CIKS-128 分组算法的相关密钥-差分攻击

郭建胜[1,2],崔竞一[1],罗 伟[3],刘翼鹏[1]
(1. 解放军信息工程大学,河南郑州 450004;2. 信息保障技术重点实验室,北京 100000;3. 78179 部队,四川成都 611843)

摘 要: 分析研究了 CIKS-128 分组密码算法在相关密钥-差分攻击下的安全性. 利用 DDP 结构和非线性函数的差分信息泄漏规律构造了一条高概率相关密钥-差分特征,并给出攻击算法,恢复出了 192bit 密钥;在此基础上,对剩余 64bit 密钥进行穷举攻击,恢复出了算法的全部 256bit 密钥. 攻击所需的计算复杂度为 2^{77} 次 CIKS-128 算法加密,数据复杂度为 2^{77} 个相关密钥-选择明文,存储复杂度为 $2^{25.4}$ 字节存储空间. 分析结果表明,CIKS-128 算法在相关密钥-差分攻击条件下是不安全的.

关键词: 分组密码;密码分析;CIKS-128 分组算法;相关密钥-差分攻击
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2016)08-1837-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2016.09.010

Related-Key Differential Attack on Block Cipher CIKS-128

GUO Jian-sheng[1,2], CUI Jing-yi[1], LUO Wei[3], LIU Yi-peng[1]
(1. *The PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*;
2. *Science and Technology on Information Assurance Laboratory, Beijing* 100000, *China*;
3. *The Unit of* 78179, *Chengdu, Sichuan*, 611843, *China*)

Abstract: The security of CIKS-128 block cipher under related-key differential attack was studied. A related-key differential of high probability was constructed with the differential information leakages in the structure of DDPs and nonlinear functions. By proposing a corresponding key recovery attack based on the related-key differential, the master key of 192 bits was recovered. The rest 64 bits of the master key could be obtained by exhaustive search. The computational complexity, the data complexity and the memory complexity are 2^{77} CIKS-128 block cipher encryptions, 2^{77} chosen-plaintexts and $2^{25.4}$ bytes of storage resources, respectively. Analysis results show that CIKS-128 is unsafe under related-key differential attack.

Key words: block cipher; cryptanalysis; CIKS-128; related-key differential attack

1 引言

随着物联网相关技术地快速发展,资源受限环境下的信息安全问题日益突出. 这类硬件设备的计算、存储资源受限的环境下,常规的分组密码算法在资源占用率和实现效率上难以满足需求. DDP(Data-Dependent Permutations)[1,2]结构具有实现速率快、资源占用小、数据处理规模灵活等特点,被广泛应用于算法设计[3~5]. 基于 DDP 结构设计的密码算法具有高效低耗特点. 然而,目前针对这类算法的安全性分析有待完善,严重制约了这类算法走向应用.

近年来,复合攻击方法的研究成为分组密码分析领域的研究热点,特别是相关密钥-差分类型的攻击方法的应用[6~10]极大推动了分组密码分析的发展. 特别地,为减小计算-存储开销,基于 DDP 结构设计的分组密码算法通常选用简单的密钥生成算法,相关密钥类型的复合攻击成为分析这类算法的有力手段之一. 2010 年,Lee 等人利用分割攻击的思想对 DDP-64 分组密码算法抵抗相关密钥-差分分析的能力进行了评估[11];2012 年,在 WAINA 会议上,Jinkeon Kang 等人提出了针对 MD-64 算法的相关密钥-扩大飞来去器攻击[12],为基于高次 DDP 结构的分组密码算法安全性分析提供了新的思路.

作为基于 DDP 结构的典型算法,CIKS-128 算法[3]采用 DDP 结构提升了数据的处理效率,选用简单的密钥生成算法降低了实现功耗,设计者声称该算法能够

收稿日期:2014-12-24;修回日期:2015-06-24;责任编辑:马兰英
基金项目:博士后科学基金(No. 2014M562582)

抵抗所有已知攻击. 针对 CIKS-128 算法,Youngdai Ko 等人于2004 年提出了相关密钥-差分攻击[13],恢复出了47bit 密钥信息;Lee 等人于 2011 年构造了算法的一条高概率相关密钥-差分特征[14],恢复出了 63bit 密钥信息,这是针对该算法最好的分析结果.

本文研究了 CIKS-128 算法的相关密钥-差分性质,利用 DDP 结构的差分信息泄漏规律构造了算法的高概率相关密钥-差分特征,并给出了相应攻击算法,恢复出了 192bit 密钥,并利用穷举攻击恢复出了算法剩余 64bit 密钥. 攻击算法计算复杂度为 2^{77}次 CIKS-128 算法加密,数据复杂度为 2^{77}个选择明文,存储复杂度为 $2^{25.4}$ 字节.

2 相关知识

2.1 符号约定

本文常用符号约定如下:

$\oplus$	逐位模 2 加
e_i	角标位置取值为 1,其它位置为 0 的二元序列,e_{i_1,i_2},e_{i_1,i_2,i_3}依此类推
$P(C)$	明文(密文)
$X_L(X_R)$	数据块 X 的左(右)半部分
ΔX	表示二元序列 X 的两组取值逐位模 2 加
$X\cdot Y$	表示二元序列 X,Y 逐位相乘
x_i	X 的第 i 比特
$X^{\ggg n}$	表示二元序列 X 循环右移 n bit
$e_i\rightarrow e_j$	输入差分为 e_i,输出差分为 e_j 的差分对
p_i,q_i	概率
$P_{n/m}$	输入输出为 n bit,控制信息为 m bit 的 DDP 结构(变换)

2.2 CIKS-128 分组密码算法

CIKS-128 算法分组长度为 128bit,密钥长度为 256bit,迭代圈数为 12 轮,算法整体结构和圈函数结构如图 1 所示.

