软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(7):1652−1660 [doi: 10.3724/SP.J.1001.2011.03837]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

模 2^n 加和模 2 加混合运算的异或分支数*

常亚勤+, 金晨辉

(解放军信息工程大学 电子技术学院,河南 郑州 450004)

On the XOR Branch Numbers of the Transformations About Modulo 2^n Addition and Modulo 2 Addition

CHANG Ya-Qin+, JIN Chen-Hui

(College of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

+ Corresponding author: E-mail: yaqinchang@yahoo.com.cn

Chang YQ, Jin CH. On the XOR branch numbers of the transformations about modulo 2^n addition and modulo 2 addition. *Journal of Software*, 2011,22(7):1652−1660. http://www.jos.org.cn/1000-9825/3837.htm

Abstract: This paper studies the xor branch numbers of diffusion structures, which uses the nonlinear transformations over the finite field *GF*(2). This paper gives the definition of the xor branch numbers of diffusion structures and the relations between it and the strength of a cipher against differential and linear cryptanalysis. Also, this paper has proven that the xor branch numbers of diffusion structures is about modulo 2^n addition, and the modulo 2 addition is equal to that of the diffusion structure over the finite field *GF*(2), which 1 is substituted for the odd coefficient and 0 for the even coefficient and the modulo 2^n addition for the modulo 2 addition. Consequently, this paper simplifies the computation problem of the xor branch numbers in this kind of nonlinear diffusion structure.

Key words: block cipher; nonlinear diffusion structure; xor branch number; mixed operator; provable security

摘 要: 研究了扩散结构为二元域上非线性变换的异或分支数.给出了扩散结构为二元域上非线性变换的异或分支数的定义及其与分组密码抗差分攻击和线性分析能力的关系,证明了以模 2^n 加和模 2 加的混合运算为扩散结构的异或分支数等于将模 2^n 加换成模 2 加且将各变元系数模 2 后所得的二元域上线性变换的异或分支数,从而简化了此类非线性扩散结构异或分支数的计算问题.

关键词: 分组密码;非线性扩散结构;异或分支数;混合运算;可证明安全性

中图法分类号: TP309 **文献标识码**: A

差分分析和线性分析是对分组密码的两种基本攻击方法,每个分组密码都应能够抵抗这两种攻击.目前,证明一个分组密码算法能够抵抗差分分析和线性分析的主要方法是证明它的差分概率和线性特征概率小于一个理想的上界,证明的手段主要是借助分支数理论[1]来证明该分组密码算法的每个差分路径和线性逼近路径都具有足够多的活动 *S* 盒.

目前,针对 SP 网络、Fesitel 模型、嵌套 SP 网络的 Fesitel 模型以及一些特殊的不平衡 Fesitel 模型都建立

* 基金项目: 河南省杰出青年科学基金(0312001800)
收稿时间: 2009-10-18; 定稿时间: 2010-03-16

了相应的分支数理论[2−7].对于这些模型,只要给出其扩散结构的分支数,就能应用分支数理论给出分组密码算法每条差分路径和线性逼近路径的活动 S 盒的下界.

在上述密码模型中,扩散结构都是二元域上的线性变换或者仿射变换.例如,Rijndael 算法、Square 算法、Aria 算法、E2 算法、Camellia 算法、CLFFA 算法等都是如此.但是,二元域上的仿射变换并不是设计扩散结构的唯一选择.在求新求异的设计思想下,可能会出现很多以二元域上的非线性变换为扩散结构的密码算法.例如,SAFER 系列分组密码算法的扩散结构都是以 $Z/(2^n)$上伪 Hadamard 变换为基石构造的环 $Z/(2^n)$上的线性变换,其中,SAFER64 的扩散结构就是 $Z/(256)$上的线性变换:

$$(y_1,y_2,...,y_8)=(x_1,x_2,...,x_8)\begin{pmatrix}8&4&4&2&4&2&2&1\\4&2&4&2&2&1&2&1\\4&2&2&1&4&2&2&1\\2&1&2&1&2&1&2&1\\4&4&2&2&2&2&1&1\\2&2&2&2&1&1&1&1\\2&2&1&1&2&2&1&1\\1&1&1&1&1&1&1&1\end{pmatrix}.$$

此外,基于模 2^n 加与模 2 加的不相容性,人们也常将模 2^n 加与模 2 加的混合运算作为密码算法的一个基本部件.例如,在 Blowfish 分组密码算法的设计中,4 个 8 进 32 出的 S 盒的结合就是采用了模 2^n 加与模 2 加的混合运算产生输出:

$$F(a,b,c,d)=((S_1(a)+S_2(b))\oplus S_3(c))+S_4(d),$$

其中,+是模 2^{32} 加.MUST1 分组算法 Fesitel 结构的 F 函数的构造中采用了如下的模 2^n 加与模 2 加的混合运算:

$$(x+y+k_1)\oplus(y\oplus k_2)\oplus(y+k_3),$$

其中,+是模 2^{32} 加.与单纯采用二元域上的线性变换相比,由于扩散结构的非线性这一特性,因而模 2^n 加与模 2 加的混合运算可望进一步提高密码算法的抗攻击能力.

目前,还未见有文献对非线性扩散结构的线性分支数进行研究.本文将针对模 2^n 加与模 2 加的混合运算这类新型的非线性扩散结构,研究其分支数的定义和计算问题.所得的结果可用于评估在将 SP 网络、Fesitel 模型、嵌套 SP 网络的 Fesitel 模型等密码模型中的线性扩散结构换成由模 2^n 加与模 2 加的混合运算构成的非线性扩散结构时,密码算法的差分路径和线性逼近路径的活动 S 盒个数的下界,从而给出此类分组密码抗差分攻击和抗线性密码分析的最低能力.

我们将首先给出模 2^n 加和模 2 加混合运算的数学描述及性质,并给出扩散结构的异或分支数的定义.然后利用扩散结构 P 的异或分支数给出了 SPS 模型的差分链概率和线性逼近链优势的上界,从而给出该模型的分支数与分组密码抗差分攻击能力和线性攻击能力的关系.最后,将证明混合运算的异或分支数等于将模 2^n 加换成模 2 加且将各变元系数模 2 后所得的二元域上线性变换的异或分支数,从而简化了此类非线性扩散结构异或分支数的计算问题,并将其该类扩散结构的异或分支数的研究和计算归结为对二元域上线性变换的异或分支数的研究和计算.

