Attacking Reduced Rounds of the ARIA Block Cipher

Ewan Fleischmann, Michael Gorski, and Stefan Lucks

Bauhaus-University Weimar, Germany
{Ewan.Fleischmann, Michael.Gorski, Stefan.Lucks}@uni-weimar.de

Abstract. ARIA [4] is a block cipher proposed at ICISC'03. Its design is very similar to the advanced encryption standard (AES). The authors propose that on 32-bit processors, the encryption speed is at least 70% of that of the AES. They claim to offer a higher security level than AES. In this paper we present two attacks of reduced round ARIA which shows some weaknesses of the cipher. Moreover, our attacks have the lowest memory requirements compared to existing attacks on ARIA with an increase in the time complexity.

Keywords: block ciphers, differential cryptanalysis, ARIA.

1 Introduction

The ARIA block cipher [4] was presented at ICISC'03. Its design is very similar to the advanced encryption standard (AES/Rijndael) [3]. The block size is 128-bit and the key size is either 128, 192 or 256 bits. It uses the same number of rounds as the AES, which are 10, 12 and 14 respectively. ARIA employs two kinds of S-Boxes and two types of substitution layers which are different between even and odd rounds. They skip using a MixComuns operation and use an 16×16 binary matrix with branch number 8 in their diffusion layer. The authors propose that ARIA can increase the efficiency in 8-bit and 32-bit software implementations in comparison to AES. Moreover, they claim to have better security against all existing attacks on block ciphers.

Wu et al. [7] showed that there exist good impossible differentials to break up to 6 rounds of ARIA. Later Li et al. [5] presented also some impossible differential attacks of up to 6 rounds of ARIA. In this paper we apply another technique on ARIA which is called the boomerang attack. We show that our attack can also break up to 6 rounds of ARIA but with the lowest data complexity compared to previous attacks. Our results should introduce a new technique for cryptanalysis on ARIA and should therefore leave some space for further research.

The boomerang attack [6] is a strong extension to differential cryptanalysis [1] in order to break more rounds than plain differential attacks can, since the cipher is treated as a cascade of two sub-ciphers, using short differentials in each sub-cipher. These differentials are combined in an adaptive chosen plaintext and ciphertext attack to exploit properties of the cipher that have a high probability. Biryukov [2] proposed a similar boomerang attack on the AES-128 which can break up to 5 and 6 out of 10 rounds.

References

[1] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *CRYPTO*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

Table 1. Comparison of attacks on ARIA

Attack	**# Rounds**	**Data**	**Time**	**Source**
Impossible Differential	5	$2^{71.3}$	$2^{71.6}$	[5]
Boomerang Attack	5	2^{57}	$2^{115.5}$	this paper
Impossible Differential	6	2^{121}	2^{112}	[7]
Impossible Differential	6	$2^{120.5}$	$2^{104.5}$	[5]
Impossible Differential	6	2^{113}	$2^{121.6}$	[5]
Boomerang Attack	6	2^{57}	$2^{171.2}$	this paper

[2] Alex Biryukov. The Boomerang Attack on 5 and 6-Round Reduced AES. In Hans Dobbertin, Vincent Rijmen, and Aleksandra Sowa, editors, *AES Conference*, volume 3373 of *Lecture Notes in Computer Science*, pages 11–15. Springer, 2004.

[3] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.

[4] Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung, Yaekwon Sohn, Jung Hwan Song, Yongjin Yeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, and Jin Hong. New Block Cipher: ARIA. In Jong In Lim and Dong Hoon Lee, editors, *ICISC*, volume 2971 of *Lecture Notes in Computer Science*, pages 432–445. Springer, 2003.

[5] Peng Zhang Ruilin Li, Bing Sun and Chao Li. New Impossible Differential Cryptanalysis of ARIA. Cryptology ePrint Archive, Report 2008/227, 2008. http://eprint.iacr.org/.

[6] David Wagner. The Boomerang Attack. In Lars R. Knudsen, editor, *FSE*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

[7] Wenling Wu, Wentao Zhang, and Dengguo Feng. Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. *J. Comput. Sci. Technol.*, 22(3):449–456, 2007.