如图 1 所示,CIKS-128 算法采用类 Feistel 结构,圈函数对右半部分处理后作为下一轮左半部分输入,左半部分直接输出作为下一轮右半部分输入,最后一轮圈函数变换后不进行左右数据块互换. 特别地,圈函数左半部分数据和圈子密钥共同作为右半部分 DDP 结构的控制信息.

圈函数 $\mathrm{Crypt}^{(e)}$ 包括:线性变换 π,$\prod$,移位变换 I,非线性函数 G,DDP 变换 $P_{64/192}$,$P_{64/192}^{-1}$,$P_{128/1}^{(e)}$以及逐位模 2 加运算. $\mathrm{Crypt}^{(0)}$ 表示加密算法圈函数,$\mathrm{Crypt}^{(1)}$ 表示解密算法圈函数.

线性变换 π 输入为 64bit 数据块 L 和两个 64bit 密钥块 $A^{(1)}$,$A^{(4)}$(或 $A^{(3)}$,$A^{(2)}$),输出 192bit 作为 $P_{64/192}$(或 $P_{64/192}^{-1}$)的控制信息

$V=(V_1,V_2,V_3,V_4,V_5,V_6)=\pi(L,L',L'')$其中$(L',L'')\in\{(L\oplus A^{(1)},L\oplus A^{(4)}),(L\oplus A^{(3)},L\oplus A^{(2)})\}$,$L,A^{(i)}\in\{1,0\}^{64}$,$i=1,2,3,4$. V_i 取值如下:

$$\begin{cases}V_1=(l_{31},l_{32},l_3,l_4,\cdots,l_{30},l_1,l_2);\\ V_2=(l'_{10}l'_{24}l'_{25}l'_{26}l'_{29}l'_{13}l'_{27}l'_{16}l'_1l'_2l'_{31}l'_{32}l'_3l'_4l'_{19}l'_6;\\ l'_7l'_8l'_9l'_{23}l'_{11}l'_{12}l'_{28}l'_{15}l'_{14}l'_{30}l'_{17}l'_{18}l'_{27}l'_5l'_{20}l'_{21}l'_{22});\\ V_1=(l''_{13},l''_{14},\cdots,l''_{32},l''_1,l''_2,\cdots,l''_8,l''_{12},l''_{10},l''_{11},l''_9);\\ V_2=(l_{33},l_{34},\cdots,l_{64});\\ V_1=(l'_{55},l'_{56},\cdots,l'_{64},l'_{33},l'_{34},\cdots,l'_{54});\\ V_2=(l''_{45},l''_{46},\cdots,l''_{64},l''_{33},l''_{34},\cdots,l''_{44}).\end{cases}$$

其中 l_i,l'_i,l''_i 分别表示 L,L',L''的第 i 比特.

线性变换$\prod$由四个长度为 16bit 的轮换的乘积构成,可描述为

(1,50,9,42,17,34,25,26,33,18,41,10,49,2,57,58);

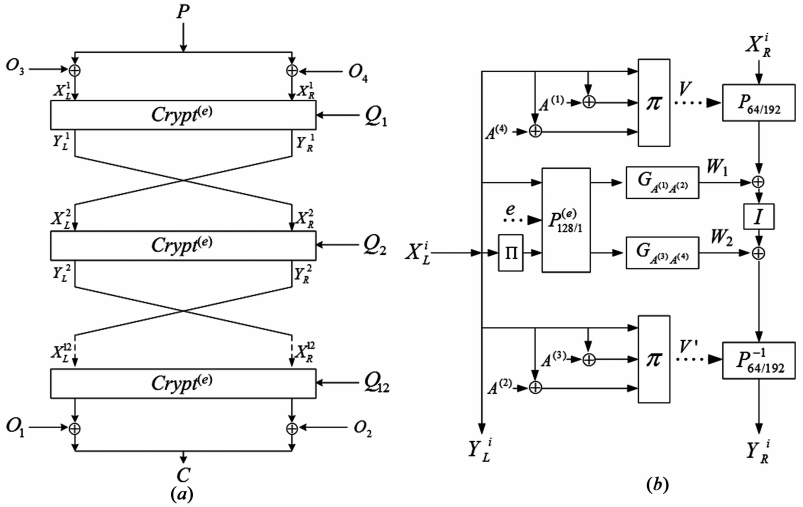

图1 (*a*)CIKS-128算法结构图;(*b*)圈函数结构图$\mathrm{Crypt}^{(e)}$

(3,64,43,24,19,48,59,8,35,32,11,56,51,16,27,40);
(4,7,28,47,52,23,12,63,36,39,60,15,20,55,44,31);(5,14,13,6,21,62,29,54,37,46,45,38,53,30,61,22).

移位变换 I 输入输出均为 64bit,若其输入为 $X=(X_1,X_2,\cdots,X_8)$,则输出为

$$Y=\mathrm{I}(X)=(X_6^{<<<4},X_5^{<<<4},X_4^{<<<4},X_3^{<<<4},X_2^{<<<4},X_1^{<<<4},X_8^{<<<4},X_7^{<<<4})$$

其中 $X_i\in\{0,1\}^8$.

非线性函数 G 定义为

$$\begin{aligned}G(L,A',A'')=&L_0\oplus A_0'\oplus(L_1\cdot A_0'')\oplus(L_2\cdot L_5)\oplus(L_6\cdot A_1')\\&\oplus(A_1''\cdot A_2')\oplus(L_4\cdot L_3)\oplus(L_1\cdot L_6\cdot L_4)\oplus\\&(L_2\cdot L_6\cdot A_1'')\oplus(L_1\cdot A_1''\cdot L_2\cdot L_4)\end{aligned}$$

其中 $L_0=L,\cdots,L_j=(1,\cdots,1,l_1,\cdots,l_{64-j})$;$A_0=A$,$A_1=(1,a_1,\cdots,a_{63})$,$A_2=(1,1,a_1,\cdots,a_{62})$ $(A=A'orA'')$;L_i,$A_i\in\{1,0\}^{64}$. 为便于区分,本文记 $G_1=G_{A^{(1)}A^{(2)}}$,$G_2=G_{A^{(3)}A^{(4)}}$.