1 模 2^n 加和模 2 加混合运算

首先给出模 2^n 加和模 2 加混合运算的数学描述.

定义 1. 设 $x_1,x_2,\ldots,x_m\in\{0,1\}^n$,$\Omega_0=\{x_1,x_2,\ldots,x_m\}$,$\Lambda=\{\oplus,\bar{+}\}$,$\bar{+}$ 是模 2^n 加.对于$\forall i\geqslant 1$,记

$$\Omega_i=\{X\Diamond Y:X,Y\in\Omega_{i-1},\Diamond\in\Lambda\},$$

则$\bigcup_{t=0}^{\infty}\Omega_t$ 中的每个元素都称为 $x_1,x_2,\ldots,x_m$ 关于模 2^n 加和模 2 加运算的一个混合运算,简称混合运算.

显然,$x_1,x_2,\ldots,x_m$ 的混合运算就是在 $\bar{+}$ 和⊕没有优先计算级的条件下,对 $x_1,x_2,\ldots,x_m$ 利用运算 $\bar{+}$ 和⊕进行递归计算的一个递归计算式.

定义 2. 设 $f(x_1,\ldots,x_m)$是 $x_1,x_2,\ldots,x_m$ 的一个混合运算,则称 x_t 在该递归表达式中的出现次数 $n_t(f)$为 x_t 在该混

合运算的计算式中的出现次数.

下面给出模 2^n 加和模 2 加混合运算的重要性质.

引理 1. 设 $x_1,x_2,\ldots,x_m\in\{0,1\}^n$,$g(x_1,\ldots,x_m)$是 $x_1,x_2,\ldots,x_m$ 混合运算,则一定存在布尔函数 l,使得

$$g_t=\bigoplus_{i=1}^{m}s_i(g)x_{i,t}\oplus l(x_{1,1},x_{1,2},...,x_{1,t-1};x_{2,1},x_{2,2},...,x_{2,t-1};...;x_{m,1},x_{m,2},...,x_{m,t-1}),$$

其中,$s_t(g)=n_t(g)\bmod 2$,$x_{t,1},x_{t,2},\ldots,x_{t,n}$ 是整数 x_t 的二进制表示的最低位到最高位,$g_1,g_2,\ldots,g_n$ 是整数 $g(x_1,\ldots,x_m)$的二进制表示的最低位到最高位.

证明:由于 $g(x_1,...,x_m)\in\bigcup_{i=1}^{\infty}\Omega_i$,故存在 $k\geqslant 1$,使得 $g(x_1,\ldots,x_m)\in\Omega_k$ 且 $g(x_1,\ldots,x_m)\in\Omega_{k-1}$.令 $s_t(g)=n_t(g)\bmod 2$,现利用归纳法证明引理 1.

当 $k=1$ 时,显然该结论成立.假设 k 时该结论成立,现证明 $k+1$ 时情形.

根据定义 1,存在 $h(x_1,\ldots,x_m),h'(x_1,\ldots,x_m)\in\Omega_{k-1}$,使得

$$g(x_1,\ldots,x_m)=h(x_1,\ldots,x_m)\oplus h'(x_1,\ldots,x_m) \tag{1}$$

或

$$g(x_1,...,x_m)=h(x_1,...,x_m)\bar{+}h'(x_1,...,x_m) \tag{2}$$

设 $1\leqslant t\leqslant n$,并记 $h_1,h_2,\ldots,h_n$ 和 $h'_1,h'_2,...,h'_n$ 分别是 $h(x_1,\ldots,x_m)$和 $h'(x_1,\ldots,x_m)$的二进制表示的最低位到最高位,则当公式(1)成立时,$g_t=h_t\oplus h'_t$;当公式(2)成立时,记 $g(x_1,x_2,\ldots,x_m)$的第 $t-1$ 位到第 t 位的进位为 $g'(h_1,h_2,...,h_{t-1},h'_1,h'_2,...,h'_{t-1})$,则

$$g_t=h_t\oplus h'_t\oplus g'(h_1,h_2,...,h_{t-1},h'_1,h'_2,...,h'_{t-1}) \tag{3}$$

因 $h,h'\in\Omega_{k-1}$,故由归纳假设可知,$h_1,h_2,...,h_{t-1},h'_1,h'_2,...,h'_{t-1}$ 只是 $x_1,x_2,\ldots,x_m$ 的二进制表示的低 $t-1$ 位变量 $x_{1,1},x_{1,2},\ldots,x_{1,t-1};x_{2,1},x_{2,2},\ldots,x_{2,t-1};\ldots;x_{m,1},x_{m,2},\ldots,x_{m,t-1}$ 的函数,且存在布尔函数φ和φ',使得

$$h_t=\bigoplus_{i=1}^{m}s_i(h)x_{i,t}\oplus\varphi(x_{1,1},x_{1,2},...,x_{1,t-1},x_{2,1},x_{2,2},...,x_{2,t-1},...,x_{m,1},x_{m,2},...,x_{m,t-1}),$$

$$h'_t=\bigoplus_{i=1}^{m}s_i(h')x_{i,t}\oplus\varphi'(x_{1,1},x_{1,2},...,x_{1,t-1},x_{2,1},x_{2,2},...,x_{2,t-1},...,x_{m,1},x_{m,2},...,x_{m,t-1}).$$

由于 $s_i(f)=s_i(h)\oplus s_i(h')$,从而由公式(3)可知:

$$g_t=\bigoplus_{i=1}^{m}[s_i(h)\oplus s_i(h')]x_{i,t}\oplus l'=\bigoplus_{i=1}^{m}s_i(g)x_{i,t}\oplus l',$$

其中,l'是变量 $x_{1,1},x_{1,2},\ldots,x_{1,t-1};x_{2,1},x_{2,2},\ldots,x_{2,t-1};\ldots;x_{m,1},x_{m,2},\ldots,x_{m,t-1}$ 的函数.这说明 $k+1$ 时结论成立,因而本引理对所有 k 成立.证毕. □

