计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2016.20148270
53(3):666-673,2016

对 8 轮 mCrypton-96 的中间相遇攻击

王高丽[1,2]　　甘　楠[2]
[1](华东师范大学计算机科学与软件工程学院　上海　200062)
[2](东华大学计算机科学与技术学院　上海　201620)
(glwang@sei.ecnu.edu.cn)

A Meet-in-the-Middle Attack on 8-Round mCrypton-96

Wang Gaoli[1,2] and Gan Nan[2]
[1](*School of Computer Science and Software Engineering*, *East China Normal University*, *Shanghai* 200062)
[2](*School of Computer Science and Technology*, *Donghua University*, *Shanghai* 201620)

Abstract　mCrypton is a lightweight block cipher introduced in Information Security Application 2006 by Lim and Korkishko. mCrypton-64/96/128 denote 3 versions of the cipher with 64/96/128 b keys respectively. In this paper, we apply the meet-in-the-middle (MITM) attack on 8-round mCrypton-96, which improves the best MITM attack result on mCrypton-96 by 1 round. When analyzing the security of block ciphers, using key relations to reduce the time complexity, memory complexity and data complexity is a common method. From the property of the key schedule of mCrypton-96, we know that each round key could calculate some information of the internal register by the algebraic structure of the key schedule, and some round keys could be deduced from the other round keys. By using the relationship of key schedule and the properties of S-box, we present a MITM attack on 8-round mCrypton-96 based on the 4-round distinguisher by adding 1 round on the top and 3 rounds at the bottom. The time, memory and data complexities of the attack are $2^{93.5}$ encryptions, 2^{47} B and 2^{57} chosen plaintexts respectively. It is illustrated that mCrypton-96 not only has an efficient performance but also possesses strong security.

Key words　cryptanalysis; meet-in-the-middle (MITM) attack; block ciphers; mCrypton; relationship of keys

摘　要　在分析分组密码算法的安全性时,利用密钥关系来降低时间、存储和数据复杂度是一个常用的手段.在 4 轮 mCrypton-96 性质的基础上,利用密钥生成算法的弱点和 S 盒的性质,降低了攻击过程中需要猜测的密钥比特数,提出了对 8 轮 mCrypton-96 算法的中间相遇攻击,攻击的时间复杂度约为 $2^{93.5}$ 次 8 轮 mCrypton-96 加密运算,存储复杂度为 2^{47} B,数据复杂度为 2^{57} 个选择明文.

关键词　密码算法分析;中间相遇攻击;分组密码;mCrypton;密钥关系

中图法分类号　TP309

分组密码算法在现代密码学中有着举足轻重的地位,1997—2000 年美国高级加密标准(advance encryption stand, AES)算法征集活动大大促进了分组密码算法的设计和分析.继美国新一代加密算

收稿日期:2014-11-20;**修回日期**:2015-07-06

基金项目:国家自然科学基金项目(61572125,61373142);东华大学硕士研究生学位论文创新资助项目(112-06-0019025)
This work was supported by the National Natural Science Foundation of China (61572125, 61373142) and the Postgraduate Dissertation Innovation Funds of Donghua University (112-06-0019025).

法标准确定之后,欧洲、日本和韩国等多国都开始各自征集密码算法标准,这将分组密码的分析和设计推向了一个高潮. 最近,轻量级分组密码算法由于它的密钥关系更简单、使用的电脑硬件资源更少、加密速度优于一般的分组密码算法而广泛用于资源受限的环境,如射频识别卡(radio frequency identification, RFID)和嵌入式环境. 轻量级分组密码算法 LED, Zorro, mCrypton, PRESENT, Piccolo, Klein, XTEA, DESL, HIGHT, CLEFIA, Twine, KATAN, 轻量级流密码算法 Grain 和 Trivium,以及基于 PRESENT 的轻量级杂凑函数等算法的出现大大促进了轻量级密码的发展. 与此同时,出现了许多对于轻量级分组密码算法的分析方法.

1977 年 Diffie 和 Hellman[1] 首次提出了中间相遇攻击方法. Henri 和 Minier[2] 在 2000 年改进了对于 AES 算法的中间相遇攻击结果,根据 4 轮 AES 算法的性质,给出了 7 轮 AES 算法的中间相遇攻击. Demirci, Selcuk[3] 在 2008 年在 5 轮 AES 算法差分性质的基础上,用中间相遇攻击方法进一步改进了对 8 轮 AES-256 的分析结果. 其中,5 轮 AES 算法的性质是由 4 轮性质发展而来的. 2010 年, Dunkelman, Keller 等人[4] 改进了对于 7/8 轮 AES-192 和 AES-256 的分析结果. 2013 年, Derbez, Fouque, Jean[5] 改进了对于 7 轮 AES-128 的中间相遇攻击结果,并且给出了对于 8 轮 AES-192, AES-256 的攻击. 2014 年,李雷波、王小云等人[6] 利用密钥生成算法的性质改进了 5 轮 AES 的性质,给出了对 AES-192 的 9 轮中间相遇攻击. 另外,文献[7-12]给出了对于其他分组密码算法的中间相遇攻击.

2006 年, Lim 和 Korkishko[13] 提出了 mCrypton 算法,它是一个典型的轻量级分组密码算法. mCrypton 是 Crypton 算法的缩减版,采用 SPN 结构,包含 3 个版本,密钥长度分别为 64 b, 96 b, 128 b.

文献[14]提出了对 7 轮 mCrypton-96/64 和对 8/9 轮 mCrypton-128 的中间相遇攻击;文献[15]采用 Biclique 技术给出了全轮 mCrypton-64/96/128 的分析结果;文献[16]给出了 8 轮 mCrypton-96/128 的碰撞攻击;文献[17]给出了 9 轮 mCrypton-96/128 的相关密钥不可能差分分析;文献[18]采用 Biclique 技术给出了全轮 mCrypton-96/128 的分析结果;文献[19]给出了 8 轮 mCrypton-128 的相关密钥矩形攻击. 本文利用密钥生成算法的性质,根据 4 轮性质,给出了对 8 轮 mCrypton-96 算法的中间相遇攻击.

