模 2 加整体逼近二元和三元模 2^n 加的噪声函数分析

陈士伟　　金晨辉
(信息工程大学电子技术学院　郑州　450004)

摘　要：整体逼近就是用一个弱密码函数替代一个强密码函数的攻击方法，这两个函数的模 2 和称为该整体逼近的噪声函数。该文研究了模 2 加整体逼近二元模 2^n 加和三元模 2^n 加时噪声函数的概率分布，给出了噪声函数的概率分布的计算公式以及噪声函数的概率值的平方和的计算公式。这些结果有助于掌握二元模 2^n 加和三元模 2^n 加对抗模 2 加的整体逼近攻击的能力。

关键词：模 2^n 加；噪声函数；线性逼近；区分攻击；概率分布；整体逼近
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-5896(2008)06-1445-05

Analysis of the Noise Functions of Macrocosm Approximation of Binary Addition and Triple Addition Modulo 2^n with XOR

Chen Shi-wei　　Jin Chen-hui
(*Institute of Electronic Technology, the University of Information Engineering, Zhengzhou* 450004, *China*)

Abstract: Macrocosm approximation is a class of attacks to ciphers by replacing a strong cipher function with a weak cipher function. The XOR of the two functions is called the noise function of this macrocosm approximation. This paper studies the probability distributions of the noise functions produced by macrocosm approximation of binary addition and triple addition modulo 2^n with XOR, and gives the computation formulae of the probability distributions of the corresponding noise functions and the square sums of the probabilities, which is helpful to recognize the ability of resistance to macrocosm approximation of binary addition and triple addition modulo 2^n with XOR.

Key words: Addition modulo 2^n ; Noise function; Linear approximation; Distinguishing attack; Probability distribution; Macrocosm approximation

1　引言

模 2^n 加运算是密码算法中常用的一个基本密码变换，它相对于逐位模 2 加运算是非线性变换。在对密码算法进行安全性分析时，常常需要对该变换进行线性逼近。对该变换的线性逼近主要有两类，第 1 类是单比特逼近方法，即考查该变换输出比特的线性组合与输入比特的线性组合接近的程度，它可用多输出布尔函数的 Walsh 循环谱刻画。单比特逼近主要用于分析密码算法的抗线性密码攻击[1]的能力。文献[2]给出了模 2^n 加运算的 Walsh 循环谱的计算公式，从而圆满解决了该变换的 Walsh 循环谱分析问题。

第 2 类是直接考查该变换与逐位模 2 加接近的程度，它可用二者的相容程度[3]刻画，也可用整体逼近的方法刻画，即用这两个函数的模 2 和函数(即噪声函数)取值分布的不平衡程度刻画。整体逼近主要用于对序列密码的区分攻击等，由于利用了更多的信息，因而攻击效果比单比特逼近更好。例如，文献[4]利用 PY 算法[5]的信息泄漏和模 2^n 加运算最低位的线性性，提出了对 PY 算法的区分攻击，文献[6]则利用逐位模 2 加运算对模 2^n 加运算进行整体逼近，从而改进了对 PY 算法的区分攻击，使区分攻击的数据复杂性降低至原来的 60552 分之一。文献[7]利用整体逼近方法，改进了文献[8]对 SNOW 2.0 算法[9]的区分攻击，使得区分攻击的数据复杂性降低至原来的 2^{23} 分之一。文献[10]利用整体逼近的思想，提出了对 Dragon 算法的区分攻击。在上述攻击中，主要利用了相应的噪声函数 $f(x)$ 的取值的不均匀性所产生的信息泄漏，区分攻击的数据复杂性主要由噪声函数 $f(x)$ 的取值概率的平方和 $\sum_a [p(f(x)=a)]^2$ 决定[6, 11, 12]。因此，研究整体逼近对于密码分析具有应用价值。

由于区分攻击的数据复杂性主要由噪声函数 $f(x)$ 的取值概率的平方和 $\sum_a [p(f(x)=a)]^2$ 决定，所以噪声函数的取值概率的平方和的确定有助于对区分攻击的数据复杂性作出估计。文献[3]分析了模 2^n 加运算与逐位模 2 加运算的相容程度，文献[4]给出了模 2^n 加，模 2 加及逻辑运算的混合变换的取值分布的一个多项式时间的计算算法，文献[6]给出了攻

