellia[C]// SAC 2005, LNCS, 2005, 3897: 51-64.

[10] 王薇,王小云. 对CLEFIA算法的饱和度分析[J]. 通信学报, 2008(10): 88-92.

[11] Zaba M R, Raddum H, Henricksen M, et al. Bit-pattern Based Integral Attack[C]// FSE 2008, LNCS, 2008, 5086: 363-381.