$P_{64/192}$ 变换输入输出均为 64bit,控制信息为 192bit,图 2 给出了 $P_{64/192}$ 的结构图. $P_{64/192}$ 由 6 层基本 $P_{2/1}$ 构成,每层包含 32 个并置的 $P_{2/1}$,层与层之间通过线性变换连接,其中基本单元 $P_{2/1}$ 定义为

$$P_{2/1}(x_1,x_2,v)=\begin{cases}(x_1,x_2), & \text{if}\quad v=0;\\(x_2,x_1), & \text{if}\quad v=1.\end{cases}$$

$P_{64/192}^{-1}$ 与 $P_{64/192}$ 结构上完全相同,其控制信息从上到下依次为 $V_6,V_5,\cdots,V_1$.

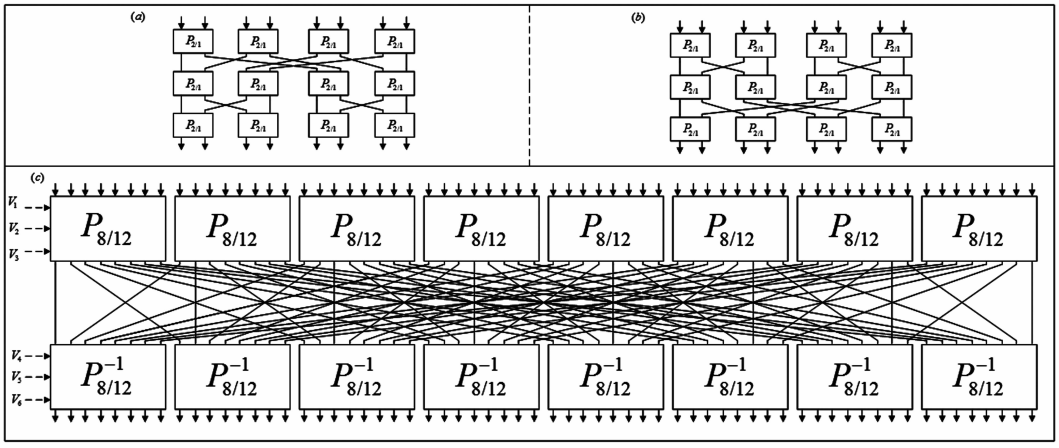

图2　$P_{64/192}$结构图

$P_{128/1}^{(e)}$ 是由加解密参数 e 控制的 DDP 变换,当执行加密算法($e=0$)时,$P_{128/1}^{(e)}$ 为恒等变换;当执行解密算法($e=1$)时,$P_{128/1}^{(e)}$ 交换两个 64bit 输入数据块作为其输出.

如表 1 所示,第 j 轮圈子密钥 $Q_j=(A_j^{(1)},A_j^{(2)},A_j^{(3)},A_j^{(4)})$,$O_i(i=1,2,3,4)$ 表示大小为 64bit 的密钥块. 记算法主密钥 $K=(K_1,K_2,K_3,K_4)$ ($K_i(i=1,2,3,4)$ 为 64 比特密钥块),当执行加密算法时,$O_i=K_i$;当执行解密算法时,$O_1=K_3$,$O_2=K_4$,$O_3=K_1$,$O_4=K_2$.

表 1　CIKS-128 算法圈子密钥

j	1	2	3	4	5	6	7	8	9	10	11	12
$A_j^{(1)}$	O_1	O_4	O_3	O_2	O_1	O_3	O_3	O_1	O_2	O_3	O_4	O_1
$A_j^{(2)}$	O_2	O_3	O_4	O_1	O_2	O_4	O_4	O_2	O_1	O_4	O_3	O_2
$A_j^{(3)}$	O_3	O_2	O_1	O_4	O_3	O_1	O_1	O_3	O_4	O_1	O_2	O_3
$A_j^{(4)}$	O_4	O_1	O_2	O_3	O_4	O_2	O_2	O_4	O_3	O_2	O_1	O_4

关于 CIKS-128 算法详细信息参见文献[3].

3　相关密钥-差分特性分析

定义 1　重量表示二元序列中 1 的个数.

针对 CIKS-128 算法,Changhoon Lee 等人[14]给出的攻击算法利用重量为 1 的差分在第 12 轮 $P_{64/192}^{-1}$ 变换中的差分转移规律恢复了部分控制信息,得到了出口白化前 63bit 数据,利用对应的密文比特,恢复出 63bit 密钥信息. 本文将第 12 轮圈函数的输出差分 $\Delta Y^{12}=(0,e_j)$ 作为第 11 轮圈函数的输出差分 $\Delta Y^{11}=(0,e_j)$(即 $\Delta X^{12}=(e_j,0)$),利用第 12 轮输入差分重量为 1 时的相关密钥-差分特性,构造新的高概率相关密钥-差分特征.

3.1　轮函数差分特性分析

下面分析第 12 轮输入差分 $\Delta X^{12}=(e_j,0)$,密钥差分 $\Delta Q_{12}=(0,0,e_{64},e_{64})$ 时,各变换环节的差分转移规律.

定义 2　若 DDP 结构的控制信息差分重量为 0 时,输入输出重量相等,则称该 DDP 结构具有差分重量平衡性.

性质 1　$P_{64/192}$($P_{64/192}^{-1}$)具有差分重量平衡性,且控制信息差分重量为 0 时,输出差分非 0 比特均匀分布.