2 模 2^n 加和模 2 加混合运算的异或分支数及其与抗差分和线性攻击能力的关系

下面给出本文所使用的一些基本定义和符号说明,设 $y\in Z/(2^n)$,记 $y=\sum_{j=1}^{n}2^{j-1}y_j$ 且诸 $y_j\in\{0,1\}$,则$(y_n,\ldots,y_2,y_1)$是 y 的二进制表示,且称 y_j 为 y 的第 j 比特.本文均假设 y 的实数表示与其二进制表示按上述方式一一对应,且对二者不加区分地使用.对于$\{0,1\}^n$ 上的 m 维向量 $x=(x_1,\ldots,x_m)$和$\beta=(\beta_1,\ldots,\beta_m)$,约定 $x\cdot\beta=(x_1,\ldots,x_m)\cdot(\beta_1,\ldots,\beta_m)=x_1\cdot\beta_1\oplus\ldots\oplus x_m\cdot\beta_m$.$\forall t:1\leqslant t\leqslant m$,约定 $x_{t,1},\ldots,x_{t,n}$ 是整数 x_t 的二进制表示的最低位到最高位.

定义 3[8]. 设 $s:\{0,1\}^n\to\{0,1\}^n,\alpha,\beta\in\{0,1\}^n$,则称

$$p_{(s)}(\alpha\to\beta)=(1/2^n)(\#\{x\in Z/(2^n):s(x)\oplus s(x\oplus\alpha)=\beta\}),$$

$$\rho_{(s)}(\alpha\to\beta)=\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{\beta\cdot s(x)\oplus\alpha\cdot x}$$

分别为 s 的差分概率和相关系数,并分别称

$$DP^{s}_{\max}(\alpha\to\beta)=\max\{p_{(s)}(\alpha\to\beta):\alpha,\beta\in\{0,1\}^n,\alpha\neq 0\},$$
$$LP^{s}_{\max}(\alpha\to\beta)=\max\{|\rho_{(s)}(\alpha\to\beta)|:\alpha,\beta\in\{0,1\}^n,\beta\neq 0\}$$

为 s 的最大差分概率和最大相关优势.这里,#{·}表示集合的元素个数,$\forall\alpha,y\in\{0,1\}^n$,$\alpha\cdot y=\alpha_n\cdot y_n\oplus\ldots\oplus\alpha_1\cdot y_1$ 表示 α 与 y 的点积.

定义 4[8]. 设 $\alpha,\beta,u,v\in\{0,1\}^{mn}$,则称 $p_{(s)}(\alpha\to u)\times p_{(P)}(u\to v)\times p_{(s)}(v\to\beta)$ 为 SPS 模型的差分传递链 $\alpha\to u\to v\to\beta$ 的转移概率,称 $|\rho_{(s)}(\alpha\to u)\times\rho_{(P)}(u\to v)\times\rho_{(s)}(v\to\beta)|$ 为 SPS 模型的线性逼近链 $\alpha\to u\to v\to\beta$ 的优势,并分别称

$$DP^{SPS}_{\max}=\max\{p_{(s)}(\alpha\to u)\times p_{(P)}(u\to v)\times p_{(s)}(v\to\beta):\alpha,\beta,u,v\in\{0,1\}^{nm},\alpha\neq 0\},$$
$$LP^{SPS}_{\max}=\max\{|\rho_{(s)}(\alpha\to u)\times\rho_{(P)}(u\to v)\times\rho_{(s)}(v\to\beta)|:\alpha,\beta,u,v\in\{0,1\}^{nm},\beta\neq 0\}$$

为 SPS 模型的差分链 $\alpha\to u\to v\to\beta$ 的最大概率和线性逼近链 $\alpha\to u\to v\to\beta$ 的最大优势.

下面给出非线性扩散结构的异或分支数的定义及其与 SPS 模型抗差分和线性攻击能力的关系.

下面的 $Z/(2^n)$ 均指模 2^n 剩余类环,对于 $Z/(2^n)$ 上的 m 维向量 $\alpha=(\alpha_1,\ldots,\alpha_m)$,称 $\alpha_1,\alpha_2,\ldots,\alpha_m$ 中非零元的个数 $W_n(\alpha)$ 为 α 相对于 n 比特分组的重量.

定义 5. 设 $f:(Z/(2^n))^m\to(Z/(2^n))^m$,则称

$$D^{(n)}_f=\min\{W_n(\alpha)+W_n(\beta):p_{(f)}(\alpha\to\beta)\neq 0:\alpha,\beta\in(Z/(2^n))^m,\alpha\neq 0\},$$
$$L^{(n)}_f=\min\{W_n(\alpha)+W_n(\beta):\rho_{(f)}(\alpha\to\beta)\neq 0:\alpha,\beta\in(Z/(2^n))^m,\beta\neq 0\}$$

分别为 f 相对于 n 比特分组的异或差分和线性分支数,简称为 f 的异或差分(线性)分支数.

显然,二元域上线性变换的异或差分(线性)分支数是定义 5 的特例.

定理 2. 设 SPS 模型中的混淆层是 $\{0,1\}^n$ 上 m 个双射的并置,q 是这 m 个双射的最大差分概率的最大值,q' 是这 m 个双射的最大相关优势的最大值,即 $q=\max_{1\leqslant i\leqslant m}DP^{S_i}_{\max}$,$q'=\max_{1\leqslant i\leqslant m}LP^{S_i}_{\max}$,则 SPS 的差分链的最大概率和线性逼近链的最大优势分别以 $q^{D^{(n)}_P}$ 和 $q'^{L^{(n)}_P}$ 为上界,即 $DP^{SPS}_{\max}\leqslant q^{D^{(n)}_P}$,$LP^{SPS}_{\max}\leqslant q^{L^{(n)}_P}$.

由定理 2 可知,已知 $D^{(n)}_P$ 和 $L^{(n)}_P$ 就可以得到 SPS 模型差分链的最大概率和线性逼近链的最大优势的上界,从而给出其抵抗差分和线性分析的可证明安全性.

下面给出模 2^n 加和模 2 加混合运算异或分支数的计算方法.

