LBlock 码的不可能差分密码性能分析

郭建胜*① 罗 伟① 张 磊② 郭渊博①
①(解放军信息工程大学 郑州 450004)
②(沈阳市 65012 部队 沈阳 110001)

摘 要：该文分析研究了LBlock分组密码算法的不可能差分性质。基于LBlock算法的轮函数结构和部分密钥分别猜测技术，给出了 21 轮和 22 轮的LBlock算法的不可能差分分析方法。攻击 21 轮LBlock算法所需的数据量约为 2^{62}，计算量约为 2^{62}次 21 轮加密；攻击 22 轮LBlock算法所需的数据量约为 $2^{62.5}$，计算量约为 $2^{63.5}$次 22 轮加密。与已有的结果相比较，分析所需的计算量均有明显的降低，是目前不可能差分分析攻击LBlock的最好结果。

关键词：分组密码；不可能差分分析；LBlock 分组密码；计算复杂性
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2013)06-1516-04
DOI: 10.3724/SP.J.1146.2012.01384

Impossible Differential Cryptanalysis of LBlock Code

Guo Jian-sheng① Luo Wei① Zhang Lei② Guo Yuan-bo①
①(*The PLA Information Engineering University*, *Zhengzhou* 450004, *China*)
②(*Unit* 65012 *of the PLA*, *Shenyang* 110001, *China*)

Abstract: The impossible differential property of LBlock block cipher is analyzed. Based on the property of the structure of round function and the technology of key-byte guessing, two impossible differential attacks on 21-round and 22-round reduced LBlock are presented. It is shown that the attack on 21-round requires about 2^{62} chosen plaintexts and 2^{62} 21-round encryptions, and on 22-round requires about $2^{62.5}$ chosen plaintexts and $2^{63.5}$ 22-round encryptions. The presented results are the best impossible differential attack on reduced-round LBlock so far.

Key words: Block cipher; Impossible differential cryptanalysis; LBlock block cipher; Computation complexity

1 引言

随着电子信息技术的快速发展，RFID(Radio Frequency IDentification)技术被广泛应用于生活的各个领域。传统加密算法在加密效率和硬件占用资源方面都不能很好地满足应用环境的要求。为了适应新技术的发展，各国的研究者相继提出了一些轻重量级的密码算法，如HIGHT[1], PRESENT[2], MIBS[3], KATAN[4], KTANTAN[4]等。

在 2011 年ANCS会议上，吴文玲等人[5,6]提出了LBlock轻重量级的分组密码算法。LBlock算法整体采用Feistel结构，分组长度为 64 bit，设计轮数为 32 轮。在算法设计报告中，作者评估了算法在差分分析、线性分析、不可能差分分析等多种分析方法下的安全性。在不可能差分分析方面，通过构造给出的 14 轮的不可能差分区分器，作者研究了 20 轮LBlock的不可能差分性质，其攻击所需的数据量为 2^{63} 个选择明文，计算量为 $2^{72.7}$ 次 20 轮加密[5,6]。

针对LBlock算法，Liu等人[7]利用不可能差分分析方法对 21 轮LBlock算法进行攻击，攻击算法需要 $2^{62.5}$ 个选择明文，计算量为 $2^{73.7}$次 21 轮加密。同样利用不可能差分分析方法，Karakoç等人[8]对 21 轮和 22 轮算法分别进行攻击，所需计算量分别为 $2^{69.5}$ 次 21 轮加密和 $2^{79.28}$次 22 轮加密。

本文研究了LBlock算法的不可能差分性质。在 14 轮不可能差分区分器的基础上，结合部分密钥分别猜测技术[9]，给出了 21 轮和 22 轮的LBlock算法的不可能差分分析方法，相应的攻击结果是不可能差分分析攻击LBlock算法的最好结果。分析结果表明，22 轮LBlock算法在不可能差分攻击下是不免疫的。