证明　根据定义,基本单元具有差分重量平衡性,且控制信息差分重量为 0 时,输出差分非 0 比特均匀分

布. $P_{64/192}$($P_{64/192}^{-1}$)由6层$P_{2/1}$构成,输入差分非0比特传递到任意输出比特需经过6个$P_{2/1}$变换,经过每个$P_{2/1}$时的输出差分非0比特均匀分布,从而输入差分非0比特经过$P_{64/192}$后的输出位置有2^6个,而$P_{64/192}$的输出比特恰好为2^6个,即任意输入比特传递到任意输出比特的概率均为2^{-6}. 证毕.

性质2 $\Delta X^{11}=(0,0),\Delta Q_{11}=(e_{64},e_{64},0,0)$时,$\Delta X^{12}=(e_j,0)$的概率为$2^{-9}$.

证明 根据线性变换π的定义,第11轮$|\Delta V|=|\Delta V'|=1$. 由$P_{2/1}$的定义,控制比特差分重量为1时,其输出差分为0的概率为2^{-1},因此$P_{64/192}$输出差分为0的概率为2^{-1},控制信息差分对$P_{64/192}^{-1}$输出差分无影响的概率为2^{-1}. 根据G_1的定义,其输出差分满足$\Delta W_1(64)=1\oplus l_{63}$,即其输出差分为$e_{64}$的概率为$2^{-1}$. 因此,$P_{64/192}^{-1}$输入差分为$e_{I(64)}=e_4$的概率为$2^{-2}$. 根据性质1,$P_{64/192}^{-1}$输出差分为$e_j(j=1,2,\cdots,64)$的概率为$2^{-2}\times 2^{-1}\times 2^{-6}=2^{-9}$. 证毕.

性质3 $\Delta X^{12}=(e_j,0)(j\neq 64),\Delta Q_{12}=(0,0,e_{64},e_{64})$时,$P_{64/192}$输出差分为0的概率为$p_1=2^{-4}$.

证明 由$P_{2/1}$的定义,控制比特差分重量为1时,其输出差分为0的概率为2^{-1}. 由π的定义可知,圈函数左半部分输入差分重量为1时,$P_{64/192}$的控制信息V的差分重量为3(不考虑密钥差分). 由于$j\neq 64$,结合密钥差分$(\Delta A^{(1)},\Delta A^{(4)})=(0,e_{64})$后,控制信息$V$的差分重量为4. 因此,$P_{64/192}$输出差分为0的概率为$p_1=2^{-4}$. 证毕.

根据性质3,可以对$P_{64/192}^{-1}$作类似分析,控制信息差分不引入非0差分比特的概率为$p_1=2^{-4}$.

性质4 $\Delta X^{12}=(e_j,0)(1\leqslant j\leqslant 58),\Delta Q_{12}=(0,0,e_{64},e_{64})$时,$G_1$输出差分为$e_j$的概率为$p_2=2^{-6}$.

证明 $\Delta X^{12}=(e_j,0),(\Delta A',\Delta A'')=(0,0)$时,$G_1$输入差分为$e_j$,其输出差分$\Delta W_1$满足:

$$\begin{cases}\Delta W_1(j)=1;\\ \Delta W_1(j+1)=a''_{j+1}\oplus l_{j-5}l_{j-3}\oplus l_{j-1}l_{j-3}a''_j;\\ \Delta W_1(j+2)=l_{j-3}\oplus l_{j-4}a''_{j+1}\oplus l_{j+1}l_{j-2}a''_{j+1};\\ \Delta W_1(j+3)=l_{j-1};\\ \Delta W_1(j+4)=l_{j+1}\oplus l_{j+3}l_{j-2}\oplus l_{j+3}l_{j+2}a''_{j+3};\\ \Delta W_1(j+5)=l_{j+3};\\ \Delta W_1(j+6)=a'_{j+5}\oplus l_{j+5}l_{j+2}\oplus l_{j+4}a''_{j+5}.\end{cases}$$

其中$\Delta W_1(i),l_i,a'_i,a''_i$分别表示$\Delta W_1,L,A',A''$的第$i$比特.

由上式可知,$\Delta W_1(i)=1$的概率为$0.5(i=j+1,j+2,j+3,j+4,j+5,j+6)$,从而$G_1$输出差分$\Delta W_1=e_j$的概率为$p_2=2^{-6}$. 证毕.

性质5 $\Delta X^{12}=(e_j,0)(1\leqslant\prod(j)\leqslant 58),\Delta Q_{12}=(0,0,e_{64},e_{64})$时,$G_2$输出差分为$e_{\prod(j)}$的概率为$p_3=2^{-7}$.

证明 根据定义,密钥差分$(\Delta A',\Delta A'')=(e_{64},e_{64})$引起的输出差分满足$\Delta W_1(64)=1\oplus l_{63}$. 又根据性质4的分析过程,$1\leqslant\prod(j)\leqslant 58$时,数据差分与密钥差分引起的输出差分非0比特位不重合,因此密钥差分对G_2输出差分无影响的概率为2^{-1}. 根据性质4,$\Delta X^{12}=(e_j,0)(1\leqslant\prod(j)\leqslant 58)$使得$G_2$输出差分为$e_{\prod(j)}$的概率为$2^{-6}$. 因此,$G_2$输出差分为$e_{\prod(j)}$的概率为$p_3=2^{-1}\times 2^{-6}=2^{-7}$. 证毕.

定理1 当$\Delta X^{12}=(e_j,0)(1\leqslant j,\prod(j)\leqslant 58),\Delta Q_{12}=(0,0,e_{64},e_{64})$时,第12轮$P_{64/192}^{-1}$输入差分为$(e_{I(j),\prod(j)})$的概率为$p_1^2p_2p_3=2^{-21}$.