1 符号说明

$\boldsymbol{U}$:$(\boldsymbol{U}_0,\boldsymbol{U}_1,\boldsymbol{U}_2,\boldsymbol{U}_3,\boldsymbol{U}_4,\boldsymbol{U}_5)$,每个 $\boldsymbol{U}_r$ 表示 16 b;

$\boldsymbol{U}_r[15,14,13,12,11,10,9,8,7,6,5,4,3,2,1,0]$:16 b,$\boldsymbol{U}_r$ 的第 0 位在最右边;

$\boldsymbol{U}_r^{<<<i}$:$\boldsymbol{U}_r$ 循环左移 i 位;

$\boldsymbol{K}_r$:第 r 轮的轮密钥;

$\boldsymbol{u}_r$:表示第 r 轮的轮密钥经过转置和列混合之后的状态;

$\boldsymbol{u}_{r,k}$:表示 $\boldsymbol{u}_r$ 的第 k 个半字节(4 b);

$\oplus$:"异或"运算;

$\cdot$:"与"运算;

$\Delta\boldsymbol{X}$:$\boldsymbol{X}\oplus\boldsymbol{X}'$;

$\boldsymbol{x}_{i,k}^j$:$\boldsymbol{x}_i^j$ 的第 k 个单元(字节或者半字节);

$\boldsymbol{x}_{i,\{k,m\}}^j$:$\boldsymbol{x}$ 的第 k 个和第 m 个单元(字节或者半字节).

2 mCrypton 算法

2.1 加密运算

mCrypton 算法是基于代换-置换网络(substitution permutation network, SPN)结构的 64 b 的轻量级分组密码算法,包含 3 个版本,密钥长度分别为 64 b, 96 b, 128 b,这 3 个版本都是 12 轮. 如矩阵 $\boldsymbol{A}$ 所示,将 64 b 的明文分组排列成 4×4 的矩阵,其中每个 a_i 为 4 b.

$$\boldsymbol{A}=\begin{pmatrix} a_0 & a_1 & a_2 & a_3\\ a_4 & a_5 & a_6 & a_7\\ a_8 & a_9 & a_{10} & a_{11}\\ a_{12} & a_{13} & a_{14} & a_{15}\end{pmatrix}.$$

S 盒 γ:mCrypton 的 S 盒运算包含 4 个 4×4 S 盒: S_0, S_1, S_2, S_3,其中 $S_0=S_2^{-1}$, $S_1=S_3^{-1}$. 设 S 盒的输入为 $\boldsymbol{A}$,则其输出为

$$S(\boldsymbol{A})=\begin{pmatrix} S_0(a_0) & S_1(a_1) & S_2(a_2) & S_3(a_3)\\ S_1(a_4) & S_2(a_5) & S_3(a_6) & S_0(a_7)\\ S_2(a_8) & S_3(a_9) & S_0(a_{10}) & S_1(a_{11})\\ S_3(a_{12}) & S_0(a_{13}) & S_1(a_{14}) & S_2(a_{15})\end{pmatrix}.$$

比特置换 π:比特置换与算法的列混合运算有相同的功能,对于矩阵 $\boldsymbol{A}$ 的每一列分别做比特置换.

设矩阵 $\boldsymbol{A}=(\boldsymbol{A}_0,\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_3)$,则经比特置换后的输出为 $\pi(\boldsymbol{A})=(\pi_0(\boldsymbol{A}_0),\pi_1(\boldsymbol{A}_1),\pi_2(\boldsymbol{A}_2),\pi_3(\boldsymbol{A}_3))$. 其中,$\pi_i$ 定义如下:令 $\boldsymbol{a}=(\boldsymbol{a}_0,\boldsymbol{a}_1,\boldsymbol{a}_2,\boldsymbol{a}_3)=\boldsymbol{A}_i(0\leqslant i\leqslant 3)$,则经过 π_i 变换后的输出为 $\boldsymbol{b}=(\boldsymbol{b}_0,\boldsymbol{b}_1,\boldsymbol{b}_2,\boldsymbol{b}_3)$,其中:

$$\boldsymbol{b}=\pi_i(\boldsymbol{a})\Leftrightarrow\boldsymbol{b}_j=\bigoplus_{k=0}^{3}(m_{(i+j+k)\bmod 4}\cdot\boldsymbol{a}_k),$$

$m_0=1110_2,m_1=1101_2,m_2=1011_2,m_3=0111_2$.

转置 τ:将矩阵的行列互换. 例如矩阵 $\begin{pmatrix}a_0&a_1\\a_2&a_3\end{pmatrix}$ 经转置变换后的输出为 $\tau\begin{pmatrix}a_0&a_1\\a_2&a_3\end{pmatrix}=\begin{pmatrix}a_0&a_2\\a_1&a_3\end{pmatrix}$.

密钥加:设输入为$(\boldsymbol{A},\boldsymbol{K})$,其中:

$$\boldsymbol{A}=\begin{pmatrix}a_0&a_1&a_2&a_3\\a_4&a_5&a_6&a_7\\a_8&a_9&a_{10}&a_{11}\\a_{12}&a_{13}&a_{14}&a_{15}\end{pmatrix},$$

$$\boldsymbol{K}=\begin{pmatrix}k_0&k_1&k_2&k_3\\k_4&k_5&k_6&k_7\\k_8&k_9&k_{10}&k_{11}\\k_{12}&k_{13}&k_{14}&k_{15}\end{pmatrix},$$

则经过密钥加运算后的输出为

$$\boldsymbol{A}\oplus\boldsymbol{K}=\begin{pmatrix}a_0\oplus k_0&a_1\oplus k_1&a_2\oplus k_2&a_3\oplus k_3\\a_4\oplus k_4&a_5\oplus k_5&a_6\oplus k_6&a_7\oplus k_7\\a_8\oplus k_8&a_9\oplus k_9&a_{10}\oplus k_{10}&a_{11}\oplus k_{11}\\a_{12}\oplus k_{12}&a_{13}\oplus k_{13}&a_{14}\oplus k_{14}&a_{15}\oplus k_{15}\end{pmatrix},$$

其中,$a_i,k_i(0\leqslant i\leqslant 15)$的长度都是 4 b.