2006-11-21 收到，2007-04-27 改回
河南省杰出青年科学基金(0312001800)资助课题

击 PY 算法时所需的噪声函数取值概率的平方和的一个多项式时间的计算算法。本文将通过对逐位模 2 加整体逼近模 2^n 加后产生的噪声函数

$$f(x_1,\cdots,x_m)=[(x_1+\cdots+x_m)\bmod 2^n]\oplus(x_1\oplus\cdots\oplus x_m) \quad (1)$$

的取值的分布规律的研究，解决用逐位模 2 加整体逼近模 2^n 加运算的效果问题。本文仅针对二元和三元的情形，研究相应的噪声函数的取值分布规律和噪声函数的取值概率的平方和，给出概率函数的计算公式和取值概率的平方和的计算公式。这些结果对于分析密码算法的抗区分攻击等攻击方法的能力，具有实际应用价值。

2 二元模 2 加整体逼近二元模 2^n 时噪声函数的概率分布

定义 1 设 $x,y\in Z/(2^n)$，则称

$$\xi_n(x,y)=[(x+y)\bmod 2^n]\oplus(x\oplus y) \quad (2)$$

为二元模 2 加整体逼近二元模 2^n 时的噪声函数。

下面给出 $\xi_n(x,y)$ 的概率分布

$$p(\xi_n=a)=\frac{1}{2^{2n}}\#\{(x,y)\in[Z/(2^n)]^2:\xi_n(x,y)=a\} \quad (3)$$

的计算公式。以下涉及 $\xi_n(x,y)$ 时，其含义均与定义 1 相同，不再具体指出。

对 $\forall x\in Z/(2^n)$，记 $x=\sum_{i=1}^{n}x_i2^{i-1}$ 且 $x_i\in\{0,1\}$，则 x 与 $(x_n,x_{n-1},\cdots,x_1)$ 一一对应。因此，本文对 $Z/(2^n)$ 中点 x 与 $(x_n,x_{n-1},\cdots,x_1)$ 不加区分，并记为 $x=(x_n,x_{n-1},\cdots,x_1)$。

由实数和的二进制表示可得引理 1。

引理 1[13] 设 $x,y,z\in Z/(2^n)$，则 $(x+y)\bmod 2^n=z$ 的充要条件是 $\forall k:0\le k\le n-1$，均有 $z_k=x_k\oplus y_k\oplus e_k$。其中 $e_0=0$ 且 $\forall k:1\le k\le n-1$，有

$$e_k=x_ky_k\oplus(x_k\oplus y_k)e_{k-1} \quad (4)$$

记 $\Omega_a^{(n)}=\{(x,y)\in[Z/(2^n)]^2:(x\hat{+}y)\oplus(x\oplus y)=a\}$，则有定理 1。

定理 1 设 $x,y,a\in Z/(2^n)$，则 $x,y\in\Omega_a^{(n)}$ 的充要条件为 $\forall k:0\le k\le n-1$，均有 $e_k=a_{k+1}$。其中 $e_0=0$ 且 $\forall k:1\le k\le n-1$，有

$$e_k=x_ky_k\oplus(x_k\oplus y_k)e_{k-1} \quad (5)$$

证明 由引理 1 即知。

定理 2 $p(\xi_n=a)=3^{\lambda(a)}\times(a_1\oplus1)/4^{n-1}$，其中 $\lambda(a)=\#\{k:1\le k\le n-1,a_k=a_{k+1}\}$。

证明 由定理 1 知，$x,y\in\Omega_a^{(n)}$ 蕴涵 $a_1=e_0=0$，故当 $a_1=1$ 时，有 $P(f=a)=0$。由定理 1 还知，$x,y\in\Omega_a^{(n)}$ 的充分必要条件是 $\forall k:1\le k\le n-1$，均有 $e_k=a_{k+1}$，即 (x_k,y_k) 满足