证明 由性质3,4,5即得. 证毕.

根据性质1和定理1,当第12轮$\Delta X^{12}=(e_j,0)(1\leqslant j,\prod(j)\leqslant 58),\Delta Q_{12}=(0,0,e_{64},e_{64})$时,对于固定的$s,t$,第12轮差分对$(e_j,0)\rightarrow(e_j,e_{s,t})$的概率为$q_{12}=2^{-21}/C_{64}^2\approx 2^{-31.98}$.

3.2 相关密钥差分特征

由$\prod$变换的定义,"$1\leqslant j,\prod(j)\leqslant 58$"等价于"$1\leqslant j\leqslant 58$且$j\neq 3,12,21,30,39,48$". 结合定理1和文献[14]给出的相关密钥-差分特征,表2给出了CIKS-128算法的相关密钥-差分特征,其中$1\leqslant j\leqslant 58$且$j\neq 3,12,21,30,39,48$.

如表2所示,本文构造的相关密钥-差分特征概率为

$$(2^{-3})^10\times 2^{-9}\times 2^{-31.98}\approx 2^{-71}$$

3.3 $P_{64/192-1}$差分特性分析

在表2的相关密钥-差分特征中,第12轮$P_{64/192}^{-1}$输入差分为$e_{1(j),\prod(j)}$,根据性质1,$P_{64/192}^{-1}$输出差分重量为2. 下面分析第12轮$P_{64/192}^{-1}$输入差分重量为2且控制信息差分不引入非0差分比特时的差分转移规律.

记v_i表示第12轮192比特的控制信息V'的第i比特.

定义3 差分传递线路是指$P_{64/192}^{-1}$中差分特征经过基本单元$P_{2/1}$对应的控制信息组成的链.

对于$P_{64/192}^{-1}$,当输入输出差分已知时,根据差分比特所经过的$P_{2/1}$是否进行比特交换即可确定相应$P_{2/1}$的控制比特,从而得到相应的差分传递线路. 根据$P_{64/192}^{-1}$的拓扑结构,重量为1的差分对$e_i\rightarrow e_j$存在一条差分传递线路. 例如$e_{16}\rightarrow e_4$的差分传递线路为:$v_{168}=1,v_{134}=1,v_{101}=1,v_{65}=1,v_{33}=1,v_2=1$,如图3所示.

表 2　相关密钥-差分特征

	文献[14]给出的相关密钥-差分特征			本文给出的相关密钥-差分特征		
轮次	ΔX^i	ΔQ_i	q_i	ΔX^i	ΔQ_i	q_i
入口白化	(e_{64},e_{64})	(e_{64},e_{64})	1	(e_{64},e_{64})	(e_{64},e_{64})	1
1	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}
2	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}
3	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}
4	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}
5	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}
6	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}
7	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}
8	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}
9	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-3}
10	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}
11	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-3}	$(0,0)$	$(e_{64},e_{64},0,0)$	2^{-9}
12	$(0,0)$	$(0,0,e_{64},e_{64})$	2^{-9}	$(e_j,0)$	$(0,0,e_{64},e_{64})$	$2^{-31.98}$
出口白化	$(0,e_j)$	$(0,0)$	1	$(e_j,e_{I(j),\Pi(j)})$	$(0,0)$	1
输出差分	$(0,e_j)$			$(e_j,e_{I(j),\Pi(j)})$		

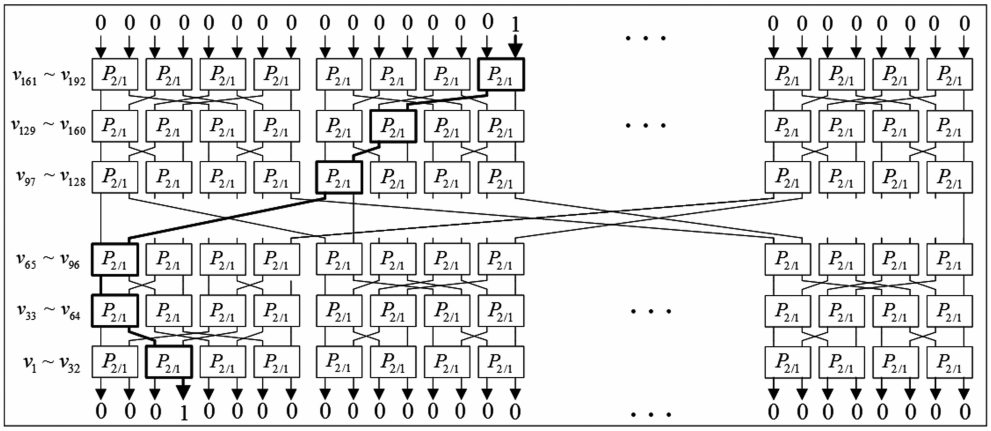

图3　$e_{16} \rightarrow e_4$的差分传递线路示意图

重量为 2 的差分对 $e_{I(j),\Pi(j)} \rightarrow e_{s,t}$存在 2 类差分传递线路,每类包括两条重量为 1 的差分传递线路. 例如 $j=57$ 时,$I(j)=53$,$\Pi(j)=58$,$e_{53,58} \rightarrow e_{4,59}$的两条差分传递线路由图4 给出:第Ⅰ类差分传递线路中,e_{53}传递到 e_4,e_{58}传递到 e_{59}(如图 4 实线所示);第Ⅱ类差分传递线路中,输入差分 e_{53}传递到 e_{59},e_{58}传递到 e_4(如图 4 虚线所示). $e_{53,58} \rightarrow e_{4,59}$的差分传递线路由表 3 给出.

