# 轻量级分组密码 Lblock 算法的 Nibble 积分攻击

王 衡,张文英,韩国勇

(山东师范大学 信息科学与工程学院,济南 250014)
E-mail: 1198956437@qq.com

**摘 要:** Lblock 算法是 2011 年提出的一种轻量级分组密码密码算法,在有限的环境下得到广泛使用. 积分攻击是一种有效的密码分析方法,对于 Lblock 算法的基于比特的积分攻击,可以先构建 8 轮区分器,再向前做 4 轮高阶积分扩散,然后在积分区分器后加上 5 轮做 17 轮积分攻击,但是攻击轮数较少,且攻击复杂度较高,本文是在基于字节的积分攻击也是首先构建 8 轮区分器,再向前做 6 轮高阶积分扩散,构造 14 轮区分器,在积分区分器后面加 7 轮,猜测部分密钥,对其进行解密,做 21 轮积分攻击,时间复杂度降低. 然后结合不同的对 Lblock 算法的攻击方法,对其进行比较,积分攻击在尽可能多的轮数下,时间复杂度降低.

**关 键 词:** Lblock; 积分攻击; 积分区分器; 基于字节的攻击; 轻量级分组密码
**中图分类号:** TP309 **文献标识码:** A **文 章 编 号:** 1000-1220(2017)08-1704-04

## Nibble Based Integral Attack on Lightweight Block Cipher Lblock

WANG Heng, ZHANG Wen-ying, HAN Guo-yong
(College of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

**Abstract:** Lblock is a light weight block cipher algorithm proposed in 2011, it is widely used in a limited environment. Integral attack is an effective method for cryptographic analysis. In terms of idea of bit-pattern based integral attack, a 8-round distinguisher of Lblock is proposed, and we can add four rounds before the first round of the distinguisher, and add five rounds after the last round of the distinguisher, it become 17 rounds, but the number of attacks is less, and the attack complexity is high. In terms of idea of nibble based integral attack, a 8-round distinguisher of Lblock is proposed, and then do 6 rounds of high order diffusion, add 7 rounds, guessing part of the round key and decrypt it, become 21 rounds integral attack, thetime complexity is reduced, then compares the different attack methods of Lblock. Integral attack as many rounds, the time complexity is reduced.

**Key words:** lblock; integral attack; integraldistinguisher; nibble based integral attack; block cipher

## 1 引 言

近年来,轻量级分组密码在限制性环境中得到广泛的应用,并受到了青睐,它们常常运用于 RFID(射频识别技术)与传感器网络. Lblock 算法[1,11] 是 2011 年新提出的一种轻量级分组密码算法,是 Feistel 结构的代表性算法,密钥为 80bit,明文块长度为 64bit,分为左右两支,每支 32bit. 对 Lblock 算法的攻击方法有很多种,例如潘志舒,郭建胜对 Lblock 基于比特的积分攻击[4]; 詹英杰等对 Lblock 的相关密钥差分攻击[5],温隆和王美琴的 Lblock 相关密钥不可能差分攻击[12] 以及郭建胜,罗伟对 Lblock 的不可能差分攻击等[3],计算复杂程度比较高. 本文基于 nibble 字节的 Lblock 的积分攻击,先构建 8 轮积分区分器,然后猜测相关密钥,直到猜测的密钥唯一确定,计算复杂度有所降低.

积分攻击[3] 是一种选择明文攻击方法,它是继差分密码分析和线性密码分析后,密码学界公认的最有效的密码分析方法之一. 积分攻击的最主要环节是分析密文的平衡性进而寻找区分器,它的基本思想是: 通过分析一些中间状态的"和"经过几轮密码变换后的演变来恢复密钥比特. 该方法已经成功对许多分组密码算法进行了攻击,结果表明积分攻击比差分密码分析以及线性密码分析更有效,使用积分攻击可以攻击尽可能多的轮数,或者是攻击相同的轮数,攻击复杂度大大降低. 当前积分攻击是 AES 最好的攻击方法之一.

## 2 Lblock 算法描述

Lblock 算法[10] 是 2011 年吴文玲等人提出的一种新的轻量级分组密码,该算法明文分组是 64bit,采用了 Feistel 结构,分为左右两支,每支 32bit,密钥是 80bit,Lblock 算法的一轮加密如图 1 所示.