$$a_{k+1}=x_ky_k\oplus(x_k\oplus y_k)a_k \quad (6)$$

(1)若 $a_{k+1}=a_k$，则式(6)等价于 $x_ky_k\oplus(x_k\oplus y_k\oplus1)a_k=0$，即 $(x_k\oplus a_k)(y_k\oplus a_k)=0$，故式(6)等价于 $(x_k,y_k)\ne(a_k\oplus1,a_k\oplus1)$，即满足式(6)的 (x_k,y_k) 共有 $3^{a_k\oplus a_{k+1}\oplus1}$ 个; (2)若 $a_{k+1}=a_k\oplus1$，则式(6)等价于 $x_ky_k\oplus(x_k\oplus y_k\oplus1)a_k=1$，即 $(x_k\oplus a_k)(y_k\oplus a_k)=1$，故式(6)等价于 $(x_k,y_k)=(a_k\oplus1,a_k\oplus1)$，即满足式(6)的 (x_k,y_k) 共有 $3^{a_k\oplus a_{k+1}\oplus1}$ 个，从而由定理 1 即知

$$\begin{aligned}|N_a^{(n)}|&=(a_1\oplus1)\times\#\{(x,y):a_{k+1}\\&=x_ky_k\oplus(x_k\oplus y_k)a_k,1\le k\le n-1\}=(a_1\oplus1)\times4\\&\quad\times\prod_{k=1}^{n-1}\#\{(x_k,y_k):a_{k+1}=x_ky_k\oplus(x_k\oplus y_k)a_k\}\\&=4(a_1\oplus1)\times\prod_{k=1}^{n-1}3^{a_{k+1}\oplus a_k\oplus1}=4\times3^{\lambda(a)}\times(a_1\oplus1)\end{aligned} \quad (7)$$

这说明 $p(\xi_n=a)=|N_a^{(n)}|/4^n=3^{\lambda(a)}\times(a_1\oplus1)/4^{n-1}$。证毕

3 三元模 2 加整体逼近三元模 2^n 时噪声函数的概率分布

定义 2 设 $x,y,z\in Z/(2^n)$，则称

$$\eta_n(x,y,z)=[(x+y+z)\bmod 2^n]\oplus(x\oplus y\oplus z) \quad (8)$$

为三元模 2 加整体逼近三元模 2^n 时的噪声函数。

以下涉及 $\eta_n(x,y,z)$ 时，其含义均与定义 2 相同，不再具体指出。对 $a\in Z/(2^n)$，记 $a^{(k)}=a\bmod 2^k$ 及

$$\Lambda_a^{(n)}=\{(x,y,z)\in[Z/(2^n)]^3:\eta_n(x,y,z)=a\} \quad (9)$$

定义 3 设 $x,y,z\in Z/(2^n)$。令 $d_0=0$，且 $\forall k:1\le k\le n-1$，记 d_k 是使得

$$x^{(k)}+y^{(k)}+z^{(k)}=d_k2^k+(x+y+z)\bmod 2^k \quad (10)$$

的非负整数，则称 d_k 为第 k 位向高位的进位。显然，$d_k\in\{0,1,2\}$。

定理 3 设 $x,y,z,a\in Z/(2^n)$，则

(1)对任意 $k\ge0$，有 $d_{k+1}=\mathrm{int}((x_{k+1}+y_{k+1}+z_{k+1}+d_k)/2)$，其中 int 为下取整函数。

(2) $x,y,z\in\Lambda_a^{(n)}$ 的充分必要条件是 $\forall k:1\le k\le n$，均有 $d_{k-1}\bmod2=a_k$。

证明 设 $x,y,z\in Z/(2^n)$，则 $\forall k:1\le k\le n$，有

$$\begin{aligned}&d_{k+1}2^{k+1}+(x+y+z)\bmod2^{k+1}=x^{(k+1)}+y^{(k+1)}+z^{(k+1)}\\&=x^{(k)}+y^{(k)}+z^{(k)}+(x_{k+1}\oplus y_{k+1}\oplus z_{k+1})2^k\\&=(x_{k+1}+y_{k+1}+z_{k+1}+d_k)2^k+(x+y+z)\bmod2^k\\&=[\mathrm{int}((x_{k+1}+y_{k+1}+z_{k+1}+d_k)/2)]2^{k+1}+(x_{k+1}\oplus y_{k+1}\\&\quad\oplus z_{k+1}\oplus d_k\bmod2)2^k+(x+y+z)\bmod2^k\end{aligned} \quad (11)$$