2.1 模2^n加和模2加混合运算的异或差分分支数

为了给出模 2^n 加和模 2 加混合运算的异或差分分支数的计算,我们首先将 $GF(2^n)$ 上二元矩阵对应的线性变换的异或差分分支数的计算归结为二元域上该矩阵对应的线性变换的异或差分分支数的计算问题,并给出模 2^n 加和模 2 加混合运算异或差分概率不为 0 的必要条件,最后给出模 2^n 加和模 2 加混合运算的异或差分分支数的计算.

引理 2. 设 M 为 $m\times m$ 二元矩阵,$g:[GF(2^n)]^m\to[GF(2^n)]^m$ 定义为 $g(y)=My$,其中,y 是有限域 $GF(2^n)$ 上的 m 维列向量,则对 $n\geqslant 1$,都有:

(1) $D^{(n)}_g=D^{(1)}_g=\min\{W_1(Mx)+W_1(x):x\in\{0,1\}^m,x\neq 0\}$;

(2) $L^{(n)}_g=L^{(1)}_g=\min\{W_1(M^Tx)+W_1(x):x\in\{0,1\}^m,x\neq 0\}$.

证明:略.

引理 3. 设 $f:(Z/(2^n))^m\to(Z/(2^n))^m$,记 $f=(f_1,f_2,\ldots,f_m)$ 且对 $1\leqslant i\leqslant m$,$f_i=(x_1,x_2,\ldots,x_m)$ 都是 $x_1,x_2,\ldots,x_m$ 的混合运算.记 $\alpha=(\alpha_1,\ldots,\alpha_m)$,$\beta=(\beta_1,\ldots,\beta_m)\in(Z/(2^n))^m$,令 $\theta=\min\{j:\alpha_{i,j}=1,1\leqslant j\leqslant n,1\leqslant i\leqslant m\}$,则 f 的异或差分对应 $\alpha\to\beta$ 的概率不为 0 的必要条件是:

(1) $\forall i:1\leqslant i\leqslant m$,都有 $\bigoplus_{k=1}^{m}[n_k(f_i)\bmod 2]\alpha_{k,\theta}=\beta_{i,\theta}$;

(2) 当 $j<\theta$ 时,对 $1\leqslant i\leqslant m$,都有 $\beta_{i,j}=0$.

证明:设 $1\leqslant i\leqslant m,1\leqslant j\leqslant n$,且 $f_i(x)$ 的第 j 比特为 $f_{i,j}(x)$,由于 $n_t(f_i)$ 是 x_t 在 $f_i=(x_1,\ldots,x_m)$ 中的出现次数,记

$c_k(f_i)=n_k(f_i)\bmod 2$,故由引理 1 可知:

$$f_{i,j}=\bigoplus_{k=1}^{m}c_k(f_i)x_{k,j}\oplus l_{i,j}(x_{1,1},x_{1,2},...,x_{1,j-1},x_{2,1},x_{2,2},...,x_{2,j-1},...,x_{m,1},x_{m,2},...,x_{m,j-1}),$$

其中,$l_{i,j}$是以 $x_{1,1},x_{1,2},\ldots,x_{1,j-1},x_{2,1},x_{2,2},\ldots,x_{2,j-1},\ldots,x_{m,1},x_{m,2},\ldots,x_{m,j-1}$ 为变量的布尔函数.

设函数 $f'(x)=f(x\oplus\alpha)$,且函数 f'的第 $i(1\leqslant i\leqslant m)$分量为 f_i'.再记 f_i' 的二进制表示中的第 j 比特为 $f_{i,j}'(1\leqslant j\leqslant n)$,则由引理 1 可知:

$$f_{i,j}'(x)=\bigoplus_{k=1}^{m}c_k(f_i)(x_{k,j}\oplus\alpha_{k,j})\oplus l_{i,j}'(x_{1,1},x_{1,2},...,x_{1,j-1},x_{2,1},x_{2,2},...,x_{2,j-1},...,x_{m,1},x_{m,2},...,x_{m,j-1}).$$

因而有 $f_{i,j}(x)\oplus f_{i,j}'(x)=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,j}\oplus l_{i,j}\oplus l_{i,j}'$.特别地,有 $f_{i,1}(x)\oplus f_{i,1}'(x)=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,1}$.

再设$\alpha,\beta\in(Z/(2^n))^m$且$\alpha\neq 0$,使 $p_{(f)}(\alpha\to\beta)\neq 0$,则有

$$p_{(f)}(\alpha\to\beta)=\frac{1}{2^{mn}}\#\{x\in(Z/(2^n))^m:f_1(x)\oplus f_1'(x)=\beta_1,...,f_m(x)\oplus f_m'(x)=\beta_m\}$$

$$=\frac{1}{2^{mn}}\#\{x\in(Z/(2^n))^m:f_{i,j}(x)\oplus f_{i,j}'(x)=\beta_{i,j},1\leqslant i\leqslant m,0\leqslant j\leqslant n-1\}.$$

并且存在 $x\in\{0,1\}^{mn}$ 使得 mn 个等式成立.由$\alpha\neq 0$ 可知,存在 i,j 使$\alpha_{i,j}\neq 1$,记$\theta=\min\{j:\alpha_{i,j}=1,1\leqslant j\leqslant n,1\leqslant i\leqslant m\}$,则对于$\forall i$,当 $j<\theta$时,均有$\alpha_{i,j}=0$.于是,对于 $1\leqslant i\leqslant m,j\leqslant\theta$有 $l_{i,j}=l_{i,j}'$,故当 $j\leqslant\theta$时,有

$$f_{i,j}(x)\oplus f_{i,j}'(x)=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,j}\oplus l_{i,j}\oplus l_{i,j}'=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,j}=\beta_{k,j}.$$

当 $j<\theta$时,由于$\forall i$ 均有$\alpha_{i,j}=0$,故有 $\beta_{i,j}=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,j}=0$ 和 $\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,\theta}=\beta_{i,\theta}$.证毕. □

下面给出模 2^n 加和模 2 加混合运算的异或差分分支数的计算定理.

