LBlock 算法的相关密钥 - 不可能差分攻击

黄永洪[1],郭建胜[2,4],罗 伟[3]
(1. 重庆邮电大学,重庆 400065;2. 解放军信息工程大学,河南郑州 450004;
3.78179 部队,四川成都 611830;4.信息保障技术重点实验室,北京 100000)

摘 要: 该文研究了 LBlock 分组密码算法在相关密钥-不可能差分条件下的安全性.利用子密钥生成算法的差分信息泄漏规律,构造了多条低重量子密钥差分链,给出了 15 轮相关密钥-不可能差分区分器.通过扩展区分器,给出了 23 轮和 24 轮 LBlock 算法的相关密钥-不可能差分攻击方法.攻击所需的数据复杂度分别为 $2^{65.2}$和 $2^{65.6}$个选择明文,计算复杂度分别为 $2^{66.2}$次 23 轮 LBlock 算法加密和 $2^{66.6}$次 24 轮 LBlock 算法加密,存储复杂度分别为 $2^{61.2}$和 $2^{77.2}$字节存储空间.与已有结果相比,首次将针对 LBlock 算法的攻击扩展到了 23 轮和 24 轮.

关键词: 分组密码; 密码分析; LBlock 算法; 相关密钥-不可能差分攻击
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2015)10-1948-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.10.011

Related-Key Impossible Differential Attacks on LBlock

HUANG Yong-hong[1], GUO Jian-sheng[2,4], LUO Wei[3]
(1. *Chongqing University of Posts and Telecommunications*, *Chongqing* 400065, *China*;
2. *The PLA Information Engineering University*, *Zhengzhou*, *Henan* 450004, *China*;
3. *The PLA Unit* 78179, *Chengdu*, *Sichuan* 611830, *China*;
4. *Science and Technology on Information Assurance Laboratory*, *Beijing* 100000, *China*)

Abstract: In this paper, the strength of LBlock against related-key impossible differential attack is examined. Based on the differential information leakages in sub-key schedule, several sub-key differentials in low weight are constructed, and a 15-round related-key impossible differential distinguisher of LBlock is presented. By extending the distinguisher, related-key impossible differential attacks on 23-round LBlock and 24-round LBlock are presented. The data complexities of the attacks are $2^{65.2}$ and $2^{65.6}$ chosen-plain-text, respectively; the computing complexities of the attacks are $2^{66.2}$ 23-round LBlock encryptions and $2^{66.6}$ 24-round LBlock encryptions, respectively; the storage complexities of the attacks are $2^{61.2}$ and $2^{77.2}$ bytes of memory space, respectively. The cryptanalysis of reduced-round LBlock are first extended to 23-round and 24-round in this paper.

Key words: block cipher; cryptanalysis; LBlock; related-key impossible differential attack

1 引言

近年来,为了满足资源受限环境对密码算法的应用需求,各国研究人员提出了一系列轻量级密码算法,如 Klein[1], LED[2], PRINTcipher[3], Piccolo[4] 以及 PRINCE[5] 等.作为分组算法设计的重要环节,子密钥生成算法成为制约分组密码算法安全性的关键因素.针对各种类型的密码算法,研究人员提出了一系列相关密钥条件下的安全性分析成果[6~8].

作为轻量级分组密码算法的典型代表,LBlock 算法由我国学者吴文玲等人[9]于 2011 年 ANCS 会议上提出.针对该算法的安全性,设计者构造了 14 轮的不可能差分区分器,给出了 20 轮的不可能差分攻击结果[9];Liu 等人[10]利用不可能差分分析方法对 21 轮算法进行攻击;Ferhat Karakoç 等人[11]对 21 轮和 22 轮算法分别进行攻击,但攻击所需计算量较高;郭等人[12]通过扩展 14 不可能差分区分器,减小了攻击 22 轮算法所需的复杂度;Marine Minier 等人[13]利用两种密钥差分给出了 22 轮算法的相关密钥-不可能差分攻击.

本文研究了 LBlock 算法的相关密钥-不可能差分性质.在构造 15 轮相关密钥-不可能差分区分器的基础上,首次给出 23 轮和 24 轮的 LBlock 算法的相关密钥-不可能差分分析方法.

