Improved Impossible Differential Cryptanalysis of ARIA*

Shenhua Li
Key Laboratory of Cryptologic
Technology and Information Security,
Ministry of Education, Shandong
University, Jinan, 250100, P.R. China
shenhuali@mail.sdu.edu.cn

Chunyan Song
Department of Computer Science
and Technology, Ocean University
of China, Qingdao, 266100, P.R.China
songcyan@hotmail.com

Abstract

Impossible differential cryptanalysis is a method recovering secret key by getting rid of the keys that satisfy impossible differential relations. This cryptanalysis has been used to attack AES and many good results were gotten. For the new block cipher ARIA is similar to AES in structure, it is necessary to research its security against impossible differential cryptanalysis. We find a new impossible differential property of the block cipher ARIA, and we propose an attack against ARIA reduced to six rounds based on this property. In our attack, 10 bytes of round keys are needed to be guessed instead of 12 bytes in the previous one, so the time complexity is reduced by 2^{16} times. It needs 2^{120} chosen plaintexts and 2^{96} encryptions in our attack.

1. Introduction

ARIA [5, 6, 7] is a block cipher designed by the researchers of South Korean in 2003. The algorithm uses a substitution-permutation network (SPN) structure based on AES [3]. The interface is the same as AES: 128-bit block size with key size of 128, 192, or 256 bits. ARIA version 1.0 [7], the current one, was announced and distributed on its official website at http://www.nsri.re.kr/ARIA/ in mid 2004. The number of rounds is 12/14/16. In December 2004, ATS(Agency for Technology and Standards) of Korea standardized ARIA as 128-bit Block Encryption Algorithm ARIA (KS X 1213).

In [5], Daesung Kwon et al., who are the designers, gave the initial analysis of ARIA including differential, linear, truncated differential, square attack and so on. They checked that there are no bytes whose difference is always zero or nonzero after 2-rounds of decryption, then they expected that there are no impossible differentials on 4 or more rounds. In 2004, Alex Biryukov et al. performed an independent security evaluation of ARIA in which they analyzed the security with respect to some different types of attacks [1]. Although they found that linear and truncated differential cryptanalysis work on ARIA up to 7 rounds, they did not give an evaluation of the security against impossible differential cryptanalysis which is an important method of attacking many block ciphers, especially AES [2, 4, 8]. Wenling Wu et al. proposed an impossible differential analysis of ARIA in 2007 [9]. They found a 4-rounds impossible differential characteristic and attacked on 6-round ARIA requiring 2^{121} chosen plaintexts and 2^{112} encryptions.

In this paper, we find a new four rounds impossible differential property of ARIA. Less bytes of the round keys are required to be guessed in the impossible differential attack on ARIA based on this property than in the previous attack. In our attack, the time complexity is 2^{96} and data complexity is 2^{120}, which is less than the previous impossible differential attacks.

This paper is organized as follows: In Section 2 we give a brief description of ARIA. In Section 3 we describe our new four rounds impossible differential property of ARIA. In Section 4 we propose the impossible differential cryptanalysis of ARIA reduced to six rounds and in Section 5 we summarize the paper.

2 A Brief Description of ARIA

2.1 Each round of ARIA consists of the following three parts

(1) Round key addition (RKA): XORing the 128-bit round key k_i, $1 \le i \le 15$.

(2) Substitution layer (SL): Two types of substitution layers, one is for the odd round, the other is for the even

*This work is supported by 973 Project (No.2007CB807902) and the National Natural Science Foundation of China (NSFC Grant No.90604036 and No.60525201.

978-0-7695-3126-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ISA.2008.10

round. ARIA uses two 8 × 8-bit S-boxes and their inverses in alternate types. One of these is the Rijndael S-box.

(3) Diffusion layer (DL): A simple linear map in which the 128-bit plaintexts are treated as byte matrice of size 4×4.