2012-10-26 收到，2012-12-28 改回
国家自然科学基金(11204379)和河南省科技创新杰出青年计划项目(104100510025)资助课题
*通信作者：郭建胜 guojs_crypt@126.com

2　LBlock 算法简介

LBlock 算法的分组长度为 64 bit，密钥长度为 80 bit，加密轮数为 32 轮，轮函数结构如图 1 所示。每一轮的轮函数包括轮子密钥加变换、非线性的 S 盒变换和扩散 P 变换 3 类变换。轮子密钥加变换为加密的中间状态与轮子密钥的模 2 加变换；LBlock 算法在非线性变换中使用了 8 个不同的 4 bit 进 4 bit 出的 S 盒变换；扩散 P 变换为 4 bit 块之间的位置变换。轮变换中 F 函数的具体结构如图 2 所示。

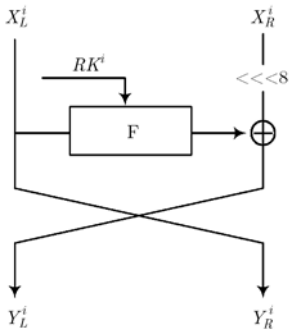

图 1 LBlock 算法的轮函数结构

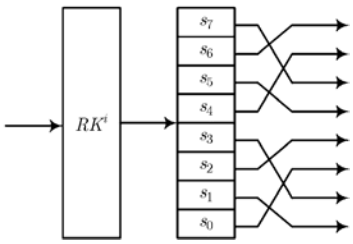

图 2 轮变换中 F 函数的结构

设算法的明文输入为 $X=(X_L,X_R)$，第 i 轮的输入为 $X^i=(X_L^i,X_R^i)$，输出为 $Y^i=(Y_L^i,Y_R^i)$，其中 $X_L,X_R\in\{0,1\}^{32}$，最右边代表最低比特位，$X_L^0=X_L$，$X_R^0=X_R$，$X_L^i=Y_L^{i-1}$，$X_R^i=Y_R^{i-1}$，则 LBlock 算法的加密过程为：当 $1\le i\le 31$ 时，有 $Y_L^i=P(S(X_L^i\oplus RK^i))\oplus(X_R^i<<<8)$，$Y_R^i=X_L^{i-1}$；当 $i=32$ 时，有 $Y_L^{32}=X_L^{31}$，$Y_R^{32}=P(S(X_L^{31}\oplus RK^{31}))\oplus(X_R^{31}<<<8)$。LBlock 算法的解密算法结构与加密结构类似，这里不再叙述。

3　LBlock 的不可能差分分析

3.1 21 轮 LBlock 的不可能差分分析

吴文玲等人[5,6]在算法的设计报告中，构造出了一条 14 轮的不可能差分区分器。具体为

$$(00000000,00\alpha00000)\xrightarrow{8r}\times\xleftarrow{6r}(0\beta000000,00000000)$$

这里 α,β 为任意非零的 4 bit 数。

针对上述 14 轮的不可能差分区分器，通过改变非零差分块 α,β 的位置，可以得到一系列 14 轮不可能差分区分器，如：

(1) $(00000000,\alpha0000000)\xrightarrow{8r}\times\xleftarrow{6r}(\beta0000000,00000000)$；

(2) $(00000000,\alpha0000000)\xrightarrow{8r}\times\xleftarrow{6r}(000\beta0000,00000000)$；

(3) $(00000000,0\alpha000000)\xrightarrow{8r}\times\xleftarrow{6r}(0000\beta000,00000000)$。

利用这些构造的不可能差分区分器，按照 LBlock 算法通过直接向前扩展 3 轮，向后扩展 4 轮构造出针对 21 轮 LBlock 算法的不可能差分区分器，进而实现对 21 轮 LBlock 算法的不可能差分分析。

下面以 14 轮不可能差分区分器 $(00000000,\alpha0000000)\xrightarrow{8r}\times\xleftarrow{6r}(\beta0000000,00000000)$ 为例，分析 21 轮 LBlock 算法在不可能差分分析下的安全性。首先给出相应的 21 轮 LBlock 算法的不可能差分区分器结构，如图 3 所示。