这说明 $d_{k+1}=\mathrm{int}((x_{k+1}+y_{k+1}+z_{k+1}+d_k)/2)$，进而有

$$\begin{aligned}(x+y+z)\bmod2^{k+1}&=(x_{k+1}\oplus y_{k+1}\oplus z_{k+1}\oplus d_k\bmod2)2^k\\&\quad+(x+y+z)\bmod2^k\end{aligned} \quad (12)$$

故当 $x,y,z\in\Lambda_a^{(n)}$ 时，有 $[(x+y+z)\oplus(x\oplus y\oplus z)]\bmod2^{k+1}=a^{(k+1)}$，进而有 $a_k=d_{k-1}\bmod2$。

反之，若 $\forall k:1\le k\le n$，均有 $d_{k-1}\bmod2=a_k$，则由归纳法和式(12)易证 $x,y,z\in\Lambda_a^{(n)}$。证毕

定理 4 设 $a\in Z/(2^n)$，则有 $p(\eta_n=a)=(a_1\oplus1)2^{\lambda_0(a)-2n+2}\cdot3^{\lambda_{11}(a)}$，其中

$$\lambda_0(a)=\#\{k:a_k=0,1\le k\le n-1\},$$
$$\lambda_{11}(a)=\#\{k:a_k=a_{k+1}=1,1\le k\le n-1\}\quad(13)$$

证明　由定理 3 知 $x,y,z\in A_a^{(n)}$ 等价于 $a_1=d_0 \bmod 2=0$ 且 $\forall k:2\le k\le n$，均有

$$a_k=d_{k-1}\bmod 2=\begin{cases}0, & x_{k-1}+y_{k-1}+z_{k-1}+d_{k-2}\ne 2,3\\ 1, & x_{k-1}+y_{k-1}+z_{k-1}+d_{k-2}=2,3\end{cases}\quad(14)$$

现根据 (a_k,a_{k-1}) 的取值分 4 种情形讨论:

(1) $(a_k,a_{k-1})=(0,0)$。则 $d_{k-2}\in\{0,2\}$ 且式 (14) 等价于 $x_{k-1}+y_{k-1}+z_{k-1}+d_{k-2}\ne 2,3$。

若 $d_{k-2}=0$，则 $(x_{k-1},y_{k-1},z_{k-1})$ 共有 $(0,0,0),(0,0,1),(0,1,0),(1,0,0)$ 这 4 个可能取值; 若 $d_{k-2}=2$，则 $(x_{k-1},y_{k-1},z_{k-1})$ 共有 $(1,1,1),(1,1,0),(1,0,1),(0,1,1)$ 这 4 个可能取值。故此时 $(x_{k-1},y_{k-1},z_{k-1})$ 总有 $4=2\times 2^{a_{k-1}\oplus 1}\times 3^{a_{k-1}=a_k=1}$ 个可能取值。这里，当 $a_{k-1}=a_k=1$ 时规定 $3^{a_{k-1}=a_k=1}=3$，否则规定 $3^{a_{k-1}=a_k=1}=1$。下同。

(2) $(a_k,a_{k-1})=(1,0)$。则 $d_{k-2}\in\{0,2\}$ 且式 (14) 等价于 $x_{k-1}+y_{k-1}+z_{k-1}+d_{k-2}=2,3$。

若 $d_{k-2}=0$，则 $(x_{k-1},y_{k-1},z_{k-1})$ 共有 $(1,1,1),(1,1,0),(1,0,1),(0,1,1)$ 这 4 个可能取值; 若 $d_{k-2}=2$，则 $(x_{k-1},y_{k-1},z_{k-1})$ 共有 $(0,0,0),(0,0,1),(0,1,0),(1,0,0)$ 这 4 个可能取值。故此时 $(x_{k-1},y_{k-1},z_{k-1})$ 总有 $4=2\times 2^{a_{k-1}\oplus 1}\times 3^{a_{k-1}=a_k=1}$ 个可能取值。