表 1 给出了针对 LBlock 算法的攻击情况.

收稿日期:2014-06-18;修回日期:2014-10-15;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61272488);博士后科学基金(No.2014M562582)

表 1　LBlock 算法的攻击对比

攻击轮数	攻击方法	数据复杂度	计算复杂度	存储复杂度	出处
20	不可能差分	2^{63}	$2^{72.7}$	\	[9]
21	不可能差分	$2^{62.5}$	$2^{73.7}$	\	[10]
21	不可能差分	\	$2^{79.28}$	\	[11]
22	不可能差分	$2^{62.5}$	$2^{63.5}$	\	[12]
22	相关密钥-不可能差分	2^{68}	2^{70}	\	[13]
23	相关密钥-不可能差分	$2^{65.2}$	$2^{66.2}$	$2^{61.2}$	本文
24	相关密钥-不可能差分	$2^{65.6}$	$2^{66.6}$	$2^{77.2}$	本文

2　相关知识

2.1　符号约定

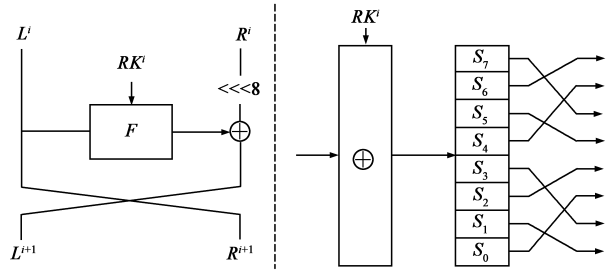
本文常用符号约定如下:

K	算法主密钥
RK^i	第 i 轮子密钥 RK^i
K^i	经过 i 轮变换后,寄存器中密钥的取值
L_j^i	第 i 轮输入左半部分第 j 个 4bit 数据块
k_i	主密钥 K 的第 i 比特
RK_j^i	第 i 轮第 j 个 4bit 密钥块
k_i^j	K^j的第 i 比特
R_j^i	第 i 轮输入右半部分第 j 个 4bit 数据块

本文约定所有数据左侧为最高位,右侧为最低位,且最低位从 0 开始计数.

2.2　LBlock 算法介绍

LBlock 算法采用 Feistel 结构,分组长度为 64bit,密钥长度为 80bit,设计轮数为 32 轮,算法圈函数和 F 函数结构如图 1(a)和图 1(b)所示.具体细节可参考文献[9].



(a) 圈函数结构　　(b) F函数结构

图1　LBlock算法结构

3　相关密钥-不可能差分区分器

3.1　子密钥差分链

LBlock 子密钥生成算法每得到 1 轮圈子密钥至多有 $k_{79-76}, k_{75-72}, k_{50-46}$共 13 比特参与更新,因此算法的差分扩散效率较低.

当 $\Delta K = 020\cdots0_{16}$时,子密钥生成算法第 12 轮输入差分为 $\Delta K^{11} = 010\cdots0_{16}$,即 S_8 输入差分重量为 1. 根据 S_8的差分分布表,构造出如表 2 所示的 6 条低重量密钥差分链.

第 1 条密钥差分链中,$k_{76}k_{75}k_{74}k_{73}$取值为 6,7,12,13,S_8输出数据对应值为 0,6,2,4,第 12 轮子密钥差分 $\Delta RK^{12} = 0600,0000_{16}$. 子密钥生成算法第 23 轮输入差分为 $\Delta K^{22} = 030\cdots0_{16}$,根据 S_8的差分分布,x_1 可能的取值有 1,5,9,13. 结合第 12 轮子密钥取值情况,得到表 3 对应关系:

表 3　x_i取值情况

x_i	$k_{46}^{22}k_{76}k_{75}k_{74}k_{73}$	x_i	$k_{46}^{22}k_{76}k_{75}k_{74}k_{73}$
13	00110,00111	2	01010,01011
x_1		x_3	
9	01100,01101	6	11010,11011
1	10110,10111	13	01000,01001
		x_4	
5	11100,11101	5	11000,11001
6	00100,00101	8	00010,00011
		x_5	
15	01110,01111	10	10010,10011
x_2			
2	10100,10101	10	00000,00001
		x_6	
7	11110,11111	8	10000,10001

3.2　15 轮相关密钥-不可能差分区分器

根据表 1 所示的 6 条密钥差分链,选取前 24 轮非零 4bit 块最多的第 6 条密钥差分链,以(00000000,00000000x)为输入差分构造第 5 轮到第 11 轮的 7 轮相关密钥-差分特征,以(00000000,000000000)为输出差分构造解密方向第 19 轮到第 12 轮的 8 轮相关密钥-差分特征.