The 128-bit data block of ARIA includes 16 bytes with every byte numbered as the following:

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

2.2 Diffusion layer (DL)

The diffusion layer is given by

$$DL : (x_0, x_1, x_2, \cdots, x_{15}) \longmapsto (y_0, y_1, y_2, \cdots, y_{15})$$

where

$$\begin{aligned}
y_0 &= x_3 \oplus x_4 \oplus x_6 \oplus x_8 \oplus x_9 \oplus x_{13} \oplus x_{14},\\
y_1 &= x_2 \oplus x_5 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{12} \oplus x_{15},\\
y_2 &= x_1 \oplus x_4 \oplus x_6 \oplus x_{10} \oplus x_{11} \oplus x_{12} \oplus x_{15},\\
y_3 &= x_0 \oplus x_5 \oplus x_7 \oplus x_{10} \oplus x_{11} \oplus x_{13} \oplus x_{14},\\
y_4 &= x_0 \oplus x_2 \oplus x_5 \oplus x_8 \oplus x_{11} \oplus x_{14} \oplus x_{15},\\
y_5 &= x_1 \oplus x_3 \oplus x_4 \oplus x_9 \oplus x_{10} \oplus x_{14} \oplus x_{15},\\
y_6 &= x_0 \oplus x_2 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{12} \oplus x_{13},\\
y_7 &= x_1 \oplus x_3 \oplus x_6 \oplus x_8 \oplus x_{11} \oplus x_{12} \oplus x_{13},\\
y_8 &= x_0 \oplus x_1 \oplus x_4 \oplus x_7 \oplus x_{10} \oplus x_{13} \oplus x_{15},\\
y_9 &= x_0 \oplus x_1 \oplus x_5 \oplus x_6 \oplus x_{11} \oplus x_{12} \oplus x_{14},\\
y_{10} &= x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_8 \oplus x_{13} \oplus x_{15},\\
y_{11} &= x_2 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_9 \oplus x_{12} \oplus x_{14},\\
y_{12} &= x_1 \oplus x_2 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{11} \oplus x_{12},\\
y_{13} &= x_0 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_{10} \oplus x_{13},\\
y_{14} &= x_0 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_9 \oplus x_{11} \oplus x_{14},\\
y_{15} &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_8 \oplus x_{10} \oplus x_{15}.
\end{aligned}$$

$DL^{-1} : (y_0, y_1, y_2, \cdots, y_{15}) \longmapsto (x_0, x_1, x_2, \cdots, x_{15})$ comes from DL by exchanging the positions of x and y in it.

3 Four Rounds Impossible Differential Property of ARIA

Property (Impossible Differential of ARIA). Given a plaintext pair which is equal in all bytes except bytes (1,12), there is no the ciphertext pair after four rounds satisfying the following three points:

(1) The ciphertexts are not equal at bytes (3,11,12,13).

(2) The ciphertexts are equal at the other bytes.

(3) The difference of the ciphertexts at bytes (3,11,12,13) are equal.

This four impossible differential property can be expressed as

$$(0, a_1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, a_{12}, 0, 0, 0) \not\leftrightarrow$$
$$(0, 0, 0, f, 0, 0, 0, 0, 0, 0, 0, f, f, f, 0, 0), \tag{1}$$

where a_1, a_{12} and f are nonzero.

We can also find many impossible differential properties similar to (1). For example:

$$(0, 0, 0, a_3, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, a_{14}, 0) \not\leftrightarrow$$
$$(0, f, 0, 0, 0, 0, 0, 0, 0, f, 0, 0, 0, 0, f, f), \tag{2}$$

$$(0, 0, 0, 0, 0, 0, a_6, 0, 0, 0, 0, 0, 0, a_{13}, 0, 0) \not\leftrightarrow$$
$$(0, 0, 0, 0, f, 0, 0, 0, f, 0, 0, 0, 0, f, f, 0), \tag{3}$$

$$(0, 0, 0, 0, 0, 0, 0, a_7, 0, 0, 0, 0, a_{12}, 0, 0, 0) \not\leftrightarrow$$
$$(0, 0, 0, 0, 0, f, 0, 0, 0, f, 0, 0, f, 0, 0, f), \tag{4}$$

$$(a_0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, a_{14}, 0) \not\leftrightarrow$$
$$(f, 0, f, 0, 0, 0, 0, 0, f, 0, 0, f, 0, 0, 0, 0). \tag{5}$$