算法第 12 轮 $P_{64/192}^{-1}$的控制信息 $V^{'}$由 X_L^{12},$(A_{12}^{(2)}, A_{12}^{(3)})=(O_2,O_3)$经过线性变换 π 生成,而 $X_L^{12}=Y_L^{12}$ 与出口白化密钥块 O_1 逐位模 2 加作为密文左半部分 C_L,即 $X_L^{12} \oplus O_1 = C_L$. 因此,结合表3 中线路Ⅰ即可建立密文与密钥块 O_1,O_2,O_3 的方程组:

表 3　$e_{53,58} \rightarrow e_{4,59}$的两类差分传递线路

线路编号	两条重量为 1 的差分对	两比特差分传递路线
Ⅰ	$e_{53} \rightarrow e_4$, $e_{58} \rightarrow e_{59}$	$v_{187}=0,v_{154}=0,v_{121}=1,v_{68}=0,v_{35}=0,v_2=0$ $v_{189}=0,v_{159}=1,v_{128}=1,v_{96}=1,v_{62}=0,v_{30}=1$
Ⅱ	$e_{53} \rightarrow e_{59}$, $e_{58} \rightarrow e_4$	$v_{187}=1,v_{156}=1,v_{124}=0,v_{96}=0,v_{62}=0,v_{30}=1$ $v_{189}=1,v_{157}=0,v_{125}=0,v_{68}=1,v_{35}=0,v_2=0$

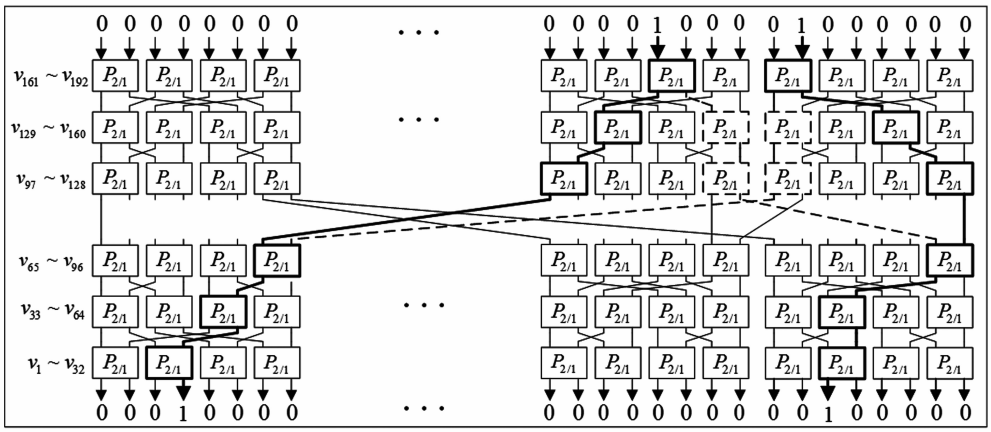

图4 $e_{53,58} \rightarrow e_{4,59}$的差分传递线路示意图

$$\begin{cases} c_{39} \oplus O_1^{39} \oplus O_2^{39} = v_{187} = 0; & c_{41} \oplus O_1^{41} \oplus O_2^{41} = v_{189} = 0; \\ c_{48} \oplus O_1^{48} \oplus O_3^{48} = v_{154} = 0; & c_{53} \oplus O_1^{53} \oplus O_3^{53} = v_{159} = 1; \\ c_{57} \oplus O_1^{57} = v_{121} = 1; & c_{64} \oplus O_1^{64} = v_{128} = 1; \\ c_{16} \oplus O_1^{16} \oplus O_2^{16} = v_{68} = 0; & c_9 \oplus O_1^9 \oplus O_2^9 = v_{96} = 1; \\ c_{26} \oplus O_1^{26} \oplus O_3^{26} = v_{35} = 0; & c_{20} \oplus O_1^{20} \oplus O_3^{20} = v_{62} = 0; \\ c_{32} \oplus O_1^{32} = v_2 = 0; & c_{30} \oplus O_1^{30} = v_{30} = 1. \end{cases}$$

根据上述方程组,利用满足表 2 中本文构造的相关密钥-差分特征的密文对,即可根据第 12 轮 $P_{64/192}^{-1}$重量为 2 的差分特征得到 12bit 密钥信息:
$O_1^{39} \oplus O_2^{39}, O_1^{48} \oplus O_3^{48}, O_1^{57}, O_1^{16} \oplus O_2^{16}, O_1^{26} \oplus O_3^{26}, O_1^{32}, O_1^{41} \oplus O_2^{41}, O_1^{53} \oplus O_3^{53}, O_1^{64}, O_1^9 \oplus O_2^9, O_1^{20} \oplus O_3^{20}, O_1^{30}$.

类似地,利用第Ⅱ类差分传递线路得到 12bit 密钥信息. 本文将由一类差分传递线路得到的 12bit 密钥信息链视为整体,对于一个满足表 2 新构造的相关密钥-差分特征的密文对,其第 12 轮 $P_{64/192}^{-1}$变换中差分对 $e_{I(j),\Pi(j)} \rightarrow e_{s,t}$等概率通过相应的两类差分传递线路. 因此,对于给定的 j,s,t,利用 2^m 对满足条件的密文对,分别得到两类差分传递线路对应的两条 12bit 密钥信息链的正确取值的期望计数次数为 2^{m-1}次,而错误密钥链的期望计数次数为 2^{m-12},因此选取足够多满足条件的密文对,通过对恢复出的 12bit 密钥信息链进行计数,能够有效区分正确密钥信息链和错误密钥信息链.

4 相关密钥-差分攻击算法

对于给定的 $j,s,t,k_{s,t}^j,k_{s,t}^{j'} \in K_{s,t}^j$表示密文差分 $\Delta C = (e_j, e_{s,t})$时,利用第 12 轮 $P_{64/192}^{-1}$重量为 2 的两类差分传递线路恢复出的两组 12bit 密钥信息.