定理 3. 设 $f:(Z/(2^n))^m\to(Z/(2^n))^m$,记 $f=(f_1,f_2,\ldots,f_m)$且对 $1\leqslant i\leqslant m,f_i=(x_1,x_2,\ldots,x_m)$都是 $x_1,x_2,\ldots,x_m$ 的混合运算.令 $g_1,\ldots,g_m:\{0,1\}^m\to\{0,1\}$使得对 $1\leqslant i\leqslant m$,有 $g_i(y_1,...,y_m)=\bigoplus_{k=1}^{m}[n_k(f_i)\bmod 2]y_k$,则 f 的异或差分分支数 $D_f^{(n)}$ 等于 $(g_1,\ldots,g_m)$的异或差分分支数 $D_g^{(1)}$,其中,$n_t(f_i)$为 x_t 在 $f_i=(x_1,\ldots,x_m)$中的出现次数.

证明:设 $1\leqslant i\leqslant m,1\leqslant j\leqslant n$,且 $f_i(x)$的第 j 比特为 $f_{i,j}(x)$,$c_k(f_i)=n_k(f_i)\bmod 2$,则由引理 1 可知:

$$f_{i,j}=\bigoplus_{k=1}^{m}c_k(f_i)x_k^{(j)}\oplus l_{i,j}(x_1^{(1)},x_1^{(2)},...,x_1^{(j-1)},x_2^{(1)},x_2^{(2)},...,x_2^{(j-1)},...,x_m^{(1)},x_m^{(2)},...,x_m^{(j-1)}),$$

其中,$l_{i,j}$是布尔函数.

设$\alpha\neq 0$ 且 $p_{(f)}(\alpha\to\beta)=\frac{1}{2^{mn}}\#\{x\in(Z/(2^n))^m:f(x)\oplus f(x\oplus\alpha)=\beta\}$,由$\alpha\neq 0$ 可知,存在 i,j 使$\alpha_{i,j}\neq 1$.记

$$\theta=\min\{j:\alpha_{i,j}=1,1\leqslant j\leqslant n,1\leqslant i\leqslant m\},$$

则由引理 3 可得 $p_{(f)}(\alpha\to\beta)\neq 0$ 的必要条件为:对于$\forall i$,当 $j<\theta$时,都有$\beta_{i,j}=0$ 和 $\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,\theta}=\beta_{i,\theta}$.

记$\beta'=(\beta_{1,\theta},\ldots,\beta_{m,\theta})^T,\alpha'=(\alpha_{1,\theta},\ldots,\alpha_{m,\theta})^T$,并记 m 级方阵 $C=(c_{i,j})_{m\times m}$ 为 $c_{i,j}=c_j(f_i)$,则由 $p_{(f)}(\alpha\to\beta)\neq 0$ 和 $\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,\theta}=\beta_{i,\theta}$ 可知,$\beta'=C\alpha'$.由于当α'的第 i 分量$\alpha_{i,\theta}\neq 0$ 时,α的第 i 分量 $\alpha_i=\sum_{k=1}^{n}2^{k-1}\alpha_{i,k}\geqslant 2^{\theta-1}\alpha_{i,\theta}\neq 0$,故有 $W_n(\alpha)\geqslant W_1(\alpha')$.同理,有 $W_n(\beta)\geqslant W_1(\beta')$,从而有:

$$W_n(\alpha)+W_n(\beta)\geqslant W_1(\alpha')+W_1(\beta')=W_1(C\alpha')+W_1(\alpha')\geqslant D_g^{(1)}.$$

故由分支数的定义可知:

$$D_f^{(n)}=\min\{W_n(\alpha)+W_n(\beta):\alpha\neq 0,p_{(f)}(\alpha\to\beta)\neq 0\}\geqslant D_g^{(1)}.$$

下面来证 $D_f^{(n)}\leqslant D_g^{(1)}$.设 $a\in\{0,1\}^m\backslash\{0\}$,使得 $W_1(Ca)+W_1(a)=D_g^{(1)}$,令 $b=Ca$,当 $1\leqslant i\leqslant m$ 时,取$\alpha,\beta\in(Z/(2^n))^m$,使得$\alpha_{i,n}=a_i,\beta_{i,n}=b_i$,并且对 $1\leqslant j\leqslant n-1,1\leqslant i\leqslant m$,有$\alpha_{i,j}=\beta_{i,j}=0$.

记 $f'(x)=f(x\oplus\alpha)$,且 f'的第 i 分量为 f_i',f_i' 的二进制表示中的第 j 比特为 $f_{i,j}'$,则由引理 1 可知:

$$f'_{i,j}(x)=\bigoplus_{k=1}^{m}c_k(f_i')(x_{k,j}\oplus\alpha_{k,j})\oplus l'_{i,j}(x_{1,1},x_{1,2},...,x_{1,j-1},x_{2,1},x_{2,2},...,x_{2,j-1},...,x_{m,1},x_{m,2},...,x_{m,j-1}),$$

并且由于 $f'(x)=f(x\oplus\alpha)$,则对于 $1\leqslant k\leqslant m$,有 $c_k(f_i')=c_k(f_i)$.

下证对任意 $x\in(Z/(2^n))^m$,$f'(x)\oplus=f(x)=\beta$恒成立.设 $1\leqslant i\leqslant m$,$x\in(Z/(2^n))^m$,则当 $1\leqslant j\leqslant n-1$ 时,由于$\alpha_{i,j}=0$,因此,

$$f'_{i,j}(x)=\bigoplus_{k=1}^{m}c_k(f_i)x_{k,j}\oplus l_{i,j}(x_{1,1},x_{1,2},...,x_{1,j-1},x_{2,1},x_{2,2},...,x_{2,j-1},...,x_{m,1},x_{m,2},...,x_{m,j-1})\text{且}l_{i,n}=l'_{i,n}.$$

从而当 $1\leqslant j\leqslant n-1$ 时, $f_{i,j}(x)\oplus f'_{i,j}(x)=0=\beta_{i,j}$ 恒成立.

