模 2^n 加与模 2 加相对结合律相容程度的分析*

关 杰,金晨辉,常亚勤
(信息工程大学 电子技术学院,河南 郑州 450004)

摘 要:模 2^n 加和模 2 加是密码算法设计中经常使用的两个编码环节,二者对于结合律的相容程度是指改变二者形成的混合等式中两个变量的运算顺序所造成的误差大小。本文研究了模 2^n 加与模 2 加相对于结合律的相容程度,给出了在改变 $[(x\oplus y)+z] \bmod 2^n$ 的运算顺序时,产生的噪声函数 $\xi(x,y,z)=[(x\oplus y)+_n z]\oplus[x\oplus(y+_n z)]$ 在各点取值的概率分布规律,以及对噪声函数所有取值点的概率值平方求和的计算公式。这些结论在区分攻击中有一定的应用价值。

关键词:模 2^n 加;异或加;相容程度;噪声函数;区分攻击
中图分类号:TN918.1 **文献标志码**:A **文章编号**:1001-2486(2012)02-0042-04

Analysis on the consistent degree of addition modulo 2^n with XOR for associative law

GUAN jie, JIN Chenhui, CHANG Yaqin
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract: Addition modulo 2^n and XOR addition are two code links which are often used in cipher algorithms, the consistent degree of the two links means the difference degree when the computing sequence is changed in the equation including the two links. The difference function between addition modulo 2^n and XOR addition corresponding to associative law is studied. When the computing sequence of $[(x\oplus y)+z] \bmod 2^n$ is changed, the computation formulae of the probability distribution of the difference function $\xi(x,y,z)=[(x\oplus y)+_n z]\oplus[x\oplus(y+_n z)]$ is given, and the square sum of the probability is given too. The results presented are useful for some distinguishing attack.

Key words: addition modulo 2^n; XOR addition; consistent degree; noise function; distinguish attack

模 2^n 加变换和模 2 加变换是密码算法设计中经常用到的编码环节,设计者经常将模 2^n 加作为密码算法的非线性部分,同时将模 2 加变换作为密码算法的线性部分,如密码算法 SNOW 2.0[1],Helix[2],Py[3]等。由于模 2^n 加和模 2 加是两个不同的群运算,且模 2^n 加变换相对于模 2 加是非线性变换,故二者的混合使用有助于增加算法的安全强度。

模 2^n 加与模 2 加的相容程度反映了将其中一种运算被另一种运算替代后所产生的误差大小,或者改变二者形成的一个混合等式中的两个变量位置或运算顺序所造成的误差大小。在对一些密码算法进行区分攻击[4]时,大多利用相应的噪声函数 $\xi(x)$ 的取值的不均匀性所产生的信息泄漏。例如,文献[5]在对 PY 算法进行区分攻击时利用了逐位模 2 加运算代替模 2^n 加运算所造成误差的分布不均匀性。区分攻击的数据复杂性主要由噪声函数 $\xi(x)$ 取值概率的平方和 $\sum_a [p(\xi=a)]^2$ 决定。

文献[6]分析了模 2 加整体逼近模 2^n 加后产生的噪声函数的概率分布,给出了取值概率及其平方和的计算公式。文献[7]指出了模 2 加和模 2^n 加是不相容的,但没有对相容程度进行分析;文献[8]分析了这两个运算相对于结合律的相容程度,证明了等式 $[(x+_n y)\oplus z]\oplus[x+_n(y\oplus z)]=0$ 成立的概率为 0.75^{n-1},这里 $+_n$ 是模 2^n 加(下同)。但是,在区分攻击和其他应用中,需要更加精细地知道在改变 $(x\oplus y)+_n z$ 运算顺序时,产生的噪声函数

$$\xi(x,y,z)=[(x\oplus y)+_n z]\oplus[x\oplus(y+_n z)]$$

的概率分布,以及概率值的平方和。本文将解决这个问题。

* **收稿日期**:2011-07-28
基金项目:通信保密重点实验室基金资助项目(9140C110202110C1101)
作者简介:关杰(1974—),女,河南郑州人,副教授,博士,硕士生导师,E-mail:guanjie007@163.com

1　模 2^n 加与模 2 加相对于结合律的噪声函数的概率分布

设 $x \in Z/(2^n)$ 且 $x = \sum_{k=1}^{n} x_k 2^{k-1}, x_k \in \{0,1\}$。以下本文均称 x_k 是 x 的第 k 位,并将之表示为 x_k 或 $(x)_k$。"$+_n$" 表示模 2^n 加。

