Information Processing Letters 114 (2014) 322–330

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard

Long Wen [a], Meiqin Wang [a,*], Andrey Bogdanov [b,*], Huaifeng Chen [a]

[a] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[b] Technical University of Denmark, Denmark

ARTICLE INFO

Article history:
Received 6 August 2013
Received in revised form 20 November 2013
Accepted 20 January 2014
Available online 21 January 2014
Communicated by V. Rijmen

Keywords:
Cryptography
Analysis of algorithms
Block cipher
Zero-correlation linear cryptanalysis
HIGHT

ABSTRACT

HIGHT is a block cipher designed in Korea with the involvement of Korea Information Security Agency. It was proposed at CHES 2006 for usage in lightweight applications such as sensor networks and RFID tags. Lately, it has been adopted as ISO standard. Though there is a great deal of cryptanalytic results on HIGHT, its security evaluation against the recent zero-correlation linear attacks is still lacking. At the same time, the Feistel-type structure of HIGHT suggests that it might be susceptible to this type of cryptanalysis. In this paper, we aim to bridge this gap.

We identify zero-correlation linear approximations over 16 rounds of HIGHT. Based upon those, we attack 27-round HIGHT (round 4 to round 30) with improved time complexity and practical memory requirements. This attack of ours is the best result on HIGHT to date in the classical single-key setting. We also provide the first attack on 26-round HIGHT (round 4 to round 29) with the full whitening key.

1. Introduction

1.1. Lightweight block ciphers, HIGHT, and existing cryptanalysis

With emerging pervasive applications in mind such as sensor networks, RFID tags and medical devices, a variety of lightweight cryptographic algorithms have been lately proposed including the two block ciphers adopted as ISO/IEC standard for lightweight encryption: PRESENT [7] proposed at CHES 2007 and CLEFIA [8] proposed at FSE 2007. Many more lightweight block ciphers have been published since then. Even the U.S. National Security Agency (NSA) has very recently contributed to the trend with two lightweight block ciphers: Simon and Speck [1]. HIGHT [6] is another lightweight block cipher designed with governmental involvement – Korea Information Security Agency (KISA).

HIGHT was proposed at CHES 2006 and then adopted as ISO standard block cipher [9]. HIGHT has 32 rounds. It accepts a 64-bit block and a 128-bit key. Each round consists of four parallel Feistel functions. Whitening keys are applied before the first and after the last round. The security of HIGHT has been extensively evaluated. Zhang et al. [10] present an integral attack on 22-round HIGHT at CANS 2009 and the time complexity is then reduced by Sasaki and Wang [11] at SAC 2012. In the impossible differential cryptanalysis of HIGHT, to be able to cryptanalyze more rounds, most of the existing attacks do not consider the pre-whitening key except the attack on 27-round HIGHT given in [14] at AfricaCrypt 2012. Lu [12] gives the first impossible differential cryptanalysis against 25-round HIGHT. Then at ACISP 2009, Özen et al. [13] successfully

* Corresponding authors.
E-mail addresses: mqwang@sdu.edu.cn (M. Wang), anbog@dtu.dk (A. Bogdanov).

http://dx.doi.org/10.1016/j.ipl.2014.01.007

Table 1
Summary of **single-key** attacks on HIGHT.

Attack	Rounds	Pre./Post.	Data	Time	Memory	Ref.
IA	22 (1∼22)	✓/✓	2^{62} CPs	$2^{118.71}$ ENs	2^{64} Bytes	[10]
IA	22 (1∼22)	✓/✓	2^{62} CPs	$2^{102.35}$ ENs	2^{64} Bytes	[11]
ID	25 (6∼30)	–/✓	2^{60} CPs	$2^{126.78}$ ENs	N/A	[12]
ID	26 (1∼26)	–/✓	2^{61} CPs	$2^{119.53}$ ENs	2^{109} Bytes	[13]
ID	26 (5∼30)	–/✓	$2^{61.6}$ CP	$2^{114.35}$ ENs	$2^{87.6}$ Bytes	[14]
ZC	**26** (4∼29)	✓/✓	$2^{62.79}$ **KPs**	$2^{119.1}$ **ENs**	2^{43} **Bytes**	**Section 4.1**
ID	27 (4∼30)	✓/✓	2^{58} CPs	$2^{126.6}$ ENs $+2^{120}$ MAs	2^{120} Bytes	[14]
ZC	**27** (4∼30)	✓/✓	$2^{62.79}$ **KPs**	$2^{120.78}$ **ENs**	2^{43} **Bytes**	**Section 4.2**