如图 2 所示,加密方向 7 轮相关密钥-差分特征输出差分(????? * ??,?? * 0??? *)第 10 个4bit 块为“ * ”,解密方向 8 轮相关密钥-差分特征输出差分(? *? *? 0? *,????????)第 10 个 4bit 块为“0”,构成矛盾,即图 2 给出了 1 个 15 轮(第 5 轮到第 19 轮)相关密钥-不可能差分区分器.

进一步观察表 2,第 6 条密钥差分非零块位置涵盖了前 5 条密钥差分链所有非零块位置,因此利用前 5 条密钥差分链均可构造 15 轮相关密钥-不可能差分区分器:

$$(\ 00000000,\ 0000000x\ ) \xrightarrow{5\text{ 到 }11\text{ 轮}} \times \xleftarrow{19\text{ 到 }12\text{ 轮}} (00000000,00000000)$$

表 2 LBlock 算法的 6 条低重量密钥差分链

轮次	密钥差分链 1	密钥差分链 2	密钥差分链 3	密钥差分链 4	密钥差分链 5	密钥差分链 6
1	**02000000**	**02000000**	**02000000**	**02000000**	**02000000**	**02000000**
2	00000000	00000000	00000000	00000000	00000000	00000000
3	**00000008**	**00000008**	**00000008**	**00000008**	**00000008**	**00000008**
4	00000000	00000000	00000000	00000000	00000000	00000000
5	00000000	00000000	00000000	00000000	00000000	00000000
6	**00000400**	**00000400**	**00000400**	**00000400**	**00000400**	**00000400**
7	00000000	00000000	00000000	00000000	00000000	00000000
8	00000000	00000000	00000000	00000000	00000000	00000000
9	**00020000**	**00020000**	**00020000**	**00020000**	**00020000**	**00020000**
10	00000000	00000000	00000000	00000000	00000000	00000000
11	00000000	00000000	00000000	00000000	00000000	00000000
12	**06000000**	**02000000**	**03000000**	**07000000**	**0b000000**	**0f000000**
13	00000000	00000000	00000000	00000000	00000000	00000000
14	**00000018**	**00000008**	**0000000c**	**0000001c**	**0000002c**	**0000003c**
15	00000000	00000000	00000000	00000000	00000000	00000000
16	00000000	00000000	00000000	00000000	00000000	00000000
17	**00000c00**	**00000400**	**00000600**	**00000d00**	**00001600**	**00001d00**
18	00000000	00000000	00000000	00000000	00000000	00000000
19	00000000	00000000	00000000	00000000	00000000	00000000
20	**00060000**	**00020000**	**00030000**	**00070000**	**000b0000**	**000f0000**
21	00000000	00000000	00000000	00000000	00000000	00000000
22	00000000	00000000	00000000	00000000	00000000	00000000
23	**0$x_1$000000**	**0$x_2$000000**	**0$x_3$800000**	**0$x_4$800000**	**0$x_5$800000**	**0$x_6$800000**
24	00000000	00000000	00000000	00000000	00000000	00000000

记“*”表示非零 4bit 块,“?”表示未知 4bit 块,“x”表示已知 4bit 块.