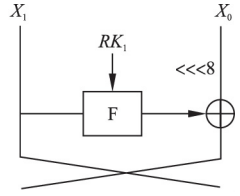


图 1 Lblock 一轮算法加密示意图
Fig. 1 An encryption algorithm of lblock

F 函数包含两部分,明文分组与密钥异或的结果进入 8 个 S 盒,以及 S 盒的输出进入一个 P 置换详见图 2 所示. <<<8 代表的是右支

收稿日期: 2016-06-02 收修改稿日期: 2016-09-27 基金项目: 国家自然科学基金项目(61272434,61672330,61602287)资助. 作者简介: 王 衡,男,1991 年生,硕士研究生,CCF 会员,研究方向为密码分析; 张文英(通信作者),女,1970 年生,博士后,教授,博士生导师,研究方向为密码学、布尔函数; 韩国勇,男,1978 年生,博士研究生,研究方向为网络信息安全管理技术.

先向左循环左移 8 个 bit 位,对应的置换关系为:

$P=\{0,1\}^{32}\rightarrow\{0,1\}^{32}$

$X=X_7\|X_6\|X_5\|X_4\|X_3\|X_2\|X_1\|X_0\rightarrow$

$X_6\|X_4\|X_7\|X_5\|X_2\|X_0\|X_3\|X_1$

Lblock 算法会用到 10 个 S 盒,每个都不一样,这 10 个不同的 S 盒都是 4 进 4 出的,这里的 n=4. 其中 $S_8$,$S_9$ 用在密钥编排中. 各个 S 盒详见表 1.

表 1　Lblock 算法的 S 盒

Table 1　S box of Lblock

| | |
|---|---|
| $S_0$ | 14 9 15 0 13 4 10 11 1 2 8 3 7 6 12 5 |
| $S_1$ | 4 11 14 9 15 13 0 10 7 12 5 6 2 8 1 3 |
| $S_2$ | 1 14 7 12 15 13 0 6 11 5 9 3 2 4 8 10 |
| $S_3$ | 7 6 8 11 0 15 3 14 9 10 12 13 5 2 4 1 |
| $S_4$ | 14 5 15 0 7 2 12 13 1 8 4 9 11 10 6 3 |
| $S_5$ | 2 3 11 12 15 14 0 9 7 10 6 3 1 8 4 5 |
| $S_6$ | 11 9 4 14 0 15 10 13 6 12 5 7 3 8 1 2 |
| $S_7$ | 13 10 15 0 14 4 9 11 2 1 8 3 7 5 12 6 |
| $S_8$ | 8 7 14 5 15 13 0 6 11 12 9 10 2 4 1 3 |
| $S_9$ | 11 5 15 0 7 2 9 13 4 8 1 12 14 10 3 6 |

Lbolck 的密钥编排如下所示:

1) K<<<29;

2) $[K_{79}\ K_{79}\ K_{77}\ K_{76}]=S_9(K_{79}\ K_{78}\ K_{77}\ K_{76})$

$[K_{75}\ K_{74}\ K_{73}\ K_{72}]=S_8(K_{75}\ K_{74}\ K_{73}\ K_{72})$

$(K_{50}\ K_{49}\ K_{48}K_{47}\ K_{46})\oplus\{i\}_2$

3) 取寄存器最左端 32bit 做轮密钥,第一轮密钥

$K_{79}\ K_{78},\cdots,K_{47}$

对于 Lblock 算法的密钥编排来说,轮密钥是经过循环移位,S 盒,异或常数得到的. 每轮只取 80bit 的左 32bit 作为轮密钥,对于 Lblock 算法,要猜测轮密钥 $K_j^i$,只需要猜测原始密钥 K [a,a-1,a-2,a-3],其中 a=(51i+47+4j) mod80,i 代表密钥轮数,j 代表第 j 个 4bit.