Next, we will prove that the impossible differential characteristic (1) is right. (See Fig. 1).

The four rounds of ARIA can be looked on as first 2 rounds and last 2 rounds.

To start with the first 2 rounds, suppose the difference of inputs satisfies the left part of (1). The difference does not change through the round key addition since two plaintexts are encrypted by same round key. After the transformation SL, the state of the difference is

$$(0, b_1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, b_{12}, 0, 0, 0),$$

where b_1, b_{12} are nonzero bytes. The DL of the first round makes the difference become

$$(0, b_{12}, b_1 \oplus b_{12}, 0, 0, b_1, b_{12}, b_1 \oplus b_{12}, b_1, b_1 \oplus b_{12}, 0, b_{12}, b_1 \oplus b_{12},$$
$$0, 0, b_1).$$

After AK and SL of the second round, the difference is

$$(0, c_1, c_2, 0, 0, c_5, c_6, c_7, c_8, c_9, 0, c_{11}, c_{12}, 0, 0, c_{15}).$$

The difference after the second DL, i.e., after the first two rounds of ARIA, is denoted as

$$(d_0, d_1, d_2, d_3, ..., d_{15}). \tag{6}$$

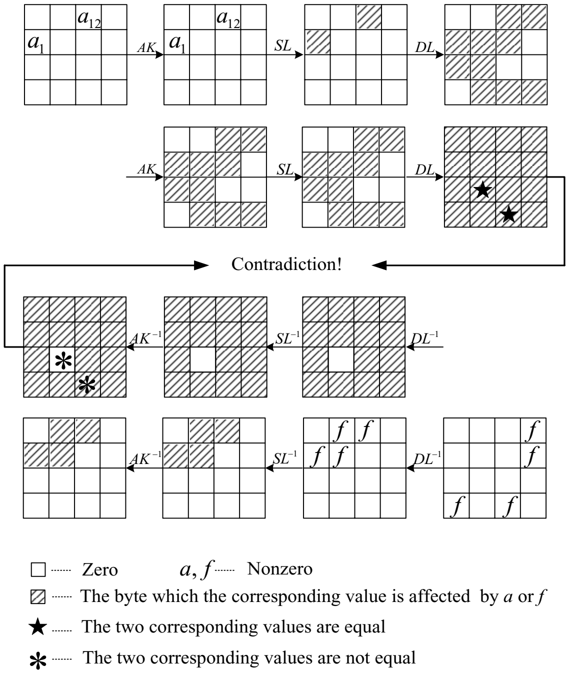
a_{12}
a_1
AK
SL
DL
Contradiction!
AK^{-1}
SL^{-1}
DL^{-1}
f
□ Zero a, f Nonzero
▨ The byte which the corresponding value is affected by a or f
★ The two corresponding values are equal
✻ The two corresponding values are not equal

Figure 1. Four rounds impossible differential property of ARIA

where, we have $d_6 = d_{11} = c_2 \oplus c_7 \oplus c_9 \oplus c_{12}$.

Furthermore, we investigate how the inverse of the last 2 rounds works on the right part of (1).

After one transformation DL^{-1}, the right part of (1) is evolved into

$$(0, f, 0, 0, f, f, 0, 0, f, 0, 0, 0, 0, 0, 0, 0).$$

Then by the transformation SL^{-1}, the difference is changed to

$$(0, e_1, 0, 0, e_4, e_5, 