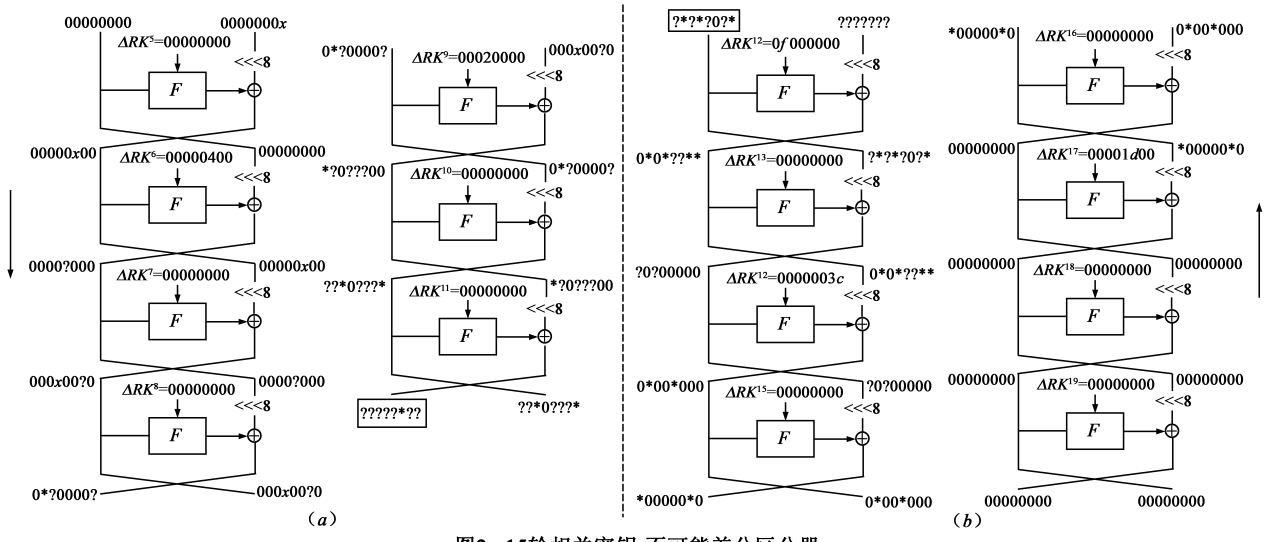


图2 15轮相关密钥-不可能差分区分器

4 相关密钥-不可能差分攻击算法

15 轮相关密钥-不可能差分区分器输入差分为(00000000,0000000x),在表 2 所示的 6 条密钥差分链条件下逆向扩展 4 轮,得到明文差分为($0c_1c_3$0000c_4,$0c_2c_5x0c_6$0c_7),如图 3 所示.

4.1 23 轮 LBlock 的相关密钥-不可能差分攻击

15 轮区分器在表 2 所示的第 1 条和第 6 条密钥差分链条件下,分别正向扩展 4 轮,如图 4 所示,得到 23 轮 LBlock 算法加密输出差分为($d_4$00$d_5$0$d_6d_2$0,00$d_3$0000d_1).

对比图 4(*a*)和图 4(*b*)可知,两条差分链正向扩展输出差分形式相同.根据表 2 中 6 条密钥差分链第 20 轮到第 23 轮密钥差分非零块的位置,对 15 轮区分器正向扩展 4 轮后输出差分均为($d_4$00$d_5$0$d_6$$d_2$0,00$d_3$0000$d_1$).

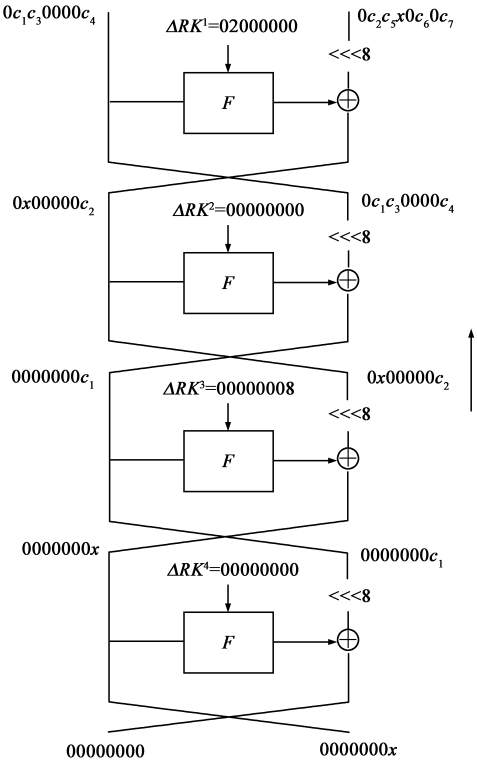


图3　逆向扩展4轮

结合图 3 和图 4 的扩展情况,选取密钥差分 $\Delta K = 020\cdots0_{16}$给出攻击算法 1.

