Information Processing Letters 116 (2016) 259–266

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Linear cryptanalysis of reduced-round SPECK

Yu Liu, Kai Fu, Wei Wang, Ling Sun, Meiqin Wang *

Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

ARTICLE INFO

Article history:
Received 15 September 2015
Accepted 5 November 2015
Available online 2 December 2015
Communicated by S.M. Yiu

Keywords:
Lightweight block cipher
SPECK
Linear approximation
Linear cryptanalysis
Cryptography

ABSTRACT

SPECK is a family of lightweight block ciphers which was proposed by United States National Security Agency and designed for optimal performance in software. The paper gives the security of SPECK against linear cryptanalysis and introduces 9, 10, 12, 15 and 16 rounds linear approximations on SPECK for block sizes of 32, 48, 64, 96 and 128 bits, respectively. Partial linear mask table is used to speed up the search progress rather than the linear mask table. Using the structure of red-black tree to store the pLMT, we deduce the search time. Combining the Segment Searching with branch-and-bound method, the search time is further reduced. For 48-, 96- and 128-bit version the lengths of the linear approximations are 1, 9 and 10 rounds longer than the previous linear cryptanalytic. For SPECK64 the correlation of the linear approximation is twice as much as the previous linear cryptanalytic. As a result, we improve the previous linear cryptanalysis and gain more obvious advantage for block lengths of 96 and 128 bits. Especially, in aspect of SPECK96/144, SPECK128/192 and SPECK128/256 we can attack the same rounds as the best previous attacks.

1. Introduction

In June 2013 the United States National Security Agency published the SPECK family of lightweight block ciphers, which was optimized for software implementations [2]. Due to SPECK's wide application prospect, it's necessary to evaluate the security against various attacks and there are numerous cryptanalyses of SPECK, such as differential cryptanalysis [1,3,5], rectangle attack [1], differential fault analysis [13] and linear cryptanalysis [15]. Among them, the best attacks on round-reduced SPECK are differential attacks presented by Abed et al. [1] and Dinur [5], while for the linear cryptanalysis, recently the only results were proposed by Yao et al. [15]. They applied Wallén's numeration algorithm [14] to Matsui's branch-and-bound framework [9] in the searching algorithm for linear trails, however, there is still a gap compared with the differential cryptanalysis. Especially for 96- and 128-bit version. Therefore, we explore the security of SPECK against linear cryptanalysis, and match the same rounds with the differential attacks for 96- and 128-bit version. Summary of the attacks is presented in Table 2.

Linear cryptanalysis is a known-plaintext attack which was introduced by Matsui as a theoretical attack on the Data Encryption Standard (DES) [8] and later successfully led to a practical cryptanalysis of DES [7]. It exploits the correlation of linear approximations between input and output of a block cipher. Since SPECK is an ARX cipher, which consists of modular addition, bit rotation and XOR operations, the key step in searching the linear approximation is to calculate the correlation of linear approximation for modular addition. The linear approximations of addition modulo 2^n was investigated by Wallén [14], where an efficient algorithm to compute the probability of linear approximation of modular addition is presented. Nyberg and Wallén applied this algorithm to find the linear approximation of the FSM of the stream cipher SNOW 2.0 [10]. A more explicit formula for linear probabilities of addi-

* Corresponding author.
E-mail address: mqwang@sdu.edu.cn (M. Wang).

http://dx.doi.org/10.1016/j.ipl.2015.11.005
0020-0190/

tion modulo 2^n was given by Schulte-Geers [11]. Based on it, Dehnavi et al. exhibited [4] a better insight for these probabilities. We name their method State Conversion for convenience.

Our Contributions:

- **A new search method for linear approximations of the SPECK family.** In the search process for linear approximations we produce the Linear Mask Table (LMT) easily by State Conversion. However, the LMT is too large to search the linear approximations. Therefore we will use partial linear mask table (pLMT) rather than LMT, similarly to the partial differential distribution tables [3]. Moreover, since the pLMT is traversed many times, it will be stored using the structure of red-black tree. Then the time of traversing the pLMT will be $O(\log m)$, where m is the total number of elements in the tree. For the cipher with large block size, the search process is divided into several parts, and these parts will be joined together into the linear approximation. This method is called Segment Searching. Combining the methods above with [9] will show several approaches to produce linear approximations for SPECK family.
- **The best known linear approximations of the SPECK family.** We present the best known linear approximations for 9-round SPECK32 with correlation 2^{-14}, 10-round SPECK48 with correlation 2^{-22}, 12-round SPECK64 with correlation 2^{-30}, 15-round SPECK96 with correlation 2^{-45} and 16-round SPECK128 with correlation 2^{-61}. The different outcomes between [15] and this paper are illustrated in Table 1. Here is the only comparison of the maximum number of rounds and correlation of the linear approximations, because there are no specific linear approximations in [15].
- **Linear attack on the variants of SPECK96 and SPECK128.** Taking advantage of these linear approximations, the paper will present attacks on SPECK of 96 and 128 bits versions, which target up to the same rounds as the differential cryptanalysis. Moreover, it will improve the previous linear cryptanalysis significantly.

Table 1
Comparison of the linear approximations on SPECK.

Block size	Maximum number of rounds		Correlation	
	[15]	this paper	[15]	this paper
32	9	9	2^{-14}	2^{-14}
48	9	10	2^{-20}	2^{-22}
64	12	12	2^{-31}	2^{-30}
96	6	15	2^{-11}	2^{-45}
128	6	16	2^{-11}	2^{-61}

A complete summary of all the best previous attacks on SPECK is described in [1,5,15] as seen in Table 2. All of the best previous attacks are based on differential cryptanalysis and related techniques.

The paper is organized as follows: Section 2 will list the notations used throughout this paper and present a brief description of SPECK family. Sections 3 and 4 present the linear approximations and the linear attacks on SPECK, respectively. Finally, we conclude the paper in Section 5.

2. Preliminaries

This section gives notations and presents a brief description of SPECK.

2.1. Notations

The following notations are used in this paper. For $a = (a[n-1], \ldots, a[0]) \in \mathbb{F}_2^n$, $b = (b[n-1], \ldots, b[0]) \in \mathbb{F}_2^n$, $c = (c[n-1], \ldots, c[0]) \in \mathbb{F}_2^n$:

$a \oplus b$	bitwise XOR of a and b,
$w(a)$	hamming weight of the binary vector a,
$\lll i$	left circular shift by i bits,
$\ggg j$	right circular shift by j bits,
$a[i]$	the i-th bit of a, $i \in \{0, \ldots, n-1\}$,
$a[i]b[j]$	bitwise AND on $a[i]$ and $b[j]$, $i,\ j \in \{0, \ldots, n-1\}$,
$a \cdot b$	the inner product of a and b, $a \cdot b = \bigoplus_{i=0}^{n-1} a[i]b[i]$,
$a\&b$	bitwise AND of a and b, $a\&b = (a[n-1]b[n-1], \ldots, a[0]b[0])$,
$a \boxplus b \ (mod\ m)$	a add to b modulo m, $m \in \mathbb{Z}^+$,

Table 2
Summary of attacks on SPECK family.

SPECK2n/k	Rounds attacked/Total rounds	Method	Time (en)	Data	Memory (block)	Reference
96/144	16/29	RC	$2^{135.9}$	$2^{90.9}$CP	$2^{90.92}$	[1]
	17/29	DC	2^{133}	2^{85}CP	$2^{18.42}$	[5]
	9/29	LC	$2^{122.90}$	$2^{27.65}$KP	–	[15]
	17/29	**LC**	2^{96}	2^{92}**KP**	2^{92}	**This paper**
128/192	18/33	RC	$2^{182.7}$	$2^{125.9}$CP	$2^{117.9}$	[1]
	18/33	DC	2^{177}	2^{113}CP	2^{18}	[5]
	9/33	LC	$2^{156.74}$	$2^{28.30}$KP	–	[15]
	18/33	**LC**	2^{128}	2^{124}**KP**	2^{124}	**This paper**
128/256	18/34	RC	$2^{182.7}$	$2^{125.9}$CP	$2^{117.9}$	[1]
	19/34	DC	2^{241}	2^{113}CP	2^{18}	[5]
	7/34	LC	$2^{220.74}$	$2^{28.30}$KP	–	[15]
	19/34	**LC**	2^{192}	2^{124}**KP**	2^{124}	**This paper**

DC: Differential Cryptanalysis. LC: Linear Cryptanalysis. RC: Rectangle Cryptanalysis. CP: Chosen Plaintexts. KP: Known Plaintexts.