IA: Integral Attack; ID: Impossible Differential; ZC: Zero-Correlation Linear; Pre.: Pre-Whitening; Post.: Post-Whitening; CP: Chosen Plaintext; KP: Known Plaintext; MA: Memory Access; EN: Encryption.

mount an impossible differential attack on 26-round HIGHT. This result was then improved by Chen et al. [14] at AfricaCrypt 2012. Note that the attack on 27-round HIGHT with full whitening keys considered proposed in [14] has time complexity $2^{126.6}$ encryptions and 2^{120} memory accesses to a table of 2^{120} bytes, which can be considered marginal with respect to brute force. In the related-key setting, attacks on 28-round [12] and 31-round [13] HIGHT were presented using impossible differential attack and related-key rectangle attack on the full HIGHT was reported in [17]. Recently, independent biclique attacks – belonging to the class of polynomial advantage attacks – on the full HIGHT have been obtained in [15,16] with time complexities $2^{126.4}$ and $2^{125.9}$ encryptions, respectively.

1.2. Zero-correlation cryptanalysis

Zero-correlation linear cryptanalysis proposed by Bogdanov and Rijmen in [4] is a novel promising attack technique for block ciphers which has its theoretical foundation in the availability of numerous key-independent unbiased linear approximations with correlation zero for many ciphers. (If p is the probability for a linear approximation to hold, its correlation is defined as $c = 2p - 1$.) Though the initial distinguisher of [4] had some limitations in terms of data complexity, they were overcome in the FSE 2012 paper [5], where the existence of multiple linear approximations with correlation zero in target ciphers was used to propose a more data-efficient distinguisher. In a follow-up work at AsiaCrypt 2012 [2], fundamental links of integral cryptanalysis to zero-correlation cryptanalysis have been revealed. Namely, integrals (similar to saturation or multiset distinguishers) have been demonstrated to be essentially a special case of the zero-correlation property. On top of that, a multidimensional distinguisher has been constructed for the zero-correlation property, which removed the unnecessary independency assumptions on the distinguishing side. At SAC 2013 [3], an FFT technique for speeding up the key recovery in zero-correlation attacks has been proposed, which resulted in increasing the number of rounds that can be cryptanalyzed for Camellia-128 and Camellia-192 in the single-key setting.

1.3. Our contributions

In this paper, we evaluate the security of HIGHT with respect to the recent technique of zero-correlation linear cryptanalysis. Our contributions can be summarized as follows.

1. We reveal 16-round linear approximations of correlation zero in HIGHT.
2. Based on those approximations, we propose a multidimensional zero-correlation attack on 27 rounds of HIGHT (round 4 to round 30) with all whitening keys. As mentioned above, in the single-key setting, the attack on the highest number of HIGHT rounds is the 27-round impossible differential attack of [14]. However, the latter provides only a marginal improvement over the brute force, given the enormous number of random accesses to a huge memory (see Table 1). Our zero-correlation attack features a lower time complexity that does not involve expensive memory accesses and a significantly reduced memory complexity, which is in fact practical. Our attack is arguably the best non-exhaustive attack on HIGHT in the classical single-key setting.
3. We provide a key-recovery attack on 26-round HIGHT (round 4 to round 29) with all whitening keys. Note that all previous attacks on 26-round HIGHT ignored the pre-whitening key. To do this, we use the technique of multidimensional zero-correlation linear cryptanalysis. Thus, this attack of ours is the first one on 26-round HIGHT with all whitening keys in the single secret key setting.

Our results along with the previous attacks on HIGHT are shown in Table 1.

1.4. Outline

This paper is organized as follows. Section 2 briefly describes HIGHT and outlines the ideas of zero-correlation linear cryptanalysis. Section 3 presents our zero-correlation linear approximations that span 16 rounds of HIGHT. Section 4 illustrates our attacks on 26-round and 27-round HIGHT. We conclude in Section 5.

2. Preliminaries

2.1. Notation

$\boxplus$: addition modular 2^8
$\oplus$: exclusive-OR (XOR)
P_i, C_i: the i-th byte of plaintext and ciphertext, $0 \leqslant i \leqslant 7$