综上所述,mCrypton 算法的 1 轮加密过程为:$\rho_{k_r}(x)=\sigma_{k_r}\circ\tau\circ\pi\circ\gamma(\boldsymbol{x})$. 经过 12 轮运算后,再经过 $\tau\circ\pi\circ\tau$ 运算,即可得密文.

2.2 96 位密钥生成规则

首先,$\boldsymbol{U}=(\boldsymbol{U}_0,\boldsymbol{U}_1,\boldsymbol{U}_2,\boldsymbol{U}_3,\boldsymbol{U}_4,\boldsymbol{U}_5)=\boldsymbol{K}$,其中 $\boldsymbol{K}$ 为主密钥,则轮密钥 $\boldsymbol{K}_r$ 的生成过程如下:

1) $\boldsymbol{T}=\boldsymbol{S}(\boldsymbol{U}_0)\oplus C_r,\boldsymbol{T}_i=\boldsymbol{T}\cdot\boldsymbol{M}_i$,

其中,$M_0=$0xf000,$M_1=$0x0f00,$M_2=$0x00f0,$M_3=$0x000f.

2) $\boldsymbol{K}_r=\begin{pmatrix}\boldsymbol{U}_1\oplus\boldsymbol{T}_0\\\boldsymbol{U}_2\oplus\boldsymbol{T}_1\\\boldsymbol{U}_3\oplus\boldsymbol{T}_2\\\boldsymbol{U}_4\oplus\boldsymbol{T}_3\end{pmatrix}$.

3) $\boldsymbol{U}=(\boldsymbol{U}_5,\boldsymbol{U}_0^{<<<3},\boldsymbol{U}_1,\boldsymbol{U}_2,\boldsymbol{U}_3^{<<<8},\boldsymbol{U}_4)$.

3 中间相遇攻击

3.1 经典的中间相遇攻击

将分组密码算法分成 2 个部分 E_1 和 E_2. E_1 所用的密钥为 $\boldsymbol{K}_1$,E_2 所用的密钥为 $\boldsymbol{K}_2$,遍历 $\boldsymbol{K}_1$,将明文 $\boldsymbol{P}$ 经过 E_1 加密得到 $E_1(\boldsymbol{P})$,并将其存入表 T_1. 遍历 $\boldsymbol{K}_2$,将相应的密文 $\boldsymbol{C}$ 经过 E_2 解密,得到 $D_2(\boldsymbol{C})$. 检测 $D_2(\boldsymbol{C})$的值是否存在表 T_1 中,如果存在,则密钥$(\boldsymbol{K}_1,\boldsymbol{K}_2)$为候选密钥. 重新选取明文,继续上述步骤,直到候选密钥唯一确定.

3.2 对 AES 的中间相遇攻击

由于 mCrypton 算法和 AES 类似,对 AES 中间相遇攻击的研究可以作为参考. 文献[3]给出 4 轮 AES 性质,并在 4 轮性质前加 1 轮,后面加 2 轮,给出了 7 轮 AES 的中间相遇攻击.

定义 1. δ 集是 $\boldsymbol{x}$ 除去某个特定单元(特定单元值遍历 0,1,…,2^n-1),其他单元都是常数的 2^n 个明文组成的集合,其中 n 为数据单元的二进制长度.

性质 1. 4 轮 AES 性质. 令 δ 集$\{\boldsymbol{x}_1^0,\boldsymbol{x}_1^1,\boldsymbol{x}_1^2,\cdots,\boldsymbol{x}_1^{255}\}$经过 4 轮 AES 加密的输出为$\{\boldsymbol{x}_5^0,\boldsymbol{x}_5^1,\boldsymbol{x}_5^2,\cdots,\boldsymbol{x}_5^{255}\}$,则有序序列$\{\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^0,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^1,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^2,\cdots,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^{255}\}$的值取决于 25 个字节,所以有序序列$\{\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^0,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^1,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^2,\cdots,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^{255}\}$最多有 2^{200} 种可能的取值. 而在随机情况下,其有 2^{2048} 种取值.

预计算过程:

将$\{\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^0,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^1,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^2,\cdots,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^{255}\}$所有可能的 2^{200} 种取值计算出来,并存在一个 Hash 表 T 中.

攻击过程:

如图 1 所示,首先选择相应的明文,猜测前 1 轮和后 2 轮的相关密钥,排除掉一些不符合情况的明文对,剩下的每 1 个明文对构造 1 个 δ 集,将 δ 集的密文部分解密,计算出$\{\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^0,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^1,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^2,\cdots,\boldsymbol{x}_{5,i}^0\oplus\boldsymbol{x}_{5,i}^{255}\}$的值. 最后,查 Hash 表 T,如果这个有序序列的值在 Hash 表 T 中,则相应猜测的密钥是候选密钥,穷举搜索其余的密钥.

2008 年,Demirci 和 Selcuk[3] 提出了 5 轮 AES 的性质,并给出了 7 轮 AES-192 和 8 轮 AES-256 的中间相遇攻击. 2010 年,Dunkelman,Keller 等人[4] 把 4 轮 AES 性质中的有序序列推广到了多重集,且相应的多重集的值取决于 16 个字节,即最多有 2^{128}

