Differential and Rectangle Attacks on Reduced-Round SHACAL-1

Jiqiang Lu[1,⋆], Jongsung Kim[2,3,⋆⋆], Nathan Keller[4,⋆⋆⋆], and Orr Dunkelman[5,†]

[1] Information Security Group, Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Jiqiang.Lu@rhul.ac.uk
[2] ESAT/SCD-COSIC, Katholieke Universiteit Leuven
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
Kim.Jongsung@esat.kuleuven.be
[3] Center for Information Security Technologies(CIST), Korea University
Anam Dong, Sungbuk Gu, Seoul, Korea
joshep@cist.korea.ac.kr
[4] Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, Israel
nkeller@math.huji.ac.il
[5] Computer Science Department, Technion
Haifa 32000, Israel
orrd@cs.technion.ac.il

Abstract. SHACAL-1 is an 80-round block cipher with a 160-bit block size and a key of up to 512 bits. In this paper, we mount rectangle attacks on the first 51 rounds and a series of inner 52 rounds of SHACAL-1, and also mount differential attacks on the first 49 rounds and a series of inner 55 rounds of SHACAL-1. These are the best currently known cryptanalytic results on SHACAL-1 in an one key attack scenario.

Keywords: Block cipher, SHACAL-1, Differential cryptanalysis, Amplified boomerang attack, Rectangle attack.

1 Introduction

The 160-bit block cipher SHACAL-1 was proposed by Handschuh and Naccache [9,10] based on the compression function of the standardized hash function

⋆ This author as well as his work was supported by a Royal Holloway Scholarship and the European Commission under contract IST-2002-507932 (ECRYPT).

⋆⋆ This author was financed by a Ph.D grant of the Katholieke Universiteit Leuven and by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD) (KRF-2005-213-D00077) and supported by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the European Commission through the IST Programme under Contract IST2002507932 ECRYPT.

⋆⋆⋆ This author was supported by the Adams fellowship.

† This author was partially supported by the Israel MOD Research and Technology Unit.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 17–31, 2006.

SHA-1 [20]. It was selected for the second phase of the NESSIE (New European Schemes for Signatures, Integrity, and Encryption) project [18], but was not recommended for the NESSIE portfolio in 2003 because of concerns about its key schedule. Since SHACAL-1 is the compression function of SHA-1 used in encryption mode, there is much significance to investigate its security against different cryptanalytic attacks.

The security of SHACAL-1 against differential cryptanalysis [2] and linear cryptanalysis [17] was first analyzed by the proposers. Subsequently, Nakahara Jr. [19] conducted a statistical evaluation of the cipher. In 2002, Kim *et al.* [15] presented a differential attack on the first 41 rounds of SHACAL-1 with 512 key bits and an amplified boomerang attack on the first 47 rounds of SHACAL-1 with 512 key bits, where the former attack is due to a 30-round differential characteristic with probability 2^{-138}, while the latter attack is based on a 36-round amplified boomerang distinguisher (see Ref. [15] for the two differentials) that was conjectured by the authors to be the longest distinguisher (*i.e.*, the distinguisher with the greatest number of rounds). However, in 2003, Biham *et al.* [5] pointed out that the step for judging whether a final candidate subkey is the right one in the amplified boomerang attacks presented in [15] is incorrect due to a flaw in the analysis on the number of wrong quartets that satisfy the conditions of a right quartet. They then corrected it with the fact that all the subkeys of SHACAL-1 are linearly dependent on the user key. Finally, by converting the Kim *et al.*'s 36-round boomerang distinguisher to a 36-round rectangle distinguisher, Biham *et al.* presented rectangle attacks on the first 47 rounds and two series of inner 49 rounds of SHACAL-1 with 512 key bits. These are the best cryptanalytic results on SHACAL-1 in an one key attack scenario, prior to the work described in this paper. Other cryptanalytic results on SHACAL-1 include the related-key rectangle attacks [7,11,14]; however, these related-key attacks [1] are very difficult or even infeasible to be conducted in most cryptographic applications, though certain current applications may allow for them, say key-exchange protocols [13].

In this paper, we exploit some better differential characteristics than those previously known in SHACAL-1. More specifically, we exploit a 24-round differential characteristic with probability 2^{-50} for rounds 0 to 23 such that we construct a 38-round rectangle distinguisher with probability $2^{-302.3}$. Based on this distinguisher, we mount rectangle attacks on the first 51 rounds and a series of inner 52 rounds of SHACAL-1 with 512 key bits. We also exploit a 34-round differential characteristic with probability 2^{-148} for rounds 0 to 33 and a 40-round differential characteristic with probability 2^{-154} for rounds 30 to 69, which can be used to mount differential attacks on the first 49 rounds and a series of inner 55 rounds of SHACAL-1 with 512 key bits, respectively.

The rest of this paper is organised as follows. In the next section, we briefly describe the SHACAL-1 cipher, the amplified boomerang attack and the rectangle attack. In Sections 3 and 4, we present rectangle and differential attacks on the aforementioned reduced-round versions of SHACAL-1, respectively. Section 5 concludes this paper.