(3) $(a_k,a_{k-1})=(0,1)$。则 $d_{k-2}=1$ 且式 (14) 等价于 $x_{k-1}+y_{k-1}+z_{k-1}\ne 1,2$，故 $(x_{k-1},y_{k-1},z_{k-1})$ 共有 $(0,0,0),(1,1,1)$ 这 $2=2\times 2^{a_{k-1}\oplus 1}\times 3^{a_{k-1}=a_k=1}$ 个可能取值。

(4) $(a_k,a_{k-1})=(1,1)$。则 $d_{k-2}=1$ 且式 (14) 等价于 $x_{k-1}+y_{k-1}+z_{k-1}=1,2$，故 $(x_{k-1},y_{k-1},z_{k-1})$ 共有 $(0,0,1),(0,1,0),(1,0,0),(1,1,0),(1,0,1),(0,1,1)$ 这 $6=2\times 2^{a_{k-1}\oplus 1}\times 3^{a_{k-1}=a_k=1}$ 个可能取值。

这说明

$$\begin{aligned}|A_a^{(n)}|&=\#\{(x,y,z):\forall k:1\le k\le n,\text{有}\,a_k=d_{k-1}\bmod 2\}\\&=8(a_1\oplus 1)\prod_{k=1}^{n-1}\#\{(x_k,y_k,z_k):a_{k+1}=d_k\bmod 2\}\\&=8(a_1\oplus 1)\prod_{k=1}^{n-1}(2\times 2^{a_k\oplus 1}\times 3^{a_k=a_{k+1}=1})=(a_1\oplus 1)2^{\lambda_0(a)+n+2}3^{\lambda_{11}(a)}\end{aligned}\quad(15)$$

因而 $p(\eta_n=a)=|A_a^{(n)}|/2^{3n}=(a_1\oplus 1)2^{\lambda_0(a)-2n+2}3^{\lambda_{11}(a)}$。证毕

4　二元模 2 加整体逼近二元模 2^n 时噪声函数取值概率的平方和

定理 5　$\sum_{a\in\{0,1\}^n}[P(\xi_n=a)]^2=\left(\frac{5}{8}\right)^{n-1}$。

证明　记 $s(n)=\sum_{a\in\{0,1\}^n}[P(\xi_n=a)]^2$，且 $\forall a\in Z/(2^n)$，记 $a=a_L+2^m a_H$，这里 $0\le a_L<2^m$。记

$$L_i=\{x\in Z/(2^m):x_m=i\},$$
$$H_i=\{x\in Z/(2^{n-m}):x_1=i\}\quad(16)$$

则由 $\lambda(b)=\lambda(b\oplus 11\cdots 1)$ 知

$$\begin{aligned}s(n-m)&=\frac{1}{16^{n-m-1}}\sum_{b\in\{0,1\}^{n-m}}(b_1\oplus 1)9^{\lambda(b)}=\frac{1}{16^{n-m-1}}\sum_{b\in H_0}9^{\lambda(b)}\\&=\frac{1}{16^{n-m-1}}\sum_{b\oplus 1\cdots 1\in H_1}9^{\lambda(b)}=\frac{1}{16^{n-m-1}}\sum_{b\in H_1}9^{\lambda(b\oplus 1\cdots 1)}\\&=\frac{1}{16^{n-m-1}}\sum_{b\in H_1}9^{\lambda(b)}\end{aligned}\quad(17)$$

从而由

$$\lambda(a)=\begin{cases}\lambda(a_H)+\lambda(a_L), & (a_H,a_L)\in(H_1\times L_0)\bigcup(H_0\times L_1)\\ \lambda(a_H)+\lambda(a_L)+1, & (a_H,a_L)\in(H_0\times L_0)\bigcup(H_1\times L_1)\end{cases}\quad(18)$$