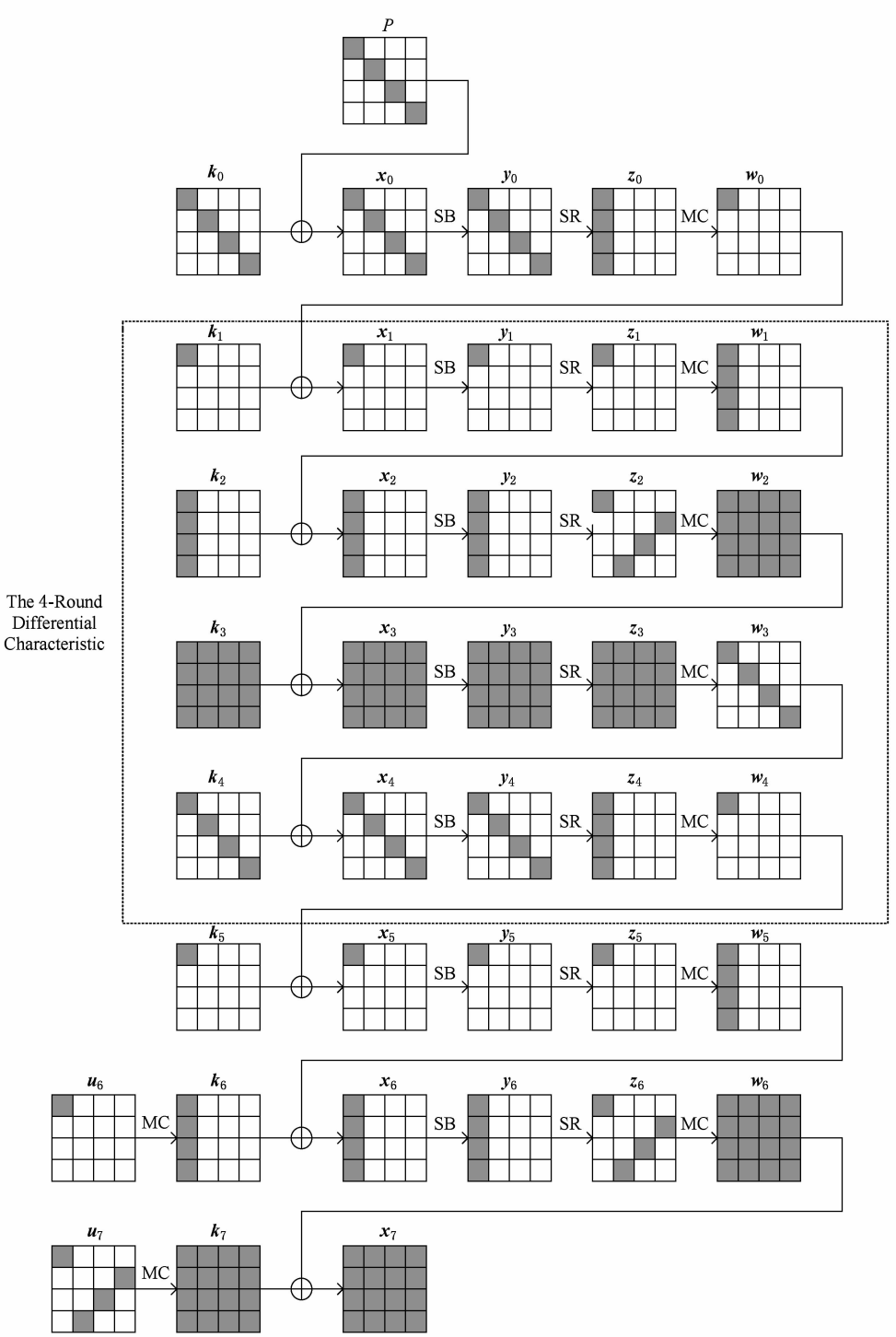

Fig. 1 Meet in the middle attack on 7-round AES in Ref[3].

图 1 文献[3]对 7 轮 AES 的攻击

种可能的取值. 而在随机情况下,其有 $\binom{510}{255}$ 种可能的取值. 多重集的提出和应用不但大大降低了预计算量,而且降低了攻击的时间复杂度.

2013 年,Derbez, Fouque, Jean[5] 在 4 轮性质中利用 S 盒的差分性质降低了计算多重集所需的参数个数,将多重集可能的取值由 2^{128} 降低到 2^{80}. 因此将攻击 7 轮 AES-128 的时间、空间和数据复杂度都降低到 2^{100} 以下,并成功地改进了对 8 轮 AES-192,AES-256 的分析结果.

2014 年,李雷波、王小云等人[6]利用密钥关系,提出了对 5 轮 AES-192,AES-256 的性质,并在此基础上首次给出了对 9 轮 AES-192 的中间相遇攻击,同时改进了对 9 轮 AES-256 的分析结果.

4 8 轮 mCrypton-96 的中间相遇攻击

4.1 4 轮 mCrypton 的性质

将 1 个 δ 集 $\{\boldsymbol{x}_0^0, \boldsymbol{x}_0^1, \boldsymbol{x}_0^2, \cdots, \boldsymbol{x}_0^{15}\}$，经过 4 轮 mCrypton 加密得到输出 $\{\boldsymbol{x}_5^0, \boldsymbol{x}_5^1, \boldsymbol{x}_5^2, \cdots, \boldsymbol{x}_5^{15}\}$，其中 $\boldsymbol{x}_{0,8}^i$(=0,1,2,…,15)遍历 1 个半字节的所有取值，$\boldsymbol{x}_0^i$ 其余半字节的值相等. $\boldsymbol{x}_0^0$ 是服从如图 2 所示的 4 轮差分路线的 1 个明文，则如下 4 轮性质成立.

性质 2. S 盒性质[20]. 如果 S 盒的输入差分唯一确定，输出差分唯一确定，则 S 盒输入对和输出对平均都只有 1 个值.