当 $j=n$ 时,

$$\begin{aligned}f_{i,n}(x)\oplus f'_{i,n}(x)&=\bigoplus_{k=1}^{m}c_k(f_i')(x_{k,j}\oplus\alpha_{k,j})\oplus\bigoplus_{k=1}^{m}c_k(f_i)x_{k,j}\oplus l_{i,n}\oplus l'_{i,n}\\&=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,n}\oplus l_{i,n}\oplus l'_{i,n}=\bigoplus_{k=1}^{m}c_k(f_i)\alpha_{k,n}\\&=\bigoplus_{k=1}^{m}c_k(f_i)a_k=b_i=\beta_{i,n}\end{aligned}$$

恒成立.故对于任意 $x\in(Z/(2^n))^m$,$f'(x)\oplus=f(x)=\beta$恒成立.即此时有 $p_{(f)}(\alpha\to\beta)=1$.再由 $W_n(\alpha)=W_1(a)$和 $W_n(\beta)=W_1(b)$及 $D_f^{(n)}$ 的定义可知:

$$D_f^{(n)}\leqslant W_n(\alpha)+W_n(\beta)=W_1(a)+W_1(b)=D_g^{(1)}.$$

这说明 $D_f^{(n)}=D_g^{(1)}$. 证毕. □

2.2 模2^n加和模2加混合运算的异或线性分支数

本节我们将给出模 2^n 加和模 2 加混合运算的异或线性分支数的计算,首先给出二元域上线性变换异或线性分支数的计算,并且给出模 2^n 加和模 2 加混合运算的异或差分分支数的计算及其一些推论.

引理 4[9]. 设 x 和 y 均是有限域 F 上的随机变量,且 x 在 F 上服从均匀分布,则 x 与 y 独立的充要条件是对于 F 上的非零元 a,$ax+y$ 都在 F 上服从均匀分布.

下面给出混合运算的异或线性分支数的计算定理.

定理 4. 设 $f:(Z/(2^n))^m\to(Z/(2^n))^m$,记 $f=(f_1,f_2,\ldots,f_m)$且对 $1\leqslant i\leqslant m$,f_i 都是 $x_1,x_2,\ldots,x_m$ 的混合运算.令 $g_1,\ldots,g_m:\{0,1\}^m\to\{0,1\}$使得对 $1\leqslant i\leqslant m$,有 $g_i(y_1,...,y_m)=\bigoplus_{k=1}^{m}[(n_k(f_i)\bmod 2)y_k]$,则 f 的异或线性分支数 $L_f^{(n)}$ 等于$(g_1,\ldots,g_m)$的异或线性分支数 $L_g^{(1)}$.

证明:设 $1\leqslant i\leqslant m$,$1\leqslant j\leqslant n$,且 $f_i(x)$的第 j 比特为 $f_{i,j}(x)$,$c_k(f_i)=n_k(f_i)\bmod 2$,则由引理 1 可知:

$$f_{i,j}=\bigoplus_{k=1}^{m}c_k(f_i)x_{k,j}\oplus l_{i,j}(x_{1,1},x_{1,2},...,x_{1,j-1},x_{2,1},x_{2,2},...,x_{2,j-1},...,x_{m,1},x_{m,2},...,x_{m,j-1}),$$

其中,$l_{i,j}$ 是以 $x_{1,1},x_{1,2},\ldots,x_{1,j-1},x_{2,1},x_{2,2},\ldots,x_{2,j-1},\ldots,x_{m,1},x_{m,2},\ldots,x_{m,j-1}$ 为变量的布尔函数.

现设$\alpha,\beta\in(Z/(2^n))^m$ 且$\beta\neq 0$,使$\rho_{(f)}(\alpha\to\beta)\neq 0$,则有

$$\begin{aligned}\rho_{(f)}(\alpha\to\beta)&=\frac{1}{2^{mn}}\sum_{x\in(Z/(2^n))^m}(-1)^{\beta_1\cdot f_1\oplus\ldots\oplus\beta_m\cdot f_m\oplus\alpha_1\cdot x_1\oplus\ldots\oplus\alpha_m\cdot x_m}\\&=\frac{1}{2^{mn}}\sum_{x\in(Z/(2^n))^m}(-1)^{\left[\bigoplus_{i=1}^{m}\bigoplus_{j=1}^{n}\beta_{i,j}\left(l_{i,j}\oplus\bigoplus_{k=1}^{m}(c_k(f_i)x_{k,j})\right)\right]\oplus\left[\bigoplus_{i=1}^{m}\bigoplus_{j=1}^{n}\alpha_{i,j}x_{i,j}\right]}\\&=\frac{1}{2^{mn}}\sum_{x\in(Z/(2^n))^m}(-1)^{\bigoplus_{j=1}^{n}\bigoplus_{i=1}^{m}\beta_{i,j}\left[\left(l_{i,j}\oplus\bigoplus_{k=1}^{m}(c_k(f_i)x_{k,j})\right)\right]\oplus\left[\bigoplus_{j=1}^{n}\bigoplus_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]}.\end{aligned}$$

记 $h=\bigoplus_{j=1}^{n}\bigoplus_{i=1}^{m}\beta_{i,j}\left[l_{i,j}\oplus\bigoplus_{k=1}^{m}(c_k(f_i)x_{k,j})\right]\oplus\left[\bigoplus_{j=1}^{n}\bigoplus_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]$,则

$$\rho_f(\alpha\to\beta)=\frac{1}{2^{mn}}\sum_{x\in(Z/(2^n))^m}(-1)^h.$$

由$\beta\neq 0$可知,存在i,j使$\beta_{i,j}=1$.令$\theta=\max\{j:\beta_{i,j}=1,1\leqslant j\leqslant n,1\leqslant i\leqslant m\}$,则对于$\forall i$,当$j>\theta$时,均有$\beta_{i,j}=0$.于是有,

$$h=\mathop{\oplus}_{j=1}^{n}\mathop{\oplus}_{i=1}^{m}\beta_{i,j}\left[l_{i,j}\oplus\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,j})\right]\oplus\left[\mathop{\oplus}_{j=1}^{n}\mathop{\oplus}_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]$$

$$=\mathop{\oplus}_{j=1}^{\theta-1}\mathop{\oplus}_{i=1}^{m}\beta_{i,j}\left[l_{i,j}\oplus\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,j})\oplus\alpha_{i,j}x_{i,j}\right]\oplus\mathop{\oplus}_{i=1}^{m}\beta_{i,\theta}l_{i,\theta}\oplus\mathop{\oplus}_{i=1}^{m}(\beta_{i,\theta}\left[\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,\theta})\right]\oplus\alpha_{i,\theta}x_{i,\theta})\oplus\left[\mathop{\oplus}_{j=\theta+1}^{n}\mathop{\oplus}_{i=1}^{m}\alpha_{i,j}x_{i,j}\right].$$