知对 $\forall m\ge 1$，有

$$\begin{aligned}s(n)&=\frac{1}{16^{n-1}}\sum_{a\in Z/(2^n)}(a_1\oplus 1)9^{\lambda(a)}\\&=\frac{1}{16^{n-1}}\sum_{a_H\in\{0,1\}^{n-m}}\sum_{a_L\in\{0,1\}^m}(a_1\oplus 1)9^{\lambda(a)}\\&=\frac{1}{16^{n-1}}\Bigg\{\sum_{a_H\in H_1}\sum_{a_L\in L_0}(a_1\oplus 1)9^{\lambda(a_H)+\lambda(a_L)}\\&\quad+\sum_{a_H\in H_0}\sum_{a_L\in L_1}(a_1\oplus 1)9^{\lambda(a_H)+\lambda(a_L)}\\&\quad+\sum_{a_H\in H_0}\sum_{a_L\in L_0}(a_1\oplus 1)9^{\lambda(a_H)+\lambda(a_L)+1}\\&\quad+\sum_{a_H\in H_1}\sum_{a_L\in L_1}(a_1\oplus 1)9^{\lambda(a_H)+\lambda(a_L)+1}\Bigg\}\\&=\frac{1}{16^{n-1}}\left[\sum_{a_H\in H_0}9^{\lambda(a_H)}\right]\left[\sum_{a_L\in L_0}(a_1\oplus 1)9^{\lambda(a_L)}+\sum_{a_L\in L_1}(a_1\oplus 1)9^{\lambda(a_L)}\right]+\frac{9}{16^{n-1}}\left[\sum_{a_H\in H_0}9^{\lambda(a_H)}\right]\\&\quad\cdot\left[\sum_{a_L\in L_0}(a_1\oplus 1)9^{\lambda(a_L)}+\sum_{a_L\in L_1}(a_1\oplus 1)9^{\lambda(a_L)}\right]\\&=\frac{10}{16^{n-1}}\left[\sum_{a_H\in H_0}9^{\lambda(a_H)}\right]\left[\sum_{a_L\in\{0,1\}^m}(a_1\oplus 1)9^{\lambda(a_L)}\right]\\&=\frac{5}{8}\times\frac{1}{16^{(n-m)-1}}\times\left[\sum_{a_H\in H_0}9^{\lambda(a_H)}\right]\\&\quad\cdot\left[\frac{1}{16^{m-1}}\times\sum_{a_L\in\{0,1\}^m}(a_1\oplus 1)9^{\lambda(a_L)}\right]=\frac{5}{8}\times s(n-m)\times s(m)\end{aligned}\quad(19)$$

由于 $s(1)=\frac{1}{16^0}\times 9^0=1$，从而有

$$s(n)=\frac{5}{8}s(n-1)=\left(\frac{5}{8}\right)^2 s(n-2)=\cdots=\left(\frac{5}{8}\right)^{n-1}s(1)=\left(\frac{5}{8}\right)^{n-1}\quad(20)$$

证毕

5　三元模 2 加整体逼近三元模 2^n 时噪声函数取值概率的平方和

引理 2　设 $f(n)=\sum_{a\in\{0,1\}^n}(a_1\oplus 1)4^{\lambda_0(a)-2n+2}9^{\lambda_{11}(a)}$，$g_i(n)=\sum_{a\in\{0,1\}^n}(a_1\oplus i)4^{\lambda_0(a)}9^{\lambda_{11}(a)}$，则有 $g_1(n)=16^{n-1}f(n)$ 且

$$g_0(n)=\frac{9^{n-1}}{16}\sum_{k=2}^{n-1}\left(\frac{4}{3}\right)^{2k}f(k)+13\times 9^{n-2} \tag{21}$$

证明 显然 $g_1(n)=16^{n-1}f(n)$ 成立。记 $M_i=\{x\in Z/(2^{n-1}):x_1=i\}$，则由 $\lambda_{11}(2b+1)=\lambda_{11}(b)+1$ 和 $\lambda_0(2b+1)=\lambda_0(b)$ 知

$$\begin{aligned}g_0(n)&=\sum_{a\in\{0,1\}^n}a_1\times 4^{\lambda_0(a)}9^{\lambda_{11}(a)}=\sum_{b\in M_0}4^{\lambda_0(2b+1)}9^{\lambda_{11}(2b+1)}\\&\quad+\sum_{b\in M_1}4^{\lambda_0(2b+1)}9^{\lambda_{11}(2b+1)}=\sum_{b\in M_0}4^{\lambda_0(b)}9^{\lambda_{11}(b)}\\&\quad+\sum_{b\in M_1}4^{\lambda_0(b)}9^{\lambda_{11}(b)+1}=g_1(n-1)+9g_0(n-1)\end{aligned} \tag{22}$$