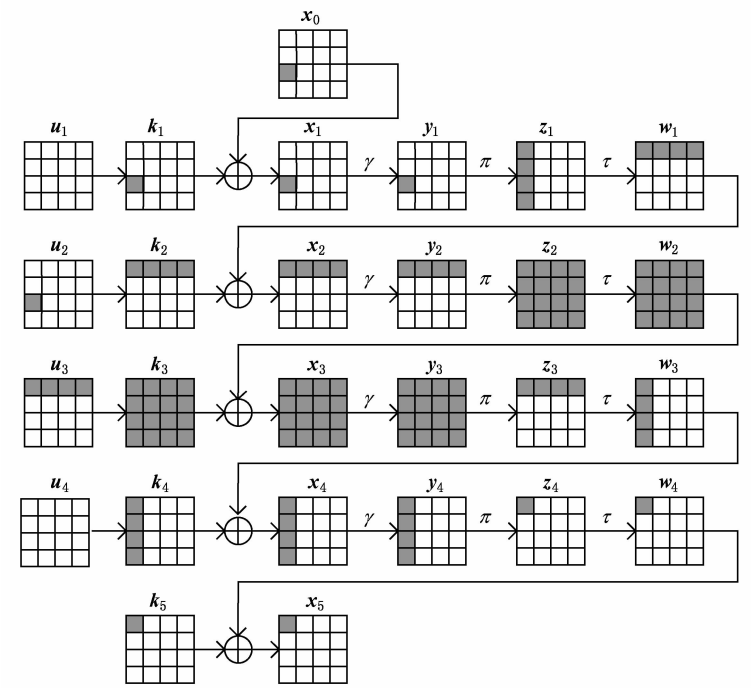

Fig. 2 the 4-round differential characteristic.

图 2 4 轮 mCrypton 的性质

性质 3. 4 轮 mCrypton 性质[14]. 有序序列 $\{\boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^1, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^2, \cdots, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^{15}\}$ 的值取决 11 个半字节：$\boldsymbol{x}_{1,8}^0$，服从图 2 所示的 4 轮差分路线的正确对的差分 $\Delta\boldsymbol{x}_{1,8}^0$ 和 $\Delta z_{4,0}$，$\boldsymbol{x}_{2,\{0,1,2,3\}}^0$，$\boldsymbol{x}_{4,\{0,4,8,2\}}^0$. 从而该有序序列最多有 2^{44} 个可能的取值.

4 轮 mCrypton 的性质证明如下：

证明. 有序序列 $\{\boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^1, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^2, \cdots, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^{15}\}$ 的值取决于 25 个半字节：$\boldsymbol{x}_{1,8}^0$，$\boldsymbol{x}_{2,\{0,1,2,3\}}^0$，$\boldsymbol{x}_{3,\{0,1,\cdots,15\}}^0$，$\boldsymbol{x}_{4,\{0,4,8,12\}}^0$. 下证该 25 个半字节的值取决于如下 11 个半字节：$\boldsymbol{x}_{1,8}^0$，$\Delta\boldsymbol{x}_{1,8}^0$，$\boldsymbol{x}_{2,\{0,1,2,3\}}^0$，$\boldsymbol{x}_{4,\{0,4,8,12\}}^0$，$\Delta z_{4,0}$. 即证明：由这 11 个半字节可推导出 $\boldsymbol{x}_3^0$.

1) 由 $\boldsymbol{x}_{1,8}^0$ 和 $\Delta\boldsymbol{x}_{1,8}^0$ 可得 $\Delta\boldsymbol{x}_{2,\{0,1,2,3\}}$，又因为 $\Delta\boldsymbol{x}_{2,\{0,1,2,3\}}^0$ 已知，故可求出 $\Delta\boldsymbol{x}_3$；

2) 由 $\boldsymbol{x}_{4,\{0,4,8,12\}}^0$ 和 $\Delta\boldsymbol{z}_{4,0}^0$ 可得 Δy_3. 从而根据 S 盒的差分性质可求 $\boldsymbol{x}_3^0$. 证毕.

说明：该有序序列最多有 2^{44} 种可能的取值，而在随机情况下，其有 2^{64} 种取值.

4.2 轮密钥之间的关系

性质 4. 令主密钥为 $\boldsymbol{K}$，中间变量值为 $\boldsymbol{U}$，将 $\boldsymbol{U}$ 初始化：$\boldsymbol{U}=\boldsymbol{K}$. 则由 $\boldsymbol{K}_8$ 可得 $\boldsymbol{u}_7$ 第 1 位的值.

证明. 根据密钥生成算法，可得 $\boldsymbol{K}_8$ 的表达式为

$$\boldsymbol{K}_8 = \begin{pmatrix} \boldsymbol{U}_5^{<<<14} \oplus [S(\boldsymbol{U}_4^{<<<11}) \oplus C_8 \cdot M_0] \\ \boldsymbol{U}_0^{<<<14} \oplus [S(\boldsymbol{U}_4^{<<<11}) \oplus C_8 \cdot M_1] \\ \boldsymbol{U}_1^{<<<11} \oplus [S(\boldsymbol{U}_4^{<<<11}) \oplus C_8 \cdot M_2] \\ \boldsymbol{U}_2^{<<<19} \oplus [S(\boldsymbol{U}_4^{<<<11}) \oplus C_8 \cdot M_3] \end{pmatrix}.$$

因为 $S(\boldsymbol{U}_4{}^{<<<11}) \oplus C_8 \cdot M_0$ 的低 12 b 的值为 0，故 $\boldsymbol{U}_5{}^{<<<14} \oplus [S(\boldsymbol{U}_4{}^{<<<11}) \oplus C_8 \cdot M_0]$ 低 12 b 的值等于 $\boldsymbol{U}_5{}^{<<<14}$ 低 12 b 的值，从而由 $\boldsymbol{K}_8$ 可得：

$\boldsymbol{U}_5[13,12,11,10;9,8,7,6;5,4,3,2]$.

同理，由 $\boldsymbol{K}_8$ 可得：

$\boldsymbol{U}_0[1,0,15,14;9,8,7,6;5,4,3,2]$,

$\boldsymbol{U}_1[4,3,2,1;0,15,14,13;8,7,6,5]$,

$\boldsymbol{U}_2[12,11,10,9;8,7,6,5;4,3,2,1]$.