定义 1　设 $x,y,z \in Z/(2^n)$,则称 $\xi(x,y,z) = [(x \oplus y) +_n z] \oplus [x \oplus (y +_n z)]$ 为模 2^n 加与模 2 加相对于结合律的噪声函数。

由 $[(x \oplus y) +_n z] = [x \oplus (y +_n z)] \oplus \xi(x,y,z)$ 知,噪声函数 $\xi(x,y,z)$ 反映了改变 $(x \oplus y) +_n z$ 和 $x \oplus (y +_n z)$ 中的运算顺序所造成的误差,故其概率分布从一个方面反映了模 2^n 加与模 2 加的相容程度。

下面给出 ξ 的概率分布的计算公式,即对 $\forall a \in Z/(2^n)$,给出 $p(\xi = a)$ 的计算公式。

引理 1[9]　设 $x,y \in Z/(2^n), d_1 = 0, z = x +_n y +_n d_1$。$\forall k: 2 \leqslant k \leqslant n$,令

$$d_k = \begin{cases} 0, & \text{若 } x_{k-1} + y_{k-1} + d_{k-1} < 2; \\ 1, & \text{若 } x_{k-1} + y_{k-1} + d_{k-1} \geqslant 2. \end{cases}$$

则 $\forall k: 1 \leqslant k \leqslant n$,都有 $z_k = x_k \oplus y_k \oplus d_k$。

以下称引理 1 中的 d_k 为模 2^n 加的第 $k-1$ 位向第 k 位的进位,并称 $\{d_k\}_{k=1}^n$ 为对应的进位序列。

引理 2　设 $x,y,z,a \in Z/(2^n)$,$\{\varphi_k\}_{k=1}^n$ 和 $\{\lambda_k\}_{k=1}^n$ 分别是 $(x \oplus y) +_n z$ 和 $x \oplus (y +_n z)$ 的进位序列,则 $\xi(x,y,z) = a$ 的充要条件是

$\forall k: 1 \leqslant k \leqslant n$,都有 $\lambda_k \oplus \varphi_k = a_k$。

证明　由于 $\xi(x,y,z) = a$ 等价于 $(x \oplus y) +_n z \oplus x \oplus (y +_n z) = a$,即 $\forall k: 1 \leqslant k \leqslant n$,都有 $((x \oplus y) +_n z)_k \oplus (x \oplus (y +_n z))_k = a_k$,再由引理 1 知,$((x \oplus y) +_n z)_k \oplus (x \oplus (y +_n z))_k = a_k$ 等价于 $(x_k \oplus y_k \oplus z_k \oplus \lambda_k) \oplus (x_k \oplus y_k \oplus z_k \oplus \varphi_k) = a_k$ 即 $\lambda_k \oplus \varphi_k = a_k$。证毕。

定理 1　设 $n \geqslant 1, a \in Z/(2^n)$,则有

$$p(\xi = a) = (a_1 \oplus 1) 2^{\lambda_1(a) - 2n + 2} 3^{\lambda_{00}(a)}$$

其中 $\lambda_1(a) = \#\{k: a_k = 1, 1 \leqslant k \leqslant n-1\}$,$\lambda_{00}(a) = \#\{k: a_k = a_{k+1} = 0, 1 \leqslant k \leqslant n-1\}$。"#" 表示集合的个数。

证明　先证对 $2 \leqslant k \leqslant n$ 及 $\forall a_k, a_{k-1}, r \in \{0,1\}$ 条件概率

$$p(\lambda_k \oplus \varphi_k = a_k \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}, \varphi_{k-1} = r) = \frac{1}{8} \#\{(x_{k-1}, y_{k-1}, z_{k-1}): \lambda_k \oplus \varphi_k = a_k \text{ 且 } \lambda_{k-1} = a_{k-1} \oplus r, \varphi_{k-1} = r\}$$