基于图 3 给出的 21 轮 LBlock 算法的不可能差分区分器，下面给出针对 21 轮 LBlock 算法的不可能差分分析算法，具体由算法 1 给出。

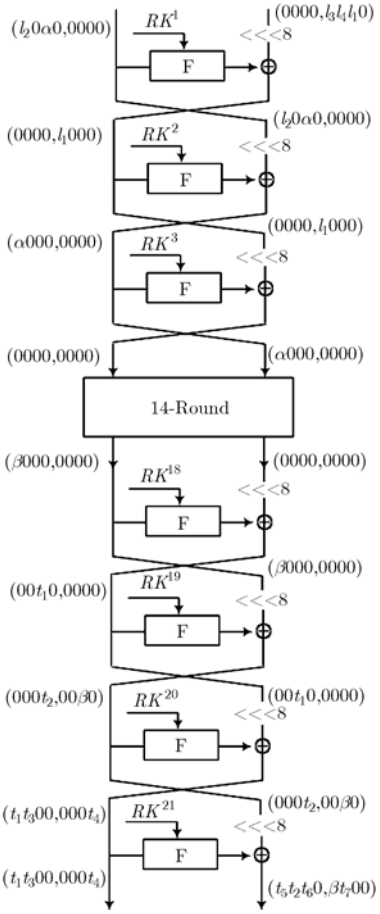

图 3 21 轮 LBlock 算法的不可能差分分析

算法 1

步骤 1 选择 n 个形如$(*C*C,CCCC,CCCC,***C)$的明文结构，其中 C 代表这 4 bit 块取固定值，$*$代表这 4 bit 块取遍2^4个值。这样的结构可构成$2^{20}\times(2^{20}-1)/2\approx 2^{39}$个输入明文对在 5 个 4 bit 块位置的差分值不为 0，其它比特块位置的差分值均为 0，从而 n 个明文结构可构成$2^{39}n$个输入明文对。

步骤 2 考察经过 21 轮加密后这$2^{39}n$个输入明文对对应的密文输出，排除那些在第 0,1,4,9,10,11,12,13 这 8 个 4 bit 块不为 0 的对应密文对。经过筛选后，剩余密文对的数量为$2^{39}n\times 2^{-32}=2^7 n$。

步骤 3 猜测$RK_0^{21},RK_6^{21},RK_7^{21}$这 12 bit 的子密钥，对剩余的$2^7 n$个密文对，部分解密第 21 轮加密运算，得到 20 轮加密的输出差分。判断其输出的右半部分在第 0,2,3,5,6,7 这 6 个 4 bit 块位置是否为 0，排除那些不为 0 的差分值输入。经过筛选后，剩余密文对的数量为$2^7 n\times 2^{-12}=2^{-5}n$。

步骤 4 猜测RK_1^{20},RK_4^{20}这 8 bit 的子密钥，对剩余的$2^{-5}n$个密文对，部分解密第 20 轮加密运算，得到 19 轮加密的输出差分。判断其输出的右半部分在第 0,1,2,3,4,6,7 这 7 个 4 bit 块位置是否为 0，排除那些不为 0 的差分值输入。经过筛选后，剩余密文对的数量为$2^{-5}n\times 2^{-8}=2^{-13}n$。

步骤 5 猜测RK_5^{19}这 4 bit 的子密钥，对剩余的$2^{-13}n$个密文对，部分解密第 19 轮加密运算，判断第 18 轮的加密右半部分输出是否在第 0,1,2,3,4,5,6 这 7 个 4 bit 块位置差分值为 0，排除那些不为 0 的差分值输入。经过筛选后，剩余密文对的数量为$2^{-13}n\times 2^{-4}=2^{-17}n$。