即当 $k=1$ 时，$g_0(n)=\sum_{i=1}^{k}9^{i-1}g_1(n-i)+9^k g_0(n-k)$ 成立。利用归纳法易证该式对 $k\le n-2$ 均成立。特别地，由 $g_0(2)=13$ 知

$$\begin{aligned}g_0(n)&=\sum_{i=1}^{n-2}9^{i-1}g_1(n-i)+9^{n-2}g_0(2)\\&=\sum_{i=1}^{n-2}9^{i-1}16^{n-i-1}f(n-i)+13\times 9^{n-2}\\&=\frac{9^{n-1}}{16}\sum_{k=2}^{n-1}\left(\frac{4}{3}\right)^{2k}f(k)+13\times 9^{n-2}\end{aligned} \tag{23}$$

证毕

下面解决 $f(k)$ 的计算问题。

引理 3 设 $f(n)=\frac{1}{16^{n-1}}\sum_{a\in\{0,1\}^n}(a_1\oplus 1)4^{\lambda_0(a)}9^{\lambda_{11}(a)}$，定义 $\alpha_1=1,\beta_1=1/4$，且 $\forall i\ge 2$，定义

$$\left.\begin{aligned}\alpha_i&=\alpha_{i-1}+\beta_{i-1}\left(\frac{4}{3}\right)^{2(i-1)}\\\beta_i&=\frac{1}{4}\beta_{i-1}+\alpha_{i-1}\frac{4}{81}\left(\frac{3}{4}\right)^{2i}\end{aligned}\right\} \tag{24}$$

则对任意的正整数 i，均有

$$f(n)=\alpha_i\frac{4}{81}\left(\frac{3}{4}\right)^{2n}\sum_{k=2}^{n-i-1}\left(\frac{4}{3}\right)^{2k}f(k)+\beta_i f(n-i)+\alpha_i\frac{52}{81}\left(\frac{3}{4}\right)^{2(n-1)} \tag{25}$$

证明 略。

引理 4 题设同引理 3，则对于任意的正整数 i，均有

$$\left.\begin{aligned}\alpha_i&=\frac{9}{\sqrt{41}}\times\frac{1}{18^i}[(13+\sqrt{41})^i-(13-\sqrt{41})^i]\\\beta_i&=\left(\frac{3}{4}\right)^{2i}\times\frac{9}{\sqrt{41}}\times\frac{1}{18^{i+1}}[(13+\sqrt{41})^i(\sqrt{41}-5)\\&\quad+(13-\sqrt{41})^i(\sqrt{41}+5)]\end{aligned}\right\} \tag{26}$$

证明 略。

定理 6 当 $n\ge 3$ 时，均有

$$\begin{aligned}\sum_{a\in\{0,1\}^n}[P(\eta_n=a)]^2&=\frac{2^{8-5n}}{\sqrt{41}}[(33\sqrt{41}+109)(13+\sqrt{41})^{n-3}\\&\quad+(33\sqrt{41}-109)(13-\sqrt{41})^{n-3}]\end{aligned} \tag{27}$$

证明 由于 $\sum_{a\in\{0,1\}^n}[P(\eta_n=a)]^2=\frac{1}{16^{n-1}}\sum_{a\in\{0,1\}^n}(a_1\oplus 1)\cdot 4^{\lambda_0(a)}9^{\lambda_{11}(a)}=f(n)$，故由引理 2 得

$$\begin{aligned}f(n)&=\alpha_{n-3}\frac{4}{81}\left(\frac{3}{4}\right)^{2n}\sum_{k=2}^{n-(n-3)-1}\left(\frac{4}{3}\right)^{2k}f(k)+\beta_{n-3}f(n-(n-3))\\&\quad+\alpha_{n-3}\frac{52}{81}\left(\frac{3}{4}\right)^{2(n-1)}\\&=\alpha_{n-3}\frac{4}{81}\left(\frac{3}{4}\right)^{2n}\left(\frac{4}{3}\right)^{4}f(2)+\beta_{n-3}f(3)+\alpha_{n-3}\frac{52}{81}\left(\frac{3}{4}\right)^{2(n-1)}\end{aligned} \tag{28}$$