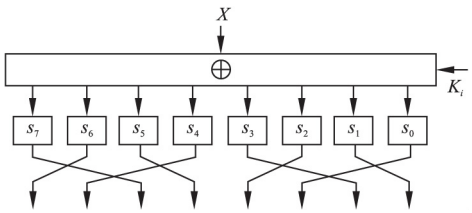


图 2　Lblock 算法的 F 函数

Fig. 2　Function F of lblock

在本文中 $L_j^i$,$R_j^i$,$K_j^i$,i 代表轮数,j 代表第 j 个 4bit,L 代表左支,R 代表右支,K 代表密钥.

## 3　积分攻击

积分攻击[3,11] 是有 Knudsen 等提出的一种分组密码选择明文攻击方法. 它的最主要环节是分析密文的平衡性进而寻找区分器,它的基本思想是: 通过分析一些中间状态的"和"经过几轮密码变换后的演变来恢复密钥比特. 该方法已经成功对许多分组密码算法进行了攻击.

在构建积分区分器时,需要用到下列一些特殊集合:

1) 活跃集. 对于任意的 $0\leqslant i\leqslant j\leqslant 2^n-1$,都有 $x_i\neq x_j$,则集合 $\{x_i\in F_{2^n},0\leqslant i\leqslant 2^n-1\}$ 是活跃集,记为 A. 例如 n=4 时,A={0000,0001,…,0000},取遍所有值.

2) 稳定集. 对于任意 $0<i\leqslant 2^n-1$,都有 $x_i=x_0$,则集合 $\{x_i\in F_{2^n},0\leqslant i\leqslant 2^n-1\}$ 是稳定集,记为 C. 例如 n=4 时,C={0000,0000,…,0000},所有情况都是 0000.

3) 平衡集. 若 $\oplus_{i=0}^{2^n-1}x_i=0$,则集合 $\{x_i\in F_{2^n},0\leqslant i\leqslant 2^n-1\}$ 是平衡集,记为 B.

这些集合满足下列性质:

1) A 集合通过 S 盒,密钥加等以后还是 A 集合,C 集合通过上述操作还是 C 集合.

2) 两个 A 集合相加以后是 B 集合,A 集合与 C 集合相加还是 A 集合,两个 B 集合相加还是 B 集合.

3) B 集合通过 S 盒时,将无法判断其平衡性.

基于 nibble 字节的 Lblock 算法,右支要先向左循环左移 8bit 位,正好是两个 nibble 字节,利用这个弱点,我们可以构造 8 轮的积分区分器.

## 4　Lblock 基于 Nibble 的积分区分器构造

根据积分攻击中集合的定义,以及他们之间的性质,选择特定形式的明文,构建 Lblock8 轮积分区分器. 选择 $2^4$ 个明文,满足的条件是 $R_8^0$ 取遍所有的 $2^4$ 个值,即为集合 A,其他半字节都取常数,即为集合 C,经过 8 轮 Lblock 加密算法后,得出部分位置为平衡集,即为集合 B,分别是 $L_6^8$,$L_4^8$,$L_2^8$,$L_0^8$,$R_7^8$,$R_3^8$,$R_2^8$,如图 3 所示.

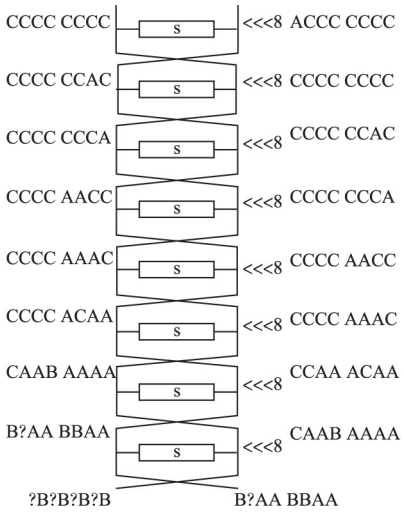


图 3　Lblock 算法基于 nibble 的 8 轮积分区分器

Fig. 3　8-round distinguisher of Lblock based on nibble

第 1 轮. $L_0$ 全是稳定集合 C,$R_{0,8}$ 是集合 A,其他 $R_0$ 为集合 C,$L_0$ 进入 S 盒后,在经过 P 置换,与右支循环左移 8bit 位以后的进行异或作为下一轮的左支,上一轮的左支作为下一轮的右支,所以第一轮的输出为 $L_1\|R_1$(CCCCCCAC,CCCCCCCC).