与 r 无关。

事实上,对 $(a_k, a_{k-1}, \varphi_{k-1})$ 的 8 种取值,可分别求出 $\lambda_{k-1} = a_{k-1} \oplus \varphi_{k-1}$,并通过对二元变量 $x_{k-1}, y_{k-1}, z_{k-1}$ 的穷举,找出满足 $\lambda_k \oplus \varphi_k = a_k$ 的 $(x_{k-1}, y_{k-1}, z_{k-1})$ 个数。该过程可借助计算机完成。结果表明,具体个数与 φ_{k-1} 的取值无关,且当 $a_k = a_{k-1} = 0$ 时,个数为 6;当 $a_{k-1} = 1$ 时,个数为 4;当 $(a_{k-1}, a_k) = (0,1)$ 时,个数为 2,即 $\forall a_k, a_{k-1}, r \in \{0,1\}$,都有

$$p(\lambda_k = \varphi_k \oplus a_k \mid \lambda_{k-1} = \varphi_{k-1} \oplus a_{k-1}, \varphi_{k-1} = r) = 2^{a_{k-1}-2} \times 3^{a_{k-1} = a_k = 0}$$

其中当 $a_k = a_{k-1} = 0$ 时,规定 $3^{a_{k-1} = a_k = 0} = 3$,否则规定 $3^{a_{k-1} = a_k = 0} = 1$。再由全概率公式知

$$\begin{aligned} & p(\lambda_k \oplus \varphi_k = a_k \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}) \\ &= \sum_{r \in \{0,1\}} p(\lambda_k \oplus \varphi_k = a_k \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}, \varphi_{k-1} = r) \\ & \quad p(\varphi_{k-1} = r \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}) \\ &= 2^{a_{k-1}-2} \times 3^{a_{k-1} = a_k = 0} \sum_{r \in \{0,1\}} p(\varphi_{k-1} = r \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}) \\ &= 2^{a_{k-1}-2} \times 3^{a_{k-1} = a_k = 0} \end{aligned}$$

又因 λ_n 和 φ_n 只与 $\lambda_{n-1}, \varphi_{n-1}, x_{n-1}, y_{n-1}, z_{n-1}$ 有关,从而由全概率公式可得

$$\begin{aligned} & p(\lambda_n \oplus \varphi_n = a_n \mid \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}, \cdots, \lambda_1 \oplus \varphi_1 = a_1) \\ &= \sum_{r \in \{0,1\}} p(\lambda_n \oplus \varphi_n = a_n \mid \varphi_{n-1} = r, \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}, \cdots, \lambda_1 \oplus \varphi_1 = a_1) \times p(\varphi_{n-1} = r \mid \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}, \cdots, \lambda_1 \oplus \varphi_1 = a_1) \\ &= p(\lambda_n \oplus \varphi_n = a_n \mid \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}) \\ & \quad \sum_{r \in \{0,1\}} p(\varphi_{n-1} = r \mid \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}, \cdots, \lambda_1 \oplus \varphi_1 = a_1) \\ &= p(\lambda_n \oplus \varphi_n = a_n \mid \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}) \end{aligned}$$

从而有

$$\begin{aligned} & p(\xi = a) \\ &= p(\lambda_n \oplus \varphi_n = a_n, \cdots, \lambda_1 \oplus \varphi_1 = a_1) \\ &= p(\lambda_n \oplus \varphi_n = a_n \mid \lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}) p(\lambda_{n-1} \oplus \varphi_{n-1} = a_{n-1}, \cdots, \lambda_1 \oplus \varphi_1 = a_1) \\ &= \cdots = p(\lambda_1 \oplus \varphi_1 = a_1) \prod_{k=2}^{n} p(\lambda_k \oplus \varphi_k = a_k \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}) \\ &= (a_1 \oplus 1) \prod_{k=2}^{n} p(\lambda_k \oplus \varphi_k = a_k \mid \lambda_{k-1} \oplus \varphi_{k-1} = a_{k-1}) \\ &= (a_1 \oplus 1) \prod_{k=2}^{n} (2^{a_{k-1}-2} \times 3^{a_{k-1} = a_k = 0}) \\ &= (a_1 \oplus 1) 2^{\lambda_1(a) - 2n + 2} 3^{\lambda_{00}(a)} \end{aligned}$$

这说明本定理成立。证毕。

2 模 2^n 加与模 2 加相对于结合律的噪声函数取值概率的平方和

为计算模 2^n 加与模 2 加相对于结合律的噪声函数取值概率的平方和,先给出几个引理。

引理 3 设 $n \geqslant 1$, $f(n) = \sum_{a\in\{0,1\}^n}(a_1 \oplus 1)4^{\lambda_1(a)}9^{\lambda_{00}(a)}$, $g_i(n) = \sum_{a\in\{0,1\}^n,a_1=i} 4^{\lambda_1(a)}9^{\lambda_{00}(a)}$, 则有 $g_0(n) = 16^{n-1}f(n)$ 和 $g_1(n) = 4^{n-2}\sum_{k=2}^{n-1}2^{2k}f(k) + 8\times 4^{n-2}$。