步骤 6 猜测RK_7^{18}这 4 bit 的子密钥，对剩余的$2^{-17}n$个密文对，部分解密第 18 轮加密运算，判断第 17 轮的加密右半部分输出差分是否全部为 0，排除那些不为 0 的差分值输入。经过筛选后，剩余密文对的数量为$2^{-17}n\times 2^{-4}=2^{-21}n$。

步骤 7 猜测RK_5^1,RK_7^1这 8 bit 的子密钥，对剩余的$2^{-21}n$个对应明文对，部分加密第 1 轮明文，判断其左半部分输出是否在第 0,1,2,4,5,6,7 这 7 个 4 bit 块位置差分值为 0，排除那些不为 0 的差分值输入。经过筛选后，剩余明文对的数量为$2^{-21}n\times 2^{-8}=2^{-29}n$。

步骤 8 猜测RK_3^2这 4 bit 的子密钥，对剩余的$2^{-29}n$个对应明文对，进行部分第 2 轮加密运算，判断其左半部分输出是否在第 0,1,2,3,4,5,6 这 7 个 4 bit 块位置差分值为 0，排除那些不为 0 的差分值输入。经过筛选后，剩余明文对的数量为$2^{-29}n\times 2^{-4}=2^{-33}n$。

步骤 9 猜测RK_7^3这 4 bit 的子密钥，对剩余的$2^{-33}n$个对应明文对，进行部分第 3 轮加密运算，判断其左半部分输出是否全部为 0，排除那些不为 0 的差分值输入。若有明文对剩余，则根据不可能差分的性质，所猜测的子密钥一定是错误密钥，必须排除。

下面分析算法 1 给出的攻击算法的计算量。

定理 1 基于图 3 给出的 21 轮 LBlock 算法的不可能差分区分器，在选择2^{42}个明文结构，即选择明文量为2^{62}的条件下，算法 1 给出的针对 21 轮 LBlock 算法的不可能差分分析算法总的计算量约为2^{62}次 21 轮加密，并且可以唯一地恢复出正确密钥。

证明 首先，对2^{62}个选择明文进行加密所需的计算量为2^{62}次 21 轮加密变换。

经过步骤 2 进行筛选后，剩余数据对为2^{49}，在步骤 3 猜测密钥部分解密判断时，若直接猜测全部 12 bit密钥，所需的计算量为$2\times 2^{49}\times 2^{12}/8=2^{59}$次一轮加密变换。这里采用“Early Abort”[10]技术，分步猜测密钥进行判断。首先猜测RK_0^{21}，部分解密第 20 轮变换，判断$S_0(L_0^{21}\oplus RK_0^{21})\oplus S_0(L_0'^{21}\oplus RK_0^{21})$是否与$t_7$相等。利用此条件筛除不符合要求的数据，对保留下来的数据再猜测RK_6^{21}，判断$S_6(L_6^{21}\oplus RK_6^{21})\oplus S_6(L_6'^{21}\oplus RK_6^{21})$是否与$t_5$相等，筛除不符合要求的数据，最后猜测$RK_7^{21}$，判断$S_7(L_7^{21}\oplus RK_7^{21})\oplus S_7(L_7'^{21}\oplus RK_7^{21})$是否与$t_5$相等，进一步筛除不符合要求的数据。从而，步骤 3 总的计算量为$2\times(2^{49}\times 2^4+2^{45}\times 2^8+2^{41}\times 2^{12})/8=3\times 2^{51}\approx 2^{53}$。

同理，步骤 4 大约需要2^{52}次一轮加密变换；步骤 5 大约需要2^{51}次一轮加密变换；步骤 6 大约需要2^{51}次一轮加密变换；步骤 7 大约需要2^{52}次一轮加密变换；步骤 8 大约需要2^{51}次一轮加密变换；选择2^{42}个明文结构，即$n=2^{42}$，根据步骤 9 有$2^{44}\times(1-2^{-4})^{2^{-33}n}<1$，此时恢复出的密钥必为正确密钥，步骤 9 大约需要2^{51}次一轮加密变换。