第 2 轮. $L_1$ 进入 F 函数后,经过 S 盒变换,仍为 CCCCCCAC,在经过 P 置换,与 $R_1$ 循环左移 8bit 后的进行异或,作为下一轮的左支,$L_1$ 作为下一轮的右支,所以第二轮的输出为 $L_2\|R_2$(CCCCCCCA,CCCCCCAC).

第 3 轮. $L_2$ 进入 F 函数后,经过 S 盒变换后仍为 CCCCCCCA,经过 P 置换后再与右支循环左移 8bit 后进行异或作为下一轮的右支,上一轮的左支作为下一轮的右支. 第三轮的输出为 $L_3 \parallel R_3$( CCCCAACC,CCCCCCCA) .

第 4 轮. $L_3$ 入 F 函数后,经过 S 盒变换后,仍为 CCCCAACC,经过 P 置换后,与右支向左循环 8bit 后的进行异或,作为下一轮的左支,左支作为下一轮的右支. 第四轮的输出 $L_4 \parallel R_4$( CCCCAAAC,CCCCAACC) .

第 5 轮. $L_4$ 进入 F 函数之后,经过 S 盒不变仍为 CCCCAAAC,经过 P 置换后再与右支循环左移 8bit 后进行异或作为下一轮的右支,上一轮的左支作为下一轮的右支. 第五轮的输出 $L_5 \parallel R_5$( CCAAACAA,CCCCAAAC) .

第 6 轮. $L_5$ 进入 F 函数后,经过 S 盒变换之后,仍为 CCAAACAA,经过 P 置换后,与右支向左循环 8bit 后的进行异或,作为下一轮的左支,左支作为下一轮的右支. 第 6 轮的输出 $L_6 \parallel R_6$( CAABAAAA,CCAAACAA) .

第 7 轮. $L_6$ 进入 F 函数后,经过 S 盒变换之后,由集合进入 S 后的性质可得,出 S 盒后为 CAA? AAAA,经过 P 置换后再与右支循环左移 8bit 后进行异或作为下一轮的右支,上一轮的左支作为下一轮的右支. 第 7 轮的输出 $L_7 \parallel R_7$( B? AABBAA,CAABAAAA) .

第 8 轮. $L_7$ 进入 F 函数后,经过 S 盒变换之后,由集合进入 S 后的性质可得,出 S 盒后为( ?? AA?? AA) ,经过 P 置换后再与右支循环左移 8bit 后进行异或作为下一轮的右支,上一轮的左支作为下一轮的右支. 第 8 轮的输出 $L_8 \parallel R_8$( ? B? B? B? B,B? AABBAA) .

对构造的 8 轮积分区分器向前做 6 轮高阶积分扩展,如图 4 所示.

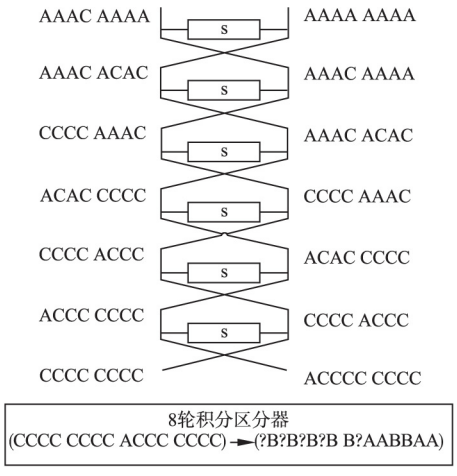


图 4 8 轮积分区分器的 6 轮高阶扩展

Fig. 4 6-round of high order diffusion of 8-round distinguisher

在 nibble 的基础上,构造了 Lblock 算法的 14 轮积分区分器,此时明文在 $L_4$ 取稳定集,其他都取活跃集,选择明文量为 $2^{60}$,14 轮过后, $L_6^{14}$,$L_4^{14}$,$L_2^{14}$,$L_0^{14}$,$R_7^{14}$,$R_3^{14}$,$R_2^{14}$ 为平衡集.

