Copyright ⓒ 2019 KSII

Related-key Impossible Boomerang Cryptanalysis on LBlock-s

**Min Xie**\***, Qiya Zeng**

State Key Laboratory of Integrated Service Networks, Xidian University Xi’an 710071, China

[e-mail: [mxie@xidian.edu.cn,](mailto:mxie@xidian.edu.cn) [m15686247918@163.com](mailto:m15686247918@163.com)]

\*Corresponding author: Min Xie

*Received March 26, 2018; revised April 2, 2019; accepted May 3, 2019;*

*published November 30, 2019*

***Abstract***

LBlock-s is the core block cipher of authentication encryption algorithm LAC, which uses the same structure of LBlock and an improved key schedule algorithm with better diffusion property. Using the differential properties of the key schedule algorithm and the cryptanalytic technique which combines impossible boomerang attacks with related-key attacks, a 15-round related-key impossible boomerang distinguisher is constructed for the first time. Based on the distinguisher, an attack on 22-round LBlock-s is proposed by adding 4 rounds on the top and 3 rounds at the bottom. The time complexity is about only 268.76 22-round encryptions and the data complexity is about 258 chosen plaintexts. Compared with published cryptanalysis results on LBlock-s, there has been a sharp decrease in time complexity and an ideal data complexity.

***Keywords:*** LBlock-s, lightweight block cipher, related-key, impossible differential, boomerang cryptanalysis

This research was supported in part by the National Key Research and Development Program of China (Grant No. 2016YFB0800601) and Key Program of NSFC-Tongyong Union Foundation (Grant No. U1636209).

[**http://doi.org/10.3837/tiis.2019.11.024**](http://doi.org/10.3837/tiis.2019.11.024) **ISSN : 1976-7277**

# Introduction

**W**ith the rapid development of electronic information technology and the widespread application of technologies such as RFID (Radio Frequency Identification), traditional block ciphers are not suitable for resource constrained environments. Therefore, lightweight block ciphers which are designed with a trade-off between the security and hardware performance for resource constrained environments have become a hot topic.

As the kernel block cipher of LAC submitted to CAESAR competition [1], LBlock-s is an improved version of LBlock [2] which is proposed by Wu et al. in ACNS 2011. Similar to LBlock, it uses a variant of Feistel structure and consists of 32 rounds. The block length and the key length are 64-bit and 80-bit, respectively. What LBlock-s differs from LBlock is that LBlock-s employs an improved key schedule algorithm with a faster diffusion speed and replaces 10 different S-boxes in LBlock with 10 identical S-boxes to reduce hardware and software costs. In terms of security, Shan et al. [3] showed that there were at least 32 active boxes in the 32-round related-key differential characteristic, that is, the probability must not be higher than 2−64, and they gave a 10-round and an 11-round related-key differential characteristics. Xiao [4] used differential cryptanalysis to give a 16-round differential path. Li et al. [5] mounted a 23-round attack on LBlock-s with improved multidimensional zero-correlation linear cryptanalysis. Using the 14-round impossible differential characteristic of LBlock which was given by the designers of LBlock, Jia [6] carried out a 21-round attack on LBlock-s. They gave the results on 22-round and 23-round attacks without the detailed analysis. And the results showed that the time complexity of 22-round attack was 278.86 22-round encryptions, which is close to the one in exhaustive search and much higher than the corresponding attack result in this paper.

Related-key cryptanalysis was independently introduced by Knudsen [7] and Biham [8] respectively. The basic idea of the technique is that the attackers find weaknesses of the key schedule algorithm to choose appropriate relation between keys and then predict the encryptions under these keys. Impossible differential cryptanalysis was proposed by Knudsen [9] and further by Biham against Skipjack [10], in which the attackers try to find a differential characteristic with a probability of 0 to eliminate the wrong keys and then to recover the correct key. Related-key cryptanalysis and impossible differential cryptanalysis are both very powerful techniques for analyzing the security of a wide variety of block ciphers, and there are many satisfactory attack results on a lot of block ciphers such as Hummingbird-2, TEA, LBlock , MIBS and so on [11-17]. Boomerang cryptanalysis was presented by Wagner in 1999 [18], which is a variant of differential cryptanalysis. The basic idea of boomerang cryptanalysis is to use short differential characteristics with relatively large probabilities to form long differential characteristics with high probability. Related-key impossible boomerang cryptanalysis [19] is obtained by using these three attacks in combination. Until now, many satisfying analysis results are obtained on AES and LBlock by

using this cryptanalytic technique [19-20].

In this paper, we study the security of LBlock-s from the aspect of related-key impossible boomerang cryptanalysis for the first time. Through analyzing the property of round function and key schedule function of LBlock-s, a 15-round related-key impossible boomerang distinguisher is carried out, and we get a 22-round related-key impossible boomerang characteristic to recover 68-bit key with time complexity of 268.76 and 258 chosen plaintexts. Up to now, this is the best attack result on 22-round LBlock-s.

**Outline.** In Section 2, a description of LBlock-s and some notations used in this paper are given. In Section 3, we study the related-key impossible boomerang cryptanalysis. In Section 4, a 15-round related-key impossible boomerang distinguisher and attack on 22-round LBlock-s are described, followed by conclusion in Section 5.

# Description of LBlock-s

## Notations

The following notations are used in this paper.

P, C: the 64-bit plaintext and the 64-bit ciphertext;

𝐾𝐾, ∆𝐾𝐾: the 80-bit master key and the difference of *K*;

𝐾𝐾𝑖𝑖, ∆𝐾𝐾𝑖𝑖: the *i*-th round subkey and the difference of 𝐾𝐾𝑖𝑖;

𝐾𝐾𝑗𝑗, ∆𝐾𝐾𝑗𝑗: the *j*-th nibble of 𝐾𝐾𝑖𝑖 and the *j*-th nibble of ∆𝐾𝐾𝑖𝑖;

𝑖𝑖 𝑖𝑖

𝑋𝑋𝑖𝑖 , ∆X𝑖𝑖: the left half of the *i*-th round input and the difference of 𝑋𝑋𝑖𝑖 ;

𝑋𝑋0: the right half of the first round input;

𝑋𝑋𝑗𝑗, ∆𝑋𝑋𝑗𝑗: the *j*-th nibble of 𝑋𝑋𝑖𝑖 and the *j*-th nibble of ∆X𝑖𝑖;

𝑖𝑖 𝑖𝑖

𝑋𝑋𝑖𝑖 ||𝑋𝑋𝑗𝑗: the concatenation of 𝑋𝑋𝑖𝑖 and 𝑋𝑋𝑗𝑗; *X*<<< *i*: a left rotation of *X* by *i* bits; *X*>>> *i*: a right rotation of *X* by *i* bits; [𝑖𝑖]2: the binary form of an integer *i*.

## Overview of LBlock-s

LBlock-s is an improved version of LBlock with a variant of Feistel structure. It consists of 32-round iterative, with the block length 64-bit and the master key length 80-bit. The encryption procedure is as follows, and the general structure is illustrated in **Fig. 1**.

1. Input P = 𝑋𝑋1||𝑋𝑋0;

2. For 𝑖𝑖 = 2,3, ⋯ 33, do the following calculation:

𝑋𝑋𝑖𝑖 = 𝐹𝐹(𝑋𝑋𝑖𝑖−1, 𝐾𝐾𝑖𝑖−1) ⊕ (𝑋𝑋𝑖𝑖−2 <<< 8); 3. Output C = 𝑋𝑋33||𝑋𝑋32;