证明 由题设

$$f(n) = \sum_{a\in\{0,1\}^n}(a_1\oplus 1)4^{\lambda_1(a)-2n+2}9^{\lambda_{00}(a)} = 16^{1-n}\sum_{a\in\{0,1\}^n,a_1=0}4^{\lambda_1(a)}9^{\lambda_{00}(a)} = 16^{1-n}g_0(n)$$

即 $g_0(n) = 16^{n-1}f(n)$ 成立。

记 $b = \{b \in Z/(2^{n-1}) : b_i = a_{i+1}, 1 \leqslant i \leqslant n-1\}$, 则

$$g_1(n) = \sum_{a\in\{0,1\}^n,a_1=1}4^{\lambda_1(a)}9^{\lambda_{00}(a)}$$

$$= \sum_{a\in\{0,1\}^n,a_1=1,a_2=1}4^{\lambda_1(a)}9^{\lambda_{00}(a)} + \sum_{a\in\{0,1\}^n,a_1=1,a_2=0}4^{\lambda_1(a)}9^{\lambda_{00}(a)}$$

$$= \sum_{b\in\{0,1\}^{n-1},b_1=1}4^{\lambda_1(a)+1}9^{\lambda_{00}(a)} + \sum_{b\in\{0,1\}^{n-1},b_1=0}4^{\lambda_1(a)+1}9^{\lambda_{00}(a)}$$

$$= 4(g_1(n-1) + g_0(n-1))$$

即当 $k = 1$ 时, $g_1(n) = \sum_{i=1}^{k}4^i g_0(n-i) + 4^k g_1(n-k)$ 成立。再利用归纳法易证该式对 $k \leqslant n-2$ 均成立。特别地,取 $k = n-2$,则由 $g_1(2) = 8$ 可知

$$g_1(n) = \sum_{i=1}^{n-2}4^i g_0(n-i) + 4^{n-2}g_1(2) = 4^{n-2}\sum_{k=2}^{n-1}2^{2k}f(k) + 8\times 4^{n-2}$$

证毕。

下面解决 $f(k)$ 的计算问题。

引理 4 设 $n \geqslant 1$, $f(n) = \sum_{a\in\{0,1\}^n}(a_0\oplus 1)4^{\lambda_1(a)-2n+2}9^{\lambda_{00}(a)}$,定义 $\alpha_1 = 1, \beta_1 = 9/16$,且 $\forall i \geqslant 2$,定义

$$\begin{cases}\alpha_i = \alpha_{i-1} + \beta_{i-1}2^{2(i-1)}\\ \beta_i = \frac{9}{16}\beta_{i-1} + \alpha_{i-1}(\frac{1}{4})^{i+1}\end{cases}$$

则对任意的正整数 i,均有

$$f(n) = \alpha_i\frac{1}{4}(\frac{1}{2})^{2n}\sum_{k=2}^{n-i-1}(2)^{2k}f(k) + \beta_i f(n-i) + \alpha_i 2\times(\frac{1}{2})^{2n} \quad (1)$$

证明 记

$b = \{b \in Z/(2^{n-1}) : b_i = a_{i+1}, 0 \leqslant i \leqslant n-2\}$,

则

$$f(n) = \frac{1}{16^{n-1}}\sum_{a\in\{0,1\}^n}(a_0\oplus 1)4^{\lambda_1(a)}9^{\lambda_{00}(a)} = \frac{1}{16^{n-1}}\sum_{a\in\{0,1\}^n,a_1=0}4^{\lambda_1(a)}9^{\lambda_{00}(a)}$$

$$= \sum_{a\in\{0,1\}^n,a_1=0,a_2=1}4^{\lambda_1(a)}9^{\lambda_{00}(a)} + \sum_{a\in\{0,1\}^n,a_1=0,a_2=0}4^{\lambda_1(a)}9^{\lambda_{00}(a)}$$

$$= 16^{1-n}(g_1(n-1) + 9g_0(n-1)) = (\frac{1}{4})^{n+1}\sum_{k=2}^{n-2}2^{2k}f(k) + \frac{9}{16}f(n-1) + 2\times(\frac{1}{4})^n$$