由于函数$\mathop{\oplus}_{j=1}^{\theta-1}\mathop{\oplus}_{i=1}^{m}\beta_{i,j}\left[l_{i,j}\oplus\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,j})\oplus\alpha_{i,j}x_{i,j}\right]\oplus\mathop{\oplus}_{i=1}^{m}\beta_{i,\theta}l_{i,\theta}$只与集合$\{x_{i,j}:1\leqslant i\leqslant m,1\leqslant j<\theta\}$中的变量有关,而与其他变量无关,因而它与线性函数

$$\psi=\mathop{\oplus}_{i=1}^{m}\left(\beta_{i,\theta}\left[\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,\theta})\right]\oplus\alpha_{i,\theta}x_{i,\theta}\right)\oplus\left[\mathop{\oplus}_{j=\theta+1}^{n}\mathop{\oplus}_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]$$

$$=\mathop{\oplus}_{i=1}^{m}\left[\mathop{\oplus}_{k=1}^{m}(\beta_{i,\theta}c_k(f_i)x_{k,\theta})\right]\oplus\mathop{\oplus}_{i=1}^{m}\alpha_{i,\theta}x_{i,\theta}\oplus\left[\mathop{\oplus}_{j=\theta+1}^{n}\mathop{\oplus}_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]$$

$$=\mathop{\oplus}_{k=1}^{m}\left[\mathop{\oplus}_{i=1}^{m}(\beta_{i,\theta}c_k(f_i)x_{k,\theta})\oplus\alpha_{k,\theta}x_{k,\theta}\right]\oplus\left[\mathop{\oplus}_{j=\theta+1}^{n}\mathop{\oplus}_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]$$

独立.如果线性函数ψ不是零值函数,则ψ一定是平衡函数.故由引理 4 可知,h是平衡函数,此时有$\rho_{(f)}(\alpha\to\beta)=0$.故$\rho_{(f)}(\alpha\to\beta)\neq 0$的必要条件是$\psi$为零值函数,即以下两个条件同时成立:

(1) $\forall k:1\leqslant k\leqslant m$,有$\mathop{\oplus}_{i=1}^{m}(\beta_{i,\theta}c_k(f_i))=\alpha_{k,\theta}$;

(2) 当$j>\theta$时,对$1\leqslant i\leqslant m$,均有$\alpha_{i,j}=0$.

现取$\alpha'=(\alpha_{1,\theta},\ldots,\alpha_{m,\theta}),\beta'=(\beta_{1,\theta},\ldots,\beta_{m,\theta})^T\in\{0,1\}^m$,则$\beta'\neq 0$.再令$m$级方阵$C=(c_{i,j})_{m\times m}$为$c_{i,j}=c_j(f_i)$,则由$\rho_{(f)}(\alpha\to\beta)\neq 0$可知条件(1)成立,即$\alpha'=C^T\beta'$.

由于当β'的第 i 分量$\beta_{i,\theta}\neq 0$ 时,β的第 i 分量$\beta_i=\sum_{k=1}^{n}2^{k-1}\beta_{i,k}\geqslant 2^{\theta-1}\beta_{i,\theta}\neq 0$,故有 $W_n(\beta)\geqslant W_1(\beta')$.同理,有$W_n(\alpha)\geqslant W_1(\alpha')$.从而

$$W_n(\alpha)+W_n(\beta)\geqslant W_1(\alpha')+W_1(\beta')=W_1(C^T\beta')+W_1(\beta')\geqslant L_g^{(1)}.$$

故有

$$L_f^{(n)}=\min\{W_n(\alpha)+W_n(\beta):\beta\neq 0,\rho_{(f)}(\alpha\to\beta)\neq 0\}\geqslant L_g^{(1)}.$$

下面来证$L_f^{(n)}\leqslant L_g^{(1)}$.设 $b\in\{0,1\}^m\backslash\{0\}$,使得$W_1(M^Tb)+W_1(b)=L_g^{(1)}$,令 $a=C^Tb$,并取$\alpha,\beta\in(Z/(2^n))^m$,使得$\alpha_i=a_i,\beta_i=b_i$对$1\leqslant i\leqslant m$成立,则有$\rho_{(f)}(\alpha\to\beta)=\frac{1}{2^{mn}}\sum_{x\in(Z/(2^n))^m}(-1)^h$,其中,

$$h=\mathop{\oplus}_{j=1}^{n}\mathop{\oplus}_{i=1}^{m}\beta_{i,j}\left[l_{i,j}\oplus\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,j})\right]\oplus\left[\mathop{\oplus}_{j=1}^{n}\mathop{\oplus}_{i=1}^{m}\alpha_{i,j}x_{i,j}\right]$$

$$=\mathop{\oplus}_{i=1}^{m}\beta_{i,1}\left[\mathop{\oplus}_{k=1}^{m}(c_k(f_i)x_{k,1})\right]\oplus\mathop{\oplus}_{i=1}^{m}\alpha_{i,1}x_{i,1}$$

$$=\mathop{\oplus}_{i=1}^{m}\mathop{\oplus}_{k=1}^{m}[c_k(f_i)\beta_{i,1}x_{k,1}]\oplus\mathop{\oplus}_{i=1}^{m}\alpha_{i,1}x_{i,1}$$

$$=\mathop{\oplus}_{k=1}^{m}\alpha_{k,1}\oplus\mathop{\oplus}_{i=1}^{m}[c_k(f_i)\beta_{i,1}]x_{k,1}$$

$$=\mathop{\oplus}_{k=1}^{m}a_k\oplus\mathop{\oplus}_{i=1}^{m}[c_k(f_i)b_i]x_{k,1}=0.$$

故有$\rho_{(f)}(\alpha\to\beta)=1$.再由$W_n(\alpha)=W_1(a),W_n(\beta)=W_1(b)$及$L_f^{(n)}$的定义可知

$$L_f^{(n)}\leqslant W_n(\alpha)+W_n(\beta)=W_1(a)+W_1(b)=L_g^{(1)}.$$

这说明$L_f^{(n)}=L_g^{(1)}$.证毕. □

推论 1. 设$f:(Z/(2^n))^m\to(Z/(2^n))^m$,记$f=(f_1,f_2,\ldots,f_m)$且对$1\leqslant i\leqslant m,f_i$都是$x_1,x_2,\ldots,x_m$的混合运算,则$f$的异或差

分分支数 $D_f^{(n)}$ 和线性分支数 $L_f^{(n)}$ 分别等于将 f 中的模 2^n 加换为模 2 加且将奇系数换成 1、偶系数换成 0 所得的二元域上线性变换 g 的异或差分分支数 $D_g^{(n)}$ 和异或线性分支数 $L_g^{(n)}$.