攻击算法 1

Step1 选择 n 个形如($C**CCCC*$, $C***C*C*$)的明文结构,其中"C"表示该 4bit 块取固定值,"$*$"表示取遍 2^4 个值.利用 n 个明文结构构造出 $2^{63}n$ 个明文对.

Step2 利用关联密钥 K, K' 加密明文,排除 23 轮加密后密文差分第 1,2,3,4,6,7,8,11,13,14 块非 0 的明文对,剩余 $2^{63}n \times 2^{-40} = 2^{23}n$ 个明文对.

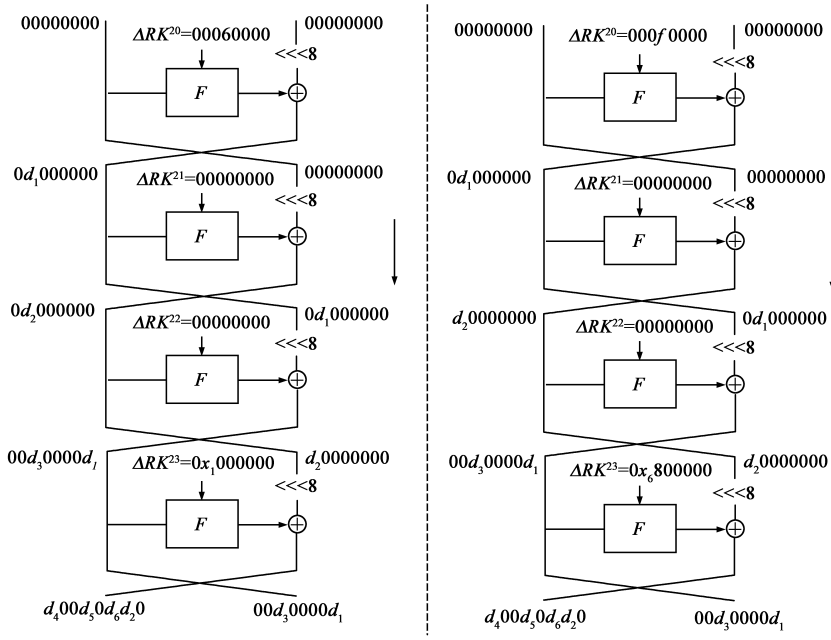
Step3 猜测 K_0^1, K_5^1, K_6^1. 对明文对进行第 1 轮加密,排除输出差分左半部分第 1,2,3,4,5,7 块非 0 的明文对,剩余 $2^{23}n \times 2^{-12} = 2^{11}n$ 明文对.

Step4 猜测 $K_0^2 \oplus L_0^2$, $K_6^2 \oplus L_6^2$. 类似 Step3 剩余明文对 $2^{11}n \times 2^{-8} = 2^3 n$.

Step5 猜测 $K_0^3 \oplus L_0^3$. 类似 Step3 剩余明文对 $2^3 n \times 2^{-4} = 2^{-1}n$.

Step6 猜测 $K_0^4 \oplus L_0^4$. 类似 Step3 剩余明文对数量为 $2^{-1}n \times 2^{-4} = 2^{-5}n$.

Step7 猜测 K_0^{23}, K_5^{23}, K_6^{23}. 对 28bit 数据猜测值对应的密文对进行第 23 轮部分解密,排除第 22 轮输出差分右半部分第 0,1,2,3,4,5,6 块不为 0 的密文对.第 1,2 条密钥差分链剩余密文对 $2^{-5}n \times 2^{-12} \times 4 = 2^{-15}n$,第 3~6 条密钥差分链剩余密文对 $2^{-5}n \times 2^{-12} \times 2 = 2^{-16}n$,分别标记每条密钥差分链剩余密文对解密时对应 x_i取值.