## 5 对 21 轮 Lblock 算法基于字节的积分攻击

对已有的 14 轮积分区分器,向后攻击 7 轮,攻击 21 轮 Lblock 算法. 选取特定的构造的 14 轮积分区分器的需要的明文,得到 21 轮加密的密文,猜测相关的密钥,从 21 轮的加密结果恢复到 14 轮的结果,验证 $X_7^{14}$ 是否是平衡集,假设第 i 轮的密钥为 $K_7^i$,$K_6^i$,$K_5^i$,…,$K_0^i$.

### 5.1 攻击步骤

**Step 1.** 选择满足 14 轮积分区分器输入形式的明文 $2^{60}$ 个,进行 21 轮加密,得到 $2^{60}$ 个密文.

**Step 2.** 猜测 21 轮密钥 $K_7^{21}$,$K_6^{21}$,$K_5^{21}$,$K_4^{21}$,$K_3^{21}$,$K_2^{21}$,$K_1^{21}$,$K_0^{21}$ 解密第 21 轮.

**Step 3.** 猜测 20 轮密钥 $K_7^{20}$,$K_6^{20}$,$K_5^{20}$,$K_4^{20}$,$K_3^{20}$,$K_2^{20}$,$K_1^{20}$,解密 20 轮计算

$$X_7^{19} = S_3(X_3^{20} \oplus K_3^{20}) \oplus X_1^{21}$$
$$X_6^{19} = S_1(X_1^{20} \oplus K_1^{20}) \oplus X_0^{21}$$
$$X_5^{19} = S_6(X_6^{20} \oplus K_6^{20}) \oplus X_7^{21}$$
$$X_4^{19} = S_4(X_4^{20} \oplus K_4^{20}) \oplus X_6^{21}$$
$$X_3^{19} = S_7(X_7^{20} \oplus K_7^{20}) \oplus X_5^{21}$$
$$X_2^{19} = S_5(X_5^{20} \oplus K_5^{20}) \oplus X_4^{21}$$
$$X_1^{19} = S_2(X_2^{20} \oplus K_2^{20}) \oplus X_3^{21}$$

**Step 4.** 猜测 19 轮密钥 $K_7^{19}$,$K_6^{19}$,$K_3^{19}$,$K_2^{19}$,$K_1^{19}$,解密第 19 轮,计算

$$X_7^{18} = S_3(X_3^{19} \oplus K_3^{19}) \oplus X_1^{20}$$
$$X_6^{18} = S_1(X_1^{19} \oplus K_1^{19}) \oplus X_0^{20}$$
$$X_5^{18} = S_6(X_6^{19} \oplus K_6^{19}) \oplus X_7^{20}$$
$$X_3^{18} = S_7(X_7^{19} \oplus K_7^{19}) \oplus X_5^{20}$$
$$X_1^{18} = S_2(X_2^{19} \oplus K_2^{19}) \oplus X_3^{20}$$

**Step 5.** 猜测 18 轮密钥 $K_7^{19}$,$K_6^{19}$,$K_5^{19}$ 解密第 18 轮,计算

$$X_5^{17} = S_6(X_6^{18} \oplus K_6^{18}) \oplus X_7^{19}$$
$$X_3^{17} = S_7(X_7^{18} \oplus K_7^{18}) \oplus X_5^{19}$$
$$X_2^{17} = S_5(X_5^{18} \oplus K_5^{18}) \oplus X_4^{19}$$

**Step 6.** 猜测 17 轮密钥 $K_3^{17}$,$K_2^{17}$ 解密 17 轮,计算

$$X_7^{16} = S_3(X_3^{17} \oplus K_3^{17}) \oplus X_1^{18}$$
$$X_1^{16} = S_2(X_2^{17} \oplus K_2^{17}) \oplus X_3^{18}$$

**Step 7.** 猜测 16 轮密钥 $K_7^{16}$ 解密 16 轮,计算

$$X_3^{15} = S_7(X_7^{16} \oplus K_7^{16}) \oplus X_5^{17}$$

**Step 8.** 猜测 15 轮密钥 $K_3^{15}$ 计算

$$X_7^{14} = S_3(X_3^{15} \oplus K_3^{15}) \oplus X_1^{16}$$

另选一组明文直到确定为止步骤详见下页图 5( 阴影部分是要猜测的密钥) .