另一方面，$\boldsymbol{K}_7$ 的表达式为

$$\boldsymbol{K}_7 = \begin{pmatrix} \boldsymbol{U}_0^{<<<14} \oplus [S(\boldsymbol{U}_5^{<<<11}) \oplus C_7 \cdot M_0] \\ \boldsymbol{U}_1^{<<<11} \oplus [S(\boldsymbol{U}_5^{<<<11}) \oplus C_7 \cdot M_1] \\ \boldsymbol{U}_2^{<<<11} \oplus [S(\boldsymbol{U}_5^{<<<11}) \oplus C_7 \cdot M_2] \\ \boldsymbol{U}_3^{<<<19} \oplus [S(\boldsymbol{U}_5^{<<<11}) \oplus C_7 \cdot M_3] \end{pmatrix},$$

将 $\boldsymbol{K}_7$ 进行转置、列混合运算,得 $\boldsymbol{u}_{7,2}$ 为

$$\begin{aligned}\boldsymbol{u}_{7,2} = (&\boldsymbol{U}_2[4]0\boldsymbol{U}_2[2]\boldsymbol{U}_2[1] \oplus \\ &0\boldsymbol{U}_2[15]\boldsymbol{U}_2[14]\boldsymbol{U}_2[13] \oplus *** \\ &0 \oplus \boldsymbol{U}_2[8]\boldsymbol{U}_2[7]0\boldsymbol{U}_2[5]).\end{aligned}$$

其中,"***"表示 $\boldsymbol{U}_2^{<<<11} \oplus [S(\boldsymbol{U}_5^{<<<11}) \oplus C_7 \cdot M_2]$ 的第 7 位、第 6 位、第 5 位. 因为由 $\boldsymbol{K}_8$ 可得 $\boldsymbol{U}_5^{<<<11}[7,6,5,4]$,$\boldsymbol{U}_2^{<<<11}[7,6,5,4]$,从而可计算出计算"***". 又因为 $\boldsymbol{U}_2[4,8]$ 可由 $\boldsymbol{K}_8$ 计算出,故可得 $\boldsymbol{u}_{7,2}[0]$. 证毕.

性质 5. 由 $\boldsymbol{K}_8$ 与 $\boldsymbol{K}_{0,\{2,6,10,14\}}$ 都可求出 $\boldsymbol{U}_1[7,6,5,4]$ 和 $\boldsymbol{U}_2[7,6,5,4]$ 的值.

证明. 由密钥生成算法,可知 $\boldsymbol{K}_0$ 的表达式如下:

$$\boldsymbol{K}_0 = \begin{pmatrix}\boldsymbol{U}_1 \oplus [(\boldsymbol{U}_5) \oplus C_0 \cdot M_0] \\ \boldsymbol{U}_2 \oplus [(\boldsymbol{U}_5) \oplus C_0 \cdot M_1] \\ \boldsymbol{U}_3 \oplus [(\boldsymbol{U}_5) \oplus C_0 \cdot M_2] \\ \boldsymbol{U}_4 \oplus [(\boldsymbol{U}_5) \oplus C_0 \cdot M_3]\end{pmatrix},$$

从而由 $\boldsymbol{K}_{0,\{2,6,10,14\}}$ 可推出 $\boldsymbol{U}_1[7,6,5,4]$ 和 $\boldsymbol{U}_2[7,6,5,4]$. 另一方面,由性质 1 的证明可知:由 $\boldsymbol{K}_8$ 亦可推出 $\boldsymbol{U}_1[7,6,5,4]$ 和 $\boldsymbol{U}_2[7,6,5,4]$. 证毕.

4.3 8 轮 mCrypton-96 的攻击过程

本节充分利用密钥之间的关系,给出对 8 轮 mCrypton-96 的中间相遇攻击,攻击过程如图 3 所示:

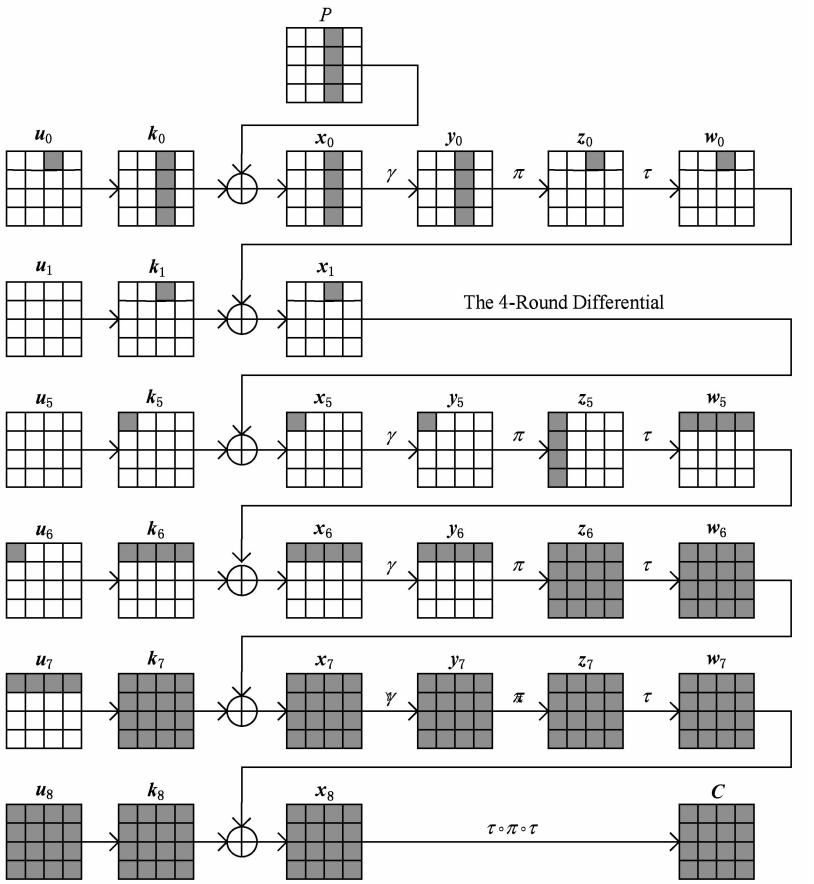

Fig. 3 Meet in the middle attack on 8-round mCrypton-96.

图 3 对 8 轮 mCrypton-96 的攻击

预计算过程:

由于 $\{\boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^1, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^2, \cdots, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^{15}\}$ 的值取决于 11 个半字节,遍历这 11 个半字节的值,计算出有序序列的所有 2^{44} 个可能的取值,并存在 Hash 表 T 中.