下面利用本文构造的相关密钥-差分特征,给出 CIKS-128 算法的相关密钥-差分攻击算法.

算法 1 相关密钥-差分攻击算法

对 $j=2,10,16,18,20,23,26,27,28,31,33,34,41,44,49,51,55,56,57$ 执行以下步骤:

Step1 选择 n 个满足差分 $X \oplus X^* = (e_{64}, e_{64})$的明文对$(X, X*)$.

Step2 利用密钥 K,K^* 分别加密明文 X,X^*,得到相应的密文 Y,Y^*,其中 $K \oplus K^* = (0,0,e_{64},e_{64})$;

对固定的 s,t 执行 *Step*3 ~ *Step*4:

Step3 抛弃不满足 $Y \oplus Y^* = (e_j, e_{s,t})$ $(1 \leqslant j \leqslant 58, j \neq 3,12,21,30,39,48)$ 的密文对,利用重量为 2 的差分对 $e_{I(j),\Pi(j)} \rightarrow e_{s,t}$恢复出第 12 轮 $P_{64/192}^{-1}$两组 12bit 控制信息,建立密文、控制信息与密钥块 O_1, O_2, O_3 的方程组,将得到两组 12bit 密钥信息 $k_{s,t}^j, k_{s,t}^{j'}$作为整体存入集合 $K_{s,t}^j$.

Step4 对集合 $K_{s,t}^j$中的 12bit 密钥比特链 $k_{s,t}^j, k_{s,t}^{j'}$分别计数,将计数次数不小于 5 次的 12bit 密钥链分别作为正确密钥,存入 $K_{s,t}^j$ *;

Step5 取另一组 s,t 执行 Step3 ~ Step4;

Step6 整理得到 $K^j = \bigcup_{s,t} K_{s,t}^j$ *

攻击算法的成功率和复杂度分析分别由定理 2 和定理 3 给出.

定理 2 $n = 2^{76}$时,利用攻击算法得到的 $K_{s,t}^{j'}$为正确密钥的概率约为 1.

证明 $n = 2^{76}$时,对于给定的 j,s,t,约有 $2^{76} \times 2^{-71} = 2^5$ 个密文对通过 Step3. 正确 $k_{s,t}^j, k_{s,t}^{j'}$的计数次数均不小于 5 次的概率为

$$\left(\sum_{i=5}^{t=2^5} C_t^i \times (\frac{1}{2})^i \times (1-\frac{1}{2})t-i\right)^2 > 0.99.$$

与此同时,错误密钥链的计数次数不小于 5 次的概率为

$$\left(\sum_{i=5}^{t=2^5} C_t^i \times (\frac{1}{2^{12}})^i \times (1-\frac{1}{2^{12}})t-i\right)^2 < 0.01.$$

因此,利用攻击算法得到的 $K_{s,t}^{r'}$ 为正确密钥的概率约为 1. 证毕.

定理 3　$n=2^{76}$ 时,利用攻击算法能够恢复出 CIKS-128 算法的 192 比特密钥信息,计算复杂度为 2^{77} 次 CIKS-128 算法加密,数据复杂度为 2^{77} 个选择明文,存储复杂度为 $2^{25.4}$ 字节.

证明　$n=2^{76}$ 时,攻击算法 Step1 的数据复杂度为 $2^{76}\times 2=2^{77}$ 个选择明文;Step2 计算复杂度为进行 2^{77} 次 CIKS-128 算法加密;Step3 存储密文数据和密钥信息链所需的存储复杂度为 $19\times(C_{64}^2\times 2^5\times 2\times 16+C_{64}^2\times 2^5\times 2\times 12/8)\approx 2^{25.4}$ 字节,Step3 计算密钥信息链的复杂度远小于 Step2 加密算法所需的复杂度,可忽略不计. 因此,攻击算法的计算复杂度为 2^{77} 次 CIKS-128 算法加密,数据复杂度为 2^{77} 个选择明文,存储复杂度为 $2^{25.4}$ 字节.

易知 $O_1\cup O_2\cup O_3=\bigcup_{j\in J}K^j$, $J=\{2,10,16,18,20,23,26,27,28,31,33,34,41,44,49,51,55,56,57\}$,执行加密算法时 $K_1=O_1$, $K_2=O_2$, $K_3=O_3$,即利用攻击算法能够恢复 192 比特密钥. 证毕.

在利用攻击算法恢复出 CIKS-128 算法 192 比特密钥的基础上,对于剩余的 64 比特密钥信息进行穷举攻击,所需的计算复杂度为 2^{64} 次 CIKS-128 算法加密. 由于 $2^{64}+2^{77}\approx 2^{77}$,利用 2^{77} 次 CIKS-128 算法加密,2^{77} 个相关密钥-选择明文以及 $2^{25.4}$ 字节存储空间,即可恢复出 CIKS-128 算法全部 256 比特密钥.

5　结束语

基于 DDP 结构类的分组密码算法主要面向对密码算法的加解密速率和资源占用要求较高的硬件环境,因此算法大多选用简单的密钥生成算法,节省了密钥计算时间和存储空间. 作为一种典型的基于 DDP 结构设计的分组密码算法,CIKS-128 算法具有低能耗、高效率的特点. 本文的分析结果表明,简单的密钥生成算法和 DDP 结构的差分重量平衡性,导致 CIKS-128 算法难以抵抗相关密钥-差分攻击. 表 4 列出了部分典型分组密码算法在相关密钥-差分攻击条件下的最优攻击结果.