统计猜测的密钥:

$K_7^{21}$,$K_6^{21}$,$K_5^{21}$,$K_4^{21}$,$K_3^{21}$,$K_2^{21}$,$K_1^{21}$,$K_0^{21}$,$K_7^{20}$,$K_6^{20}$,$K_5^{20}$,$K_4^{20}$,$K_3^{20}$,$K_2^{20}$,$K_1^{20}$,$K_7^{19}$,$K_6^{19}$,$K_3^{19}$,$K_2^{19}$,$K_1^{19}$,$K_7^{18}$,$K_6^{18}$,$K_5^{18}$,$K_3^{17}$,$K_2^{17}$,$K_7^{16}$,$K_3^{15}$,

经过综合,只需要猜测 72bit 的初始密钥( 31,60,73,74,75,76,77,78bit 位没猜) .

### 5.2 攻击复杂度

对于正确的密钥一定能保证 $R_7^{14}$ 为平衡集,而错误的密钥使 $R_7^{14}$ 也是平衡集的概率是 $2^{-4}$,而不使 $R_7^{12}$ 为平衡集的密钥则一定是错误的,经过一组明文淘汰后,所剩的错误密钥数量为: $(2^{72}-1) * 2^{-4} = 2^{68}$,要确定唯一的密钥,则要用 18 组 $(17+1)$ 数据,可以确定唯一的密钥,所以攻击的数据复杂度

为: $2^{60}*\ 18=2^{64.2}$ 个明文,因为 64.2 已经超过了明文的 bit 大小 64,所以数据复杂度为 $2^{64}$.

而攻击的时间复杂度可以如下所示: Step1 需要猜测 $2^{60}$ 次 21 轮加密, Step2 需要猜测 32bit 密钥,有 $2^{32}$ 种可能,而密文有 $2^{32}$ 种可能,则一共需要 $2^{32}*\ 2^{32}$ 次 S 盒查表,Step3 需要猜测 28bit 密钥,有 $2^{28}$ 种可能,密文则有 $2^{28}$ 种可能值,一共需要 $2^{28}*\ 2^{28}$ 次 S 盒查表,Step4 则需要猜测 12bit 密钥,则有 $2^{12}$ 种可能,密文则有 $2^{20}$ 种可能值,一共需要 $2^{12}*\ 2^{20}$ 次 S 盒查表,STEP5 则需要猜测 1bit 密钥,有 2 种可能,密文有 $2^{12}$ 种可能值,一共需要 $2^{1}*\ 2^{12}$ 次 S 盒查表,Step6,Step7,Step8 由于密钥都已经猜过,只看密文就可以,则分别需要 $2^{8}$, $2^{4}$, $2^{4}$ 次查表操作. 21 轮算法则需要 $21*\ 8=168$ 次 S 盒查表操作,则一共可以相当于 $2^{60}+(2^{32}*\ 2^{32}+2^{28}*\ +2^{12}*\ 2^{20}+2^{1}*\ 2^{12}+2^{8}+2^{4}+2^{4})/(21*\ 8)\approx 2^{60}$ 次 21 轮加密. 则每一组明文时的时间复杂度都是 $2^{60}$,所以此攻击方法的时间复杂度为 $18*\ 2^{60}=2^{64.2}$.

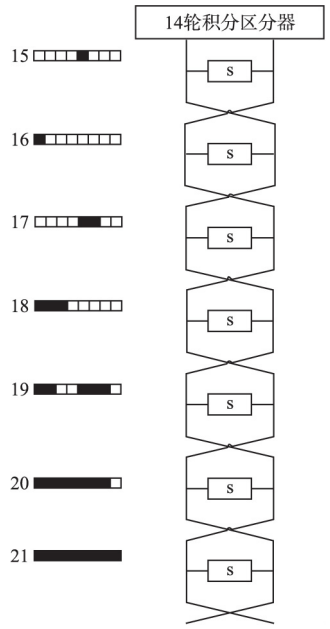


图 5　后 7 轮涉及到需要猜测的密钥

Fig. 5　Key need to guess in later 7rounds

## 6　总　结

本文对 Lblock 算法进行积分攻击的研究,构造了 8 轮积分区分器,并向前做高阶积分扩展将 8 轮积分区分器至 14 轮,利用 Lblock 算法密钥扩展算法中主密钥与轮密钥之间的关系,对 21 轮 Lblock 算法进行积分攻击. 相比于其他 Lblock 算法的攻击方法,比较结果见表 2 所示. 由表可得,基于 nibble 的 Lblock 算法积分攻击在尽可能多的轮数下,时间复杂度降低.