综上所述，攻击算法 1 所需要的总的计算量约为$(2^{53}+2^{52}+2^{51}+2^{51}+2^{52}+2^{51}+2^{51})/21+2^{62}\approx 2^{62}$次 21 轮加密，并且可以唯一地恢复出正确密钥。

3.2 22 轮 LBlock 的不可能差分分析

在 21 轮 LBlock 算法不可能差分分析的基础上，再向前扩展一轮，即可实现对 22 轮 LBlock 算法不可能差分分析。

攻击所选择的明文结构为$(CCCC,***C,***C,*C*C)$，需要猜测 56 bit 的轮子密钥。为了唯一地确定正确密钥，所选择的明文结构个数为$2^{30.5}$，从

而攻击需要 $2^{62.5}$ 个选择明文，计算量约为 $2^{63.5}$ 次 22 轮加密。

表 1 给出了不可能差分分析的比较结果。

表 1 LBlock 的不可能差分分析结果比较

攻击轮数	选择明文	计算量	出处
20	2^{63}	$2^{72.7}$	文献[5,6]
21	$2^{62.5}$	$2^{73.7}$	文献[7]
21	2^{62}	2^{62}	本文
22	$2^{62.5}$	$2^{63.5}$	本文

4　结束语

通过分析研究 LBlock 算法的结构，本文给出了 21 轮和 22 轮的 LBlock 算法的不可能差分分析方法。攻击 21 轮 LBlock 算法所需的数据量约为 2^{62}，计算量约为 2^{62} 次 21 轮加密；攻击 22 轮 LBlock 算法所需的数据量约为 $2^{62.5}$，计算量约为 $2^{63.5}$ 次 22 轮加密。与已有的结果相比较，这是不可能差分分析攻击 LBlock 的最好结果。

参 考 文 献

[1] Hong D, Sung J, Lim J, *et al*.. HIGHT: a new block cipher suitable for low-resource device[J]. *LNCS*, 2006, 4249: 46–59.

[2] Bogdanov A, Kundsen L R, Leander G, *et al*.. PRESENT: an ultra-lightweight block cipher[J]. *LNCS*, 2007, 4727: 450–466.

[3] Izadi M, Sadeghiyan B, Sadeghian S, *et al*.. MIBS: a new lightweight block cipher[J]. *LNCS*, 2009, 5888: 334–348.

[4] De Canniere C, Dunkelman O, Knezevic M. KATAN and KTANTAN-a family of small and efficient hardware-oriented block cipher[J]. *LNCS*, 2009, 5747: 272–288.

[5] Wu Wen-ling and Zhang Lei. LBlock: a lightweight block cipher[J]. *LNCS*, 2011, 6715: 327–344.

[6] Wu Wen-ling and Zhang Lei. LBlock: a lightweight block cipher[EB/OL]. Cryptology ePrint Archive, Report 2011, 345, http:eprint.iacr.org/. 2011.

[7] Liu Ya, Gu Da-wu, Liu Zhi-qiang, *et al*.. Impossible differential attacks on reduced-round LBlock[J]. *LNCS*, 2012, 7232: 97–108.

[8] Karakoç F, Demirci H, and Emre Harmanc A. Impossible differential cryptanalysis of reduced-round LBlock[J]. *LNCS*, 2012, 7322: 179–188.

[9] Zhang Peng, Li Tui lin, Sun Bing, *et al*.. New impossible differential cryptanalysis of ARIA[EB/OL]. Cryptology ePrint Archive, Report 2008, 227, http:eprint.iacr.org/. 2008.

[10] Lu J, Kim J, *et al*.. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1[J]. *LNCS*, 2008, 4964: 370–386.

郭建胜：　男，1972 年生，教授，研究方向为密码学与信息安全.

罗　伟：　男，1987 年生，硕士生，研究方向为分组密码设计与分析.

张　磊：　男，1985 年生，硕士，研究方向为分组密码设计与分析.