攻击过程:

1) 选择 2^{41} 个明文结构,每个明文结构包含 2^{16} 个明文,其遍历第 2,6,10,14 个半字节的值,其余半字节的值为常数. 则一共有 $2^{41} \times 2^{31} = 2^{72}$ 对明文,计算其相应的密文.

2) 对于每个明密文对,猜测 $\Delta \boldsymbol{y}_{6,\{0,1,2,3\}}$,经过比特置换和转置,因为其都是线性变化,所以能够计算出相应的 $\Delta \boldsymbol{x}_7$,又由密文对经过相应的线性变化可以计算出 $\Delta \boldsymbol{y}_7$,从而根据 S 盒性质,由 $(\Delta \boldsymbol{x}_7, \Delta \boldsymbol{y}_7)$ 可计算出 $(\boldsymbol{x}_7, \boldsymbol{y}_7)$,将 $\boldsymbol{y}_7$ 经过线性变化得到 $\boldsymbol{w}_7$,与 $\boldsymbol{x}_8$ 进行异或运算可得 $\boldsymbol{K}_8$.

3) 猜测 $\Delta \boldsymbol{y}_{5,0}$,进行相应的线性运算,计算出 $\Delta \boldsymbol{x}_{6,\{0,1,2,3\}}$,根据 S 盒的性质,计算出 $\boldsymbol{y}_{6,\{0,1,2,3\}}$,然后

将 $\boldsymbol{x}_7$ 经过相应的线性变化,与 $\boldsymbol{y}_{6,\{0,1,2,3\}}$ 进行异或,计算出相应的 $\boldsymbol{u}_{7,\{0,1,2,3\}}$. 再根据性质 4,由 $\boldsymbol{u}_{7,\{0,1,2,3\}}$ 和第 2)步计算出的 $\boldsymbol{K}_8$ 可排除掉 2 种情况.

4) 猜测 $\boldsymbol{w}_{0,2}$,经过相应的线性变化,计算出 $\Delta\boldsymbol{y}_{0,\{2,6,10,14\}}$,从明文对计算出 $\Delta\boldsymbol{x}_{0,\{2,6,10,14\}}$,根据 S 盒的性质,计算出 $\boldsymbol{x}_{0,\{2,6,10,14\}}$,再异或上明文,得到 $\boldsymbol{K}_{0,\{2,6,10,14\}}$. 则根据性质 5,由 $\boldsymbol{K}_8$ 与 $\boldsymbol{K}_0$ 可排除掉 2^8 种情况.

5) 对于所有可能的候选密钥,选择相应明文对中的 1 个明文并得到 $\boldsymbol{w}_{0,2}$. 令 $\boldsymbol{w}_{0,2}$ 遍历 0,1,…,15,计算出相应的明文(δ 集)并询问密文. 猜测 $\boldsymbol{u}_{6,0}$,解密密文得到有序序列$\{\boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^1, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^2, \cdots, \boldsymbol{x}_{5,0}^0 \oplus \boldsymbol{x}_{5,0}^{15}\}$的值.

6) 查 Hash 表 T,如果表 T 中存在有序序列的值,则认为密钥猜测是正确的. 穷举搜索其余未知的密钥.

根据攻击过程可知时间复杂度主要由攻击过程的步骤 3～5 构成. 步骤 1 的复杂度是对 2^{57} 个明文进行 8 轮 mCrypton 加密. 步骤 2 对每 1 对明文都猜测 $\Delta\boldsymbol{y}_{6,\{0,1,2,3\}}$,所以步骤 2 的时间复杂度约为 $2^{72}2^{16}2^{-3}$ 次 8 轮 mCrypton 加密. 步骤 3 在步骤 2 的基础上又猜测了 $\Delta\boldsymbol{y}_{5,0}$,即增加了 2^4 种情况,每一种情况可以计算出 1 个 $\boldsymbol{u}_{7,\{0,1,2,3\}}$,所以步骤 3 的时间复杂度约为 $2^{72}\times2^{20}\times2^{-3}$ 次 8 轮 mCrypton 加密运算. 步骤 4 在步骤 3 的基础上又猜测了 $\boldsymbol{w}_{0,2}$,每一种情况可以计算出 1 个 $\boldsymbol{K}_{0,\{2,6,10,14\}}$,所以步骤 4 的时间复杂度约为 $2^{72}\times2^{24}\times2^{-4}$ 次 8 轮 mCrypton 加密运算. 步骤 5 的时间复杂度约为$2^{72}\times2^{19}\times2^{4}\times2^{-2}$ 次 8 轮 mCrypton 加密运算. 从而在线攻击的时间复杂度约为 $2^{93.5}$. 相对于在线攻击时间复杂度,预计算的时间复杂度可以忽略不计. 预计算过程的存储复杂度是 2^{47} B,在线攻击的存储复杂度忽略不计. 数据复杂度为 2^{57} 个选择明文.

5 总 结

本文通过研究发现了 mCrypton-96 密钥生成算法的漏洞,利用密钥生成算法的弱点并结合 4 轮 mCrypton-96 算法的性质[14],给出了 8 轮 mCrypton-96 算法的中间相遇攻击,比之前的分析结果增加了 1 轮. 攻击的时间复杂度为 $2^{93.5}$ 次加密运算,数据复杂度为 2^{57} 个选择明文,空间复杂度为 2^{47} B. 关于 mCrypton 算法的分析结果如表 1 所示:

Table 1 Summary of Attack Results on mCrypton

表 1 mCrypton 算法的分析结果

Version	Round	Data Complexity	Time Complexity	Memory Complexity	Method	Reference
mCrypton-64	7	2^{57}	2^{57}	2^{44}	MIMT	Ref[14]
	12	2^{48}	$2^{63.38}$		Biclique	Ref[15]
mCrypton-96	7	2^{57}	2^{57}	2^{44}	MIMT	Ref[14]
	8	2^{57}	$2^{93.5}$	2^{47}	MIMT	This paper
	8	2^{48}	2^{65}	$2^{81.6}$	CA	Ref[16]
	9	$2^{59.9}$	$2^{74.9}$	$2^{63.9}$	RKIDC	Ref[17]
	12	$2^{27.54}$	$2^{94.09}$	2^{20}	Biclique	Ref[18]
mCrypton-128	7	2^{57}	2^{57}	2^{44}	MIMT	Ref[14]
	8	2^{46}	2^{46}		RKR	Ref[19]
	8	2^{48}	2^{65}	$2^{81.6}$	CA	Ref[16]
	8	2^{57}	2^{96}	2^{44}	MIMT	Ref[14]
	9	$2^{59.7}$	$2^{66.7}$	$2^{55.7}$	RKIDC	Ref[17]
	9	2^{53}	2^{116}	2^{120}	MIMT	Ref[14]
	12	$2^{20.1}$	$2^{125.84}$	2^{20}	Biclique	Ref[18]
	12	2^{48}	$2^{126.56}$		Biclique	Ref[15]

MIMT: meet-in-the-middle attack; CA: collision attack; RKIDC: relate key impossible differential cryptanalysis; RKR: relate key rectangle attack.

参 考 文 献

[1] Diffie W, Hellman M E. Special feature exhaustive cryptanalysis of the NBS Data Encryption Standard [J]. Computer, 1997, 10(6): 74-84

[2] Gilbert H, Minier M. A collision attack on 7 rounds of Rijndael [C] //Proc of the 3rd AES Candidate Conf. Berlin: Springer, 2000: 230-241

[3] Demirci H, Selcuk A. A meet-in-the-middle attack on 8-round AES [G] //LNCS 5922: Proc of Fast Software Encryption. Berlin: Springer, 2008: 116-126

[4] Dunkelman O, Keller N, Shamir A. Improved single key attack on 8-round AES-192 and AES-256 [G] //LNCS 6477: Proc of Advances in Cryptology—ASIACRYPT 2010. Berlin: Springer, 2010: 158-176

[5] Derbez P, Fouque P A, Jean J. Improved key recovery attacks on reduced-round AES in the single-key setting [G] //LNCS 7881: Proc of Advances in Cryptology—EUROCRYPT 2013. Berlin: Springer, 2013: 371-387

[6] Li L, Jia K, Wang X. Improved single-key attacks on 9-round AES-192/256 [G] //LNCS 8540: Proc of Fast Software Encryption. Berlin: Springer, 2015: 127-146

[7] Guo Jian, Peyrin T, Poschmann A, et al. The LED block cipher [G] //LNCS 6917: Proc of Cryptographic Hardware and Embedded Systems (CHES 2011). Berlin: Springer, 2011: 326-341

[8] Gérard B, Grosso V. Block ciphers that are easier to mask: How far can we go? [G] //LNCS 8086: Proc of Cryptographic Hardware and Embedded Systems—CHES 2013. Berlin: Springer, 2013: 383-399

[9] Sekar G, Mouha N, Velichkov V, et al. Meet-in-the-middle attacks on reduced-round XTEA [G] //LNCS 6558: Proc of Topics in Cryptology-CT-RSA 2011. Berlin: Springer, 2011: 250-267

[10] Lu J, Wei Y, Pasalic E, et al. Meet-in-the-Middle attack on reduced versions of the camellia block cipher [G] //LNCS 7631: Proc of Advances in Information and Computer Security. Berlin: Springer, 2012: 197-215

[11] Chen Jiazhe, Li Leibo. Low data complexity attack on reduced camellia-256 [G] //LNCS 7372: Proc of Australasian Conf on Information Security and Privacy. Berlin: Springer, 2012: 101-114

[12] Bogdanov A, Rechberger C. A 3-subset Meet-in-the-Middle Attack: Cryptanalysis of the lightweight block cipher KTANTAN [G] //LNCS 6544: Proc of Selected Areas in Cryptography. Berlin: Springer, 2011: 229-240

[13] Lim C H, Korkishko T. mCrypton-A lightweight block cipher for security of low-cost RFID tags and sensors [G] //LNCS 3786: Proc of Information Security Application. Berlin: Springer, 2006: 243-258

[14] Hao Y, Bai D, Li L. A meet-in-the-middle attack on round-reduced mCrypton using the differential enumeration technique [G] //LNCS 8792: Proc of Network and System Security. Berlin: Springer, 2014: 166-183

[15] Jeong K, Kang H, Lee C, et al. Weakness of lightweight block ciphers mCrypton and LED against biclique cryptanalysis [J]. Peerto-Peer Networking and Applications, 2015, 8(4): 716-732

[16] Kang J, Jeong K, Sung J, et al. Collision attacks on AES-192, AES-256, mCrypton-192/256, mCrypton-96/128 and anubis [J/OL]. Journal of Applied Mathematics, 2013 [2015-06-18]. http://downloads. hindawi. com/journals/jam/aip/73673. pdf

[17] Mala H, Dakhilalian M, Shakiba M. Cryptanalysis of mCrypton—A lightweight block cipher for security of RFID tags and sensors [J]. International Journal of Communication Systems, 2012, 25(4): 415-426

[18] Shakiba M, Dakhilalian M, Mala H. Non-isomorphic Biclique cryptanalysis and its application to full-round mCrypton [EB/OL]. (2013-03-08) [2015-06-18]. http://eprint. iacr. org/2013/141. pdf

[19] Park J H. Security analysis of mCrypton proper to low-cost ubiquitous computing devices and applications [J]. International Journal of Communication Systems, 2009, 22(8): 959-969

[20] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds, advances in cryptology [G] //LNCS 1592: Proc of Advances in Cryptology-EUROCRYPT'99. Berlin: Springer, 1999: 12-23

Gan Nan, born in 1992. MSc candidate in the School of Computer Science and Technology, Donghua University. His main research interest is cryptanalysis of block ciphers (nannangan123@163. com).

Wang Gaoli, born in 1982. Received her BSc degree in fundamental mathematics in 2003, and PhD degree in cryptography in 2008, both from Shandong University of China, Jinan. Associate professor in the School of Computer Science and Technology, Donghua University, Shanghai. Her research interests include cryptanalysis and design of Hash functions and block ciphers.