(*a*) 第1条密钥差分链条件下正向扩展4轮　　(*b*) 第6条密钥差分链条件下正向扩展4轮

图4　正向扩展4轮

Step8 猜测 $K_7^{22} \oplus L_7^{22}$. 对 40bit 数据猜测值剩余的密文对分别进行第 22 轮部分解密,排除第 21 轮输出差分右半部分第 0,1,2,3,4,5,7 块不为 0 的密文对.第 1,2 条密钥差分链剩余密文对 $2^{-15}n \times 2^{-4} = 2^{-19}n$,第 3 ~ 6 条密钥差分链剩余密文对 $2^{-16}n \times 2^{-4} = 2^{-20}n$.

Step9 猜测 $K_6^{21} \oplus L_6^{21}$. 对剩余密文对分别进行第 21 轮部分解密,排除第 20 轮输出差分右半部分不为 0 的密文对.第 1,2 条密钥差分链剩余密文对 $2^{-19}n \times 2^{-4} = 2^{-23}n$,第 3 ~ 6 条密钥差分链剩余密文对数量为 $2^{-20}n \times 2^{-4} = 2^{-24}n$.

Step10 猜测 $K_4^{20} \oplus L_4^{20}$. 对剩余密文对分别进行第 20 轮部分解密,排除第 19 轮输出差分右半部分不为 0 的密文对.若有密文对剩余,根据不可能差分性质,猜测一定错误.

取 $n = 33.2$ 时,$2^{52} \times (1 - 2^{-4})^{2^{-24}n} < 1$ 时,算法能够得到 52bit 猜测数据的唯一正确值.

定理 1 攻击算法 1 数据复杂度为 $2^{65.2}$个选择明文;计算复杂度为 $2^{66.2}$次 23 轮 LBlock 算法加密;存储复杂度为 $2^{61.2}$字节.

证明 $n = 2^{33.2}$时,Step1 的数据复杂度为 $2^{32}n = 2^{65.2}$个选择明文. Step2 利用关联密钥加密需要 $2 \times 2^{65.2} = 2^{66.2}$次 23 轮 LBlock 算法加密,存储 $2^{23}n = 2^{56.2}$个明文对及其对应密文对需要 $2^{56.2} \times 4 \times 8 = 2^{61.2}$字节.

Step3, Step4, Step7 需要猜测多个 4bit 数据,采用"Early Abort"技术[14],以 Step3 为例:首先猜测 K_0^1,判断 $S_0(L_0^1 \oplus K_0^1) \oplus S_0(L_0^1 \oplus \Delta L_0^1 \oplus K_0^1)$与 ΔR_0^1 是否相等,排除不符合的明文对;其次猜测 K_5^1,判断 $S_5(L_5^1 \oplus K_5^1) \oplus S_5(L_5^1 \oplus \Delta L_5^1 \oplus K_5^1)$与 ΔR_2^1 是否相等,排除不符合的明文对;最后猜测 K_6^1,判断 $S_6(L_6^1 \oplus K_6^1) \oplus S_6(L_6^1 \oplus \Delta L_6^1 \oplus K_6^1)$与 ΔR_5^1 是否相等,排除不符合的明文对.共需 $2 \times (2^{56.2} \times 2^4 + 2^{52.2} \times 2^8 + 2^{48.2} \times 2^{12})/8/23 \approx 2^{55.3}$次 23 轮 LBlock 算法加密.由此分析得到,Step3 ~ Step11 所需的计算复杂度总和远小于加密选择明文所需的计算复杂度,即攻击算法 1 的计算复杂度约为 $2^{66.2}$次 23 轮 LBlock 算法加密. 证毕

4.2 24 轮 LBlock 的相关密钥-不可能差分攻击

对图 4 所示的差分向下扩展 1 轮,得到输出差分为 $(d_3 d_8 d_7 0 d_9 d_1 0 d_{10}, d_4 00 d_5 0 d_6 d_2 0)$的 15 轮区分器.类似于攻击算法 1,对差分为$(0c_1 c_3 0000 c_4, 0c_2 c_5 x 0 c_6 0 c_7)$的明文对进行加密,筛选出差分为$(d_3 d_8 d_7 0 d_9 d_1 0 d_{10}, d_4 00 d_5 0 d_6 d_2 0)$的密文对,攻击 24 轮 LBlock 算法总共猜测 17 块,要排除错误猜测需 $2^{68} \times (1 - 2^{-4})^{2^{-24}m} < 1$. 取 $m = 2^{33.6}$,能够得到 68bit 猜测数据正确值.攻击 24 轮 LBlock 算法的数据复杂度为 $2^{65.6}$个选择明文;计算复杂度为 $2^{66.6}$次 24 轮 LBlock 算法加密;存储复杂度为 $2^{39}m \times 4 \times 8 = 2^{77.2}$字节.