即当 $i = 1$ 时,式(1)成立。现设当 $i = k$ 时,式(1)成立,即

$$f(n) - \beta_k f(n-k) = \alpha_k[\frac{1}{4}(\frac{1}{2})^{2n}\sum_{i=2}^{n-k-1}2^{2i}f(i) + 2\times(\frac{1}{2})^{2n}]$$

再将

$$f(n-k) = \frac{1}{4}(\frac{1}{2})^{2(n-k)}\sum_{i=2}^{n-k-2}(2)^{2i}f(i) + \frac{9}{16}f(n-k-1) + 2\times(\frac{1}{2})^{2(n-k)}$$

代入上式,可得

$$f(n) = [\alpha_k\frac{1}{4}(\frac{1}{2})^{2n} + \beta_k\frac{1}{4}(\frac{1}{2})^{2(n-k)}]\sum_{i=2}^{n-k-2}2^{2i}f(i) + [\alpha_k(\frac{1}{2})^{2(k+2)} + \frac{9}{16}\beta_k]f(n-k-1) + [2\alpha_k(\frac{1}{2})^{2n} + 2\beta_k(\frac{1}{2})^{2(n-k)}]$$

$$= \frac{1}{4}(\frac{1}{2})^{2n}\alpha_{k+1}\sum_{i=2}^{n-k-2}2^{2i}f(i) + \beta_{k+1}f(n-k-1) + 2(\frac{1}{2})^{2n}\alpha_{k+1}$$

即当 $i = k+1$ 时,式(1)成立,故由归纳法知式(1)总成立。证毕。

引理5 题设同引理4,则对于任意的正整数 $i \geqslant 1$,均有

$$\alpha_i = \frac{4}{\sqrt{41}}\times\frac{1}{8^i}[(13+\sqrt{41})^i - (13-\sqrt{41})^i]$$

$$\beta_i = \frac{1}{2}\times\frac{1}{\sqrt{41}}\times\frac{1}{32^i}[(13+\sqrt{41})^i(\sqrt{41}+5) + (13-\sqrt{41})^i(\sqrt{41}-5)]$$

证明 由 $\alpha_i = \alpha_{i-1} + \beta_{i-1}2^{2(i-1)}$ 知

$$\beta_{i-1} = (\frac{1}{2})^{2(i-1)}(\alpha_i - \alpha_{i-1})$$

从而由 $\beta_i = \frac{9}{16}\beta_{i-1} + \alpha_{i-1}(\frac{1}{2})^{2i+2}$ 得到

$$(\frac{1}{2})^{2i}(\alpha_{i+1} - \alpha_i)$$

$$= \frac{9}{16}\left(\frac{1}{2}\right)^{2(i-1)}(\alpha_i - \alpha_{i-1}) + \alpha_{i-1}\left(\frac{1}{2}\right)^{2i+2}$$

即 $\alpha_{i+1} = \frac{13}{4}\alpha_i - 2\alpha_{i-1}$。由于方程 $\lambda^2 - \frac{13}{4}\lambda + 2 = 0$ 的两个解分别为

$$\lambda_1 = \frac{13 + \sqrt{41}}{8},\ \lambda_2 = \frac{13 - \sqrt{41}}{8}$$

从而由组合数学知,存在常数 c_1 和 c_2,使得对 $\forall i \geqslant 1$,都有

$$\alpha_i = c_1{\lambda_1}^i + c_2{\lambda_2}^i$$

由引理4知,$\alpha_1 = 1$ 和 $\alpha_2 = \frac{13}{4}$,将它们代入上式可得 $c_1 = 4/\sqrt{41}$,$c_2 = -4/\sqrt{41}$,故有

$$\alpha_i = \frac{4}{\sqrt{41}} \times \frac{1}{8^i}[(13 + \sqrt{41})^i - (13 - \sqrt{41})^i]$$

进而有

$$\beta_i = \frac{1}{2} \times \frac{1}{\sqrt{41}} \times \frac{1}{32^i}[(13 + \sqrt{41})^i(\sqrt{41} + 5) + (13 - \sqrt{41})^i(\sqrt{41} - 5)]$$

证毕。

定理 2　当 $n \geqslant 1$ 时,均有

$$\sum_{a \in \{0,1\}^n}[p(\xi(x,y,z) = a)]^2 = \frac{2^{7-5n}}{\sqrt{41}}[(49\sqrt{41} + 317)(13 + \sqrt{41})^{n-3} + (49\sqrt{41} - 317)(13 - \sqrt{41})^{n-3}]$$