表 2　对 Lblock 算法不同攻击方法的结果比较

Table 2　Comparison of the results of different attacks on Lblock

| 攻击方法 | 轮数 | 数据量 | 计算复杂度 | 文献 |
|---|---|---|---|---|
| 基于字节的积分攻击 | 21 | $2^{64}$ | $2^{64.2}$ | 本文 |
| 基于 bit 的积分攻击 | 17 | $2^{63.7}$ | $2^{63.7}$ | 文献 [5] |
| 相关密钥不可能差分 | 19 | $2^{64}$ | $2^{70}$ | 文献 [6] |
| 不可能差分 | 19 | $2^{63}$ | $2^{72.7}$ | 文献 [2] |

**References:**

[1] Izadi M, Sadeghiyan B, Sadeghian S, et al. MIBS: a new lightweight block cipher [C]. Cryptology & Network Security, International Conference LNCS, 2009, 5888: 334-348.

[2] Wu Wen-ling, Zhang Lei. LBlock: a lightweight block cipher [C]. Applied Cryptography & Network Security-international Conference LNCS, 2011, 6715: 327-344.

[3] Li Chao, Su Bing, Li Rui-lin. Attack method and example analysis of block cipher [M]. Beijing: Beijing Science Press, 2010.

[4] Pan Zhi-shu, Guo Jian-sheng. Bit-pattern based integral attack on LBlock [J]. Journal of Information Engineering University, 2013, 14(1): 30-35.

[5] 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.

[6] Wu Wen-ling, Feng Deng-guo, Zhang Wen-tao. Design and analysis of block cipher [M]. Beijing: Tsinghua University Press, 2009.

[7] Zaba M, Raddum H, Henricksen M, et al. Bit-pattern based integral attack [C]. Fast Software Encryption, LNCS 2008, 5086: 363-381.

[8] Wang Gao-li, Wang Shao-hui. Integral cryptanalysis of reduced-round MIBS block cipher [J]. Journal of Chinese Computer Systems, 2012, 33(4): 773-777.

[9] Yu Xiao-li, Wu Wen-ling, Li Yan-jun. Integral attack of educed-round MIBS block cipher [J]. Journal of Computer Research and Development, 2013, 50(10): 2117-2125.

[10] Li Lin, Wu Wen-ling, Zheng Ya-feng. Automatic search for key-bridging technique: applications to LBlock and TWINE [C]. Fast Software Encryption, 2016, 9783: 247-267.

[11] Zhang Hui-ling, Wu Wen-ling, Wang Yan-feng. Integral attack against bit-oriented block ciphers [J]. Information Security and Cryptology, 2015, 9558: 102-118.

[12] Related-key impossible differential attack on reduced-round lblock [J]. Journalof Computer Scienceand Technology, 2014, 29(1): 165-176.

**附中文参考文献:**

[3] 李　超,孙　兵,李瑞林. 分组密码的攻击方法与实例分析 [M]. 北京: 北京科学出版社, 2010.

[4] 潘志舒,郭建胜. LBlock 算法的基于比特积分攻击 [J]. 信息工程大学学报, 2013, 14(1): 30-35.

[5] 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.

[6] 吴文玲,冯登国,张文涛. 分组密码的设计与分析 [M]. 北京: 清华大学出版社, 2009.

[8] 王高丽,王少辉. 对 MIBS 算法的 Intergal 攻击 [J]. 小型微型计算机系统, 2012, 33(4): 773-777.

[9] 于晓丽,吴文玲,李艳俊. 低轮 MIBS 分组密码的积分分析 [J]. 计算机研究与发展, 2013, 50(10): 2117-2125.