5 结束语

本文利用 LBlock 子密钥生成算法差分扩散不充分的信息泄漏规律,构造了多条低重量密钥差分链,给出了 15 轮相关密钥-不可能差分区分器,首次给出了 23 轮和 24 轮 LBlock 算法的攻击方法.

参考文献

[1] Gong Z, Nikove S, Law Y W. KLEIN: a new family of lightweight block ciphers [J]. RFID Security and Privacy, 2012, LNCS 7055: 1 – 18.

[2] Guo J, Peyein T, Poschmann A, et al. The LED block cipher [A]. CHES 2011 [C]. Nara, Japan, LNCS 6917, 2011. 326 – 341.

[3] Knudsen L, Leander G, Poschmann A, et al. PRINTcipher: a block cipher for IC-Printing [A]. CHES 2010 [C]. Santa Barbara, USA, LNCS 6225, 2010. 16 – 32.

[4] Shibutani K, Isobe T, Hiwatari H, et al. Piccolo: an ultra-lightweight block cipher [A]. CHES 2011 [C]. Nara, Japan, LNCS 6917, 2011. 342 – 357.

[5] Borghoff J, Canteaut A, Güneysu T, et al. PRINCE-a low-latency block cipher for pervasive computing applications [A]. ASIACRYPT 2012 [C]. Beijing, China, LNCS 7658, 2012. 208 – 225.

[6] 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 Jiansheng. Related-key differential attack on Cobra-H64 [J]. Acta Electronica Sinica, 2013, 41(8): 1569 – 1573. (in Chinese)

[7] Hu Z, Qin Z. Related key impossible differential cryptanalysis of AES-256 [J]. International Journal of Advancements in Computing Technology, 2012, 4(3): 91 – 98.

[8] Ding Lin, Guan Jie. Related-key chosen IV attack on K2 [J]. Chinese Journal of Electronics, 2011, 20(2): 365 – 369.

[9] Wu W L, Zhang L. LBlock: a lightweight block cipher [A]. ANCS 2011 [C]. Nerja, Spain, LNCS 6715, 2011. 327-344.

[10] Liu Y, Gu D, Liu Z, et al. Impossible differential attacks on reduced-round LBlock [A]. ISPEC 2012 [C]. Hangzhou, China, LNCS 7232, 2012. 97 – 108.

[11] Karakoc F, Demirci H, Harmanca E. Impossible differential cryptanalysis of reduced-round LBlock [A]. WISTP 2012 [C]. Egham, UK, LNCS 7322, 2012. 179 – 188.

[12] 郭建胜,罗伟,张磊,等. LBLock 码的不可能差分密码性能分析 [J]. 电子与信息学报, 2013, 35(6): 1516 – 1519.
Guo Jiansheng, Luo Wei, Zhang Lei, et al. Impossible differential cryptanalysis of LBlock code [J]. Journal of Electronics

& Information Technology, 2013, 35(6): 1516 – 1519. (in Chinese)

[13] 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.

[14] Lu J, Kim J, Nathan K, et al. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1[A]. RSA 2008[C]. San Francisco, CA, USA, LNCS 4964, 2008. 370 – 386.

作者简介

黄永洪　男. 1974 年 5 月出生,重庆永川人. 工程师. 2000 年获信息工程大学硕士学位. 研究方向为信息安全和电子证据.

郭建胜(通讯作者)　男. 1972 年 6 月出生,河南沁阳人. 教授、博士生导师. 2004 年获解放军信息工程大学博士学位. 主要研究方向为信息安全.

E-mail: tsg_31@126.com