证明　当 $n = 1,2$ 时,直接验证,即知定理2成立。下设 $n \geqslant 3$。由于

$$\begin{aligned}
&\sum_{a \in \{0,1\}^n}[p(\xi = a)]^2 \\
&= \sum_{a \in \{0,1\}^n}[(a_1 \oplus 1)2^{\lambda_1(a)-2n+2}3^{\lambda_{00}(a)}]^2 \\
&= \sum_{a \in \{0,1\}^n, a_1 = 0}(a_1 \oplus 1)4^{\lambda_1(a)-2n+2}9^{\lambda_{00}(a)} + \\
&\quad \sum_{a \in \{0,1\}^n, a_1 = 1}(a_1 \oplus 1)4^{\lambda_1(a)-2n+2}9^{\lambda_{00}(a)} \\
&= \sum_{a \in \{0,1\}^n, a_1 = 0}4^{\lambda_1(a)-2n+2}9^{\lambda_{00}(a)} \\
&= \frac{1}{16^{n-1}}\sum_{a \in \{0,1\}^n}(a_1 \oplus 1)4^{\lambda_1(a)}9^{\lambda_{00}(a)} = f(n)
\end{aligned}$$

故由引理4得

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

再由 $f(2) = \frac{5}{8}$,$f(3) = \frac{98}{256}$ 可得

$$f(n) = \frac{9}{2}\left(\frac{1}{2}\right)^{2n}\alpha_{n-3} + \frac{98}{256}\beta_{n-3}$$,即

$$f(n) = \frac{2^{7-5n}}{\sqrt{41}}[(49\sqrt{41} + 317)(13 + \sqrt{41})^{n-3} + (49\sqrt{41} - 317)(13 - \sqrt{41})^{n-3}]$$

证毕。

3　结束语

本文进一步分析了模 2^n 加与模 2 加相对于结合律的相容程度,给出了改变 $(x \oplus y) +_n z$ 和 $(x \oplus y) +_n z$ 的运算顺序所造成的噪声函数 $\xi(x,y,z) = [(x \oplus y) +_n z] \oplus [x \oplus (y +_n z)]$ 的概率值及其平方和的计算公式,并在 $1 \leqslant n \leqslant 10$ 时,借助计算机验证了所得结论的正确性。本文的结果对于研究密码算法的抗区分攻击等攻击方法的能力,具有实际的应用价值。在后续的研究中,我们将探索本文结论在密码分析中的应用,研究刻画模 2^n 加与模 2 加相容程度的其他途径,并利用概率论手段对其进行定量刻画。

参考文献(References)

[1] Ekdahl P, Johansson T. A new version of the stream cipher Snow[C]// Proc of Selected Areas in Cryptography - SAC 2002, LNCS 2595: 47 - 61.

[2] Doug W, Bruce S, Stefan L, et al. Helix: fast encryption and authentication in a single cryptographic primitive[C]// Proc of Fast Software Encryption 2003, Berlin: Springer-Verlag, 2003: 330 - 347.

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

[4] Baigneres T, Junod P, Vandenay S. How far can we go beyond linear cryptanalysis[C]// Proc of Advances in Cryptology-Asiacrypt 2004, LNCS 3329: 432 - 450.

[5] Crowley P. Improved cryptanalysis of PY[R]. ESTREAM ECRYT Stream Cipher Project, Report 2006/010, 2006.

[6] 陈士伟, 金晨辉. 模2加整体逼近二元和三元模 2^n 加的噪声函数分析[J]. 电子与信息学报, 2008, 30(6): 1445 - 1449.
CHEN Shiwei, JIN Chenhui. Analysis of the noise functions of macrocosm approximation of binary addition and triple addition modulo 2^n with XOR[J]. Jornal of Electronics & Information Teohnology, 2008, 30(6): 1445 - 1449. (in Chinese)

[7] Lai X J, Massey J L. A proposal for a new block encryption standard[C]// Proc of Advances in Cryptology EUROCRYPT' 90, 1990: 389 - 404.

[8] 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[J]. 高校应用数学学报, 2003, 18(2): 247 - 250.
GUO Jiansheng, JIN Chenhui. Analysis on the consistent degree of addition modulo 2^n with XOR [J]. Applied Mathematics A Journal of Chinese Universities, 2003, 18(2): 247 - 250.

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