对比传统的差分攻击,相关密钥-差分攻击要求密钥生成算法具有较差的差分扩散特性. LBlock、AES-256 的密钥生成算法差分扩散特性较好,相关密钥-差分攻击效果较差. 作为基于 DDP 结构的典型分组密码算法,Cobra-H128、CIKS-128 的密钥生成算法比较简单,密钥长度分别为 128bit 和 256bit,与文献[17]相比,本文以相当的复杂度攻击得到了 CIKS-128 全部 256 密钥比特. 针对 CIKS-128 算法,本文首次恢复出了算法的全部密钥比特,攻击结果明显优于 Youngdai Ko 和 Lee 给出的攻击结果. 分析结果表明,利用 DDP 结构设计算法时,一应当充分考虑 DDP 结构的差分信息泄漏规律,在不影响效率的前提下,利用一些密码学指标较好的变换与 DDP 结构结合使用,提升圈函数密码学指标;二增强密钥生成算法的差分扩散性,降低各圈子密钥的相关性.

表 4　部分算法在相关密钥-差分攻击下的攻击结果

算法	密钥长度	攻击方法	算法轮数	攻击轮数	数据复杂度	时间复杂度	出处
LBlcok	80bit	相关密钥-差分	32	22	$2^{64.1}$	2^{67}	文献[15]
AES-256	256bit	相关密钥-差分	14	14	2^{131}	2^{131}	文献[16]
Cobra-H128	128bit	相关密钥-差分	12	12	2^{76}	2^{76}	文献[17]
CIKS-128	256bit	相关密钥-差分	12	12	2^{77}	2^{77}	本文

参考文献

[1] Moldovyan A A. Fast block ciphers based on controlled permutations[J]. Computer Science Journal of Moldova, 2000,8(3):270 – 283.

[2] Moldovyan A A, Moldovyan N A. A cipher based on data-dependent permutation[J]. Journal of Cryptology, 2002, 15(1):61 – 72.

[3] Sklavos N, Moldovyan N A, Koufopavlou O. High speed networking security:design and implementation of two new DDP-based ciphers[J]. Mobile Networks and Applications-MONET, 2005, 10(1-2):219 – 231.

[4] Minh N, Bac D, Duy H. New SDDO-based block cipher for wireless sensor network security[J]. I. J. Computer Network and Network Security, 2010, 10(3):54 – 60.

[5] Bac Do Thi, Minh Nguyen Hieu, Duy Ho Ngoc. An effective and secure cipher based on SDDO[J]. I. J. Computer Network and Information Security, 2012, 4(11):1 – 10.

[6] Biryukov A, Nikolic I. Search for related-key differential characteristics in DES-Like ciphers[A]. LNCS 6733:FSE 2011[C]. Lyngby, Denmark:Springer, 2011. 18 – 34.

[7] Minier M, Naya-Plasencia M. A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock[J]. Information Processing Letters, 2012,

112(16):624 -629.

[8] 詹英杰,关杰,丁林,等. 对简化版 LBLock 算法的相关密钥不可能差分攻击[J]. 电子与信息学报,2012,34(9):2161 -2166.
Zhan Ying-jie, Guan Jie, Ding Lin, et al. Related-key impossible differential attack on reduced round LBlock[J]. Journal of Electronics & Information Technology, 2012, 34(9):2161 -2166. (in Chinese)

[9] Tomer Ashur, Orr Dunkelman. A practical related-key boomerang attack for the full MMB block cipher[A]. LNCS 8257:Cryptology and Network Security 2013[C]. Paraty, Brazil: Springer. 2013. 20 -22.

[10] Marine Minier. On the security of piccolo lightweight block cipher against related-key impossible differentials [A]. LNCS 8250:INDOCRYPR 2013[C]. Mumbai, India: Springer, 2013. 308 -318.

[11] Lee Changhoon, Lee Sangjin, Park Jong Hyuk, et al. Security analysis of pure DDP-based cipher proper for multimedia and ubiquitous device[J]. Telecommunication System, 2010, 44(3-4):267 -279.

[12] Kang Jinkeon, Jeong Kitae, Yeo Sang-Soo, et al. Related-key attack on the MD-64 block cipher suitable for pervasive computing environments[A]. 26th International Conference on Advanced Information Networking and Applications Workshops(WAINA 2012)[C]. Fukuoka: IEEE, 2012. 726 -731.

[13] Ko Youngdai, Lee Changhoon, Hong Seokhie, et al. Related-key attacks on DDP based ciphers: CIKS-128 and CIKS-128H[A]. LNCS 3348: INDOCRYPT 2004[C]. Chennai, India: Springer, 2004. 191 -205.

[14] Lee Changhoon, Kim Jongsung, Sung Jaechul, et al. Cryptanalysis of CIKS-128 and CIKS-128H suitable for intelligent multimedia and ubiquitous computing systems [J]. Computing and Informatics, 2011, 30(3): 447 -466.

[15] Shusheng Liu, Zheng Gong, Libian Wang. Improved related-key differential attacks on reduced-round LBlock[A]. Information and Communications Security-14th International Conference(ICICS 2012)[C]. Hong Kong, China: Springer, 2012. 58 -69.

[16] Alex Biryukov, Dmitry Khovratovich, Ivica Nikoli′c. Distinguisher and related-key attack on the full AES-256 [A]. CRYPTO'09, Santa Barbara [C]. CA, USA: Springer, 2009. 231 -249.

[17] 罗伟,郭建胜. Cobra-H64/128 算法的相关密钥-差分攻击[J]. 电子学报,2013,41(8):1569 -1573.
LUO Wei, GUO Jian-sheng. Related-key differetial attacks on cobra-H64/128[J]. Acta Electronica Sinica, 2013, 41(8):1569 -1573. (in Chinese)

作者简介

郭建胜 男,1972 年出生,河南沁阳人,博士,解放军信息工程大学教授、博士生导师,主要研究方向为密码学和信息安全.
E-mail: tsg_31@126.com

崔竞一(通讯作者) 男,1992 出生,河南登封人,解放军信息工程大学硕士生,主要研究方向为密码分析.
E-mail: tsg_31@126.com