推论 2. 设 $f:(Z/(2^n))^m\to(Z/(2^n))^m$,记 $f=(f_1,f_2,\ldots,f_m)$且对 $1\leqslant i\leqslant m$,$f_i=(x_1,x_2,\ldots,x_m)$都是 $x_1,x_2,\ldots,x_m$ 的混合运算,则当 m=2 时,有 $D_f^{(n)}\leqslant 2$ 和 $L_f^{(n)}\leqslant 2$;当 m=8 时,有 $D_f^{(n)}\leqslant 5$ 和 $L_f^{(n)}\leqslant 5$;当 m=16 时,有 $D_f^{(n)}\leqslant 8$ 和 $L_f^{(n)}\leqslant 8$.

证明:设 $g:\{0,1\}^m\to\{0,1\}^m$ 是二元域上的线性变换.当 m=2 时,对穷举所有 g 并计算 $D_g^{(1)},L_g^{(1)}$,可知 $D_g^{(1)}\leqslant 2$,$L_g^{(1)}\leqslant 2$;再由文献[8]可知,当 m=8 时,有 $D_g^{(1)}\leqslant 5,L_g^{(1)}\leqslant 5$;当 m=16 时,有 $D_g^{(1)}\leqslant 8,L_g^{(1)}\leqslant 8$,从而由定理 3、定理 4 可知,推论 2 成立.证毕. □

定理 3、定理 4 通过将模 2^n 加和模 2 加混合运算的异或分支数归结为二元域上线性变换的分支数的方法,解决了其异或分支数的计算问题.SPS 模型中,P 变换的异或分支数反映了该模型抗差分攻击和线性分析的最低能力.与二元域上的线性变换不同,对于混合运算 f,$p_{(f)}(u\to v)\neq 0,\rho_{(f)}(u\to v)\neq 0$ 可能意味着 $p_{(f)}(u\to v),|\rho_{(f)}(u\to v)|$远小于 1,因而对 SPS 模型的差分链和线性逼近链的实际概率与优势远比按 $p_{(f)}(u\to v)=1$ 估计的要小,因而该模型抗差分和线性攻击的实际能力可以更强.

3 结束语

本文给出了扩散结构为二元域上的非线性变换的异或分支数的一个定义及其与分组密码抗差分攻击和线性分析能力的关系,并将以模 2^n 加和模 2 加混合运算为扩散结构的异或分支数归结为二元域上线性变换的异或分支数的计算.本文的研究结果对于评估以 SPS 模型为基础设计的分组密码抗差分攻击和线性分析的最低能力有实际的应用价值.SPS 模型所得研究结果在分析实际密码算法中的应用,以及扩散结构 P 的小于 1 的非零概率对抗差分和线性攻击的实际能力影响等,是需要进一步研究的问题.

References:

[1] Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis [Ph.D. Thesis]. Brussel: Katholieke Universiteit Leuven, 1995.

[2] Hong S, Lee S, Lim J, Sung J, Cheon D, Cho I. Provable security against differential and linear cryptanalysis for the SPN structure. In: Bruce S, ed. Proc. of the 7th Int'l Workshop, Fast Software Encryption 2000. LNCS 1978, New York: Springer-Verlag, 2000. 273−283. [doi: 10.1007/3-540-44706-7_19]

[3] Nicolas T. The best differential characteristics and subtleties of the Biham-Shamir attacks on DES. 2005. http://eprint.iacr.org/2005/202

[4] Kanda M. Practical security evaluation against differential and linear cryptanalyses for Feistel ciphers with SPN round function. In: Douglas R, Stafford T, eds. Proc. of the 7th Annual Int'l Workshop on Selected Areas in Cryptography. LNCS 2012, Ontario: Springer-Verlag, 2001. 324−338. [doi: 10.1007/3-540-44983-3_24]

[5] Zhang WT, Qing SH, Wu WL. Provable security for SPN block ciphers containing Feistel structure. Journal of Computer Research and Development, 2004,41(8):1389−1397 (in Chinese with English abstract).

[6] Wang NP. Security analysis for a class of generalized Feistel ciphers. Journal of Dalian Maritime University, 2007,33(3):63−67 (in Chinese with English abstract).

[7] Wang NP, Jin CH, Yu ZP. Furthermore analyses of linear provable security for a class of unbalanced Feistel networks. Acta Electronica Sinica, 2006,34(10):1799−1802 (in Chinese with English abstract).

[8] Kang JS, Hong S, Lee SJ, Yi O, Park C, Lim J. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. ETRI Journal, 2001,23(4):158−167. [doi: 10.4218/etrij.01.0101.0402]

[9] Jin CH. Spectra characterizations of nonsigular feedback polynomials over finite fields and residue class rings. Journal of China Institute of Communications, 2000,21(1):74−77 (in Chinese with English abstract).

附中文参考文献:

[5] 张文涛,卿斯汉,吴文玲.嵌套 Feistel 结构的 SP 型分组密码的可证明安全性.计算机研究与发展,2004,41(8):1389–1397.

[6] 王念平.一类广义 Feistel 密码的安全性能分析.大连海事大学学报,2007,33(3):63–67.

[7] 王念平,金晨辉,余昭平.非平衡 Feistel 网络的线性可证明安全性的进一步分析.电子学报,2006,34(10):1799–1802.

[9] 金晨辉.有限域和剩余类环上非奇异反馈多项式的谱刻划.通信学报,2000,21(1):74–77.

常亚勤(1980－),女,河南郑州人,博士生,主要研究领域为密码学.

金晨辉(1965－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.