再由 $f(2)=\frac{5}{4},f(3)=\frac{33}{64}$ 可得 $f(n)=\frac{8768}{6561}\left(\frac{3}{4}\right)^{2n}\alpha_{n-3}+\frac{33}{64}\cdot\beta_{n-3}$，即

$$\begin{aligned}f(n)&=\frac{2^{8-5n}}{\sqrt{41}}[(33\sqrt{41}+109)(13+\sqrt{41})^{n-3}\\&\quad+(33\sqrt{41}-109)(13-\sqrt{41})^{n-3}]\end{aligned} \tag{29}$$

利用上述结果，我们可对常用的 n，分别计算出 $\sum_{a\in\{0,1\}^n}[P(\xi_n=a)]^2$ 和 $\sum_{a\in\{0,1\}^n}[P(\eta_n=a)]^2$ 的值如表 1。

表 1 二元和三元情形噪声函数的平方和的比较

n	2	4	8	16	32
$\sum_{a\in\{0,1\}^n}[P(\xi_n=a)]^2$	1.25×2^{-1}	1.953128×2^{-3}	1.192093×2^{-5}	1.776357×2^{-11}	1.972153×2^{-22}
$\sum_{a\in\{0,1\}^n}[P(\eta_n=a)]^2$		1.050780×2^{-2}	1.026474×2^{-5}	1.917760×2^{-15}	1.639000×2^{-23}

6 结束语

本文研究了模 2 加整体逼近二元和三元模 2^n 加时噪声函数的概率分布，给出了噪声函数的概率分布的计算公式及噪声函数的概率值的平方和的计算公式，从而解决了用逐位模 2 加整体逼近模 2^n 加运算的效果分析问题。这些结果对于分析密码算法的抗区分攻击等攻击方法的能力，具有实际应用价值。

参 考 文 献

[1] Matsui M. Linear cryptanalysis method for DES cipher. In Advances in Cryptology-Eurocrypt 1993, LNCS 3788: 386-397.

[2] Wallen J. Linear approximations of addition modulo 2^n. In

Fast Software Encryption 2003, LNCS 2887: 261–273.

[3] 郭建胜，金晨辉. 逐位模 2 加运算与模 2^n 加运算的相容程度分析. 高校应用数学学报, 2003, 18(2): 247–250.
Guo J S and Jin C H. Consistent degree analysis of bit-wise exclusive-OR and addition module 2^n. *Application Mathematics A Journal of Chinese Universities*, 2003, 18(2): 247–250.

[4] Sekar G, Paul S, and Preneel B. Distinguishing attacks on the stream cipher Py. ESTREAM, ECRYT Stream Cipher Project, report 2005/081, 2005.

[5] Biham E and Seberry J. Py(Roo): A fast and secure stream cipher using rolling arrays. ESTREAM, ECRYT Stream Cipher Project, report 2005/023, 2005.

[6] Crowley P. Improved cryptanalysis of PY. ESTREAM, ECRYT Stream Cipher Project, report 2006/010, 2006.

[7] Maximov A and Johansson T. Fast computation of large distributions and its cryptographic applications. In Advances in Cryptology -Asiacrypt 2005, LNCS 3788: 313–332.

[8] Watanabe D, Biryukov A, and De Canniere C. A distinguishing attack of SNOW 2.0 with linear masking method. In Selected Areas in Cryptography ——SAC 2003, Springer-Verlag, 2003: 222–233.

[9] Ekdahl P and Johansson T. A new version of the stream cipher Snow. In Selected Areas in Cryptography——SAC 2002, LNCS 2595: 47–61.

[10] Englund H and Maximov A. Attack the Dragon. http://crypto/streamciphers/dragon-256/062. pdf, 2005.

[11] Junod P. On the optimality of linear, differential, and sequential distinguishers. In Advances in Cryptology-Eurocrypt 2003, LNCS 2656: 17–32.

[12] Baigneres T, Junod P, and Vandenay S. How far can we go beyond linear cryptanalysis? In Advances in Cryptology -Asiacrypt 2004, LNCS 3329: 432–450.

[13] Rueppel R A. Analysis and design of stream ciphers. Berlin: Springer-Verlag, 1986: 182–187.

陈士伟：　女，1983 年生，硕士生，研究方向为密码学.

金晨辉：　男，1965 年生，教授，博士生导师，主要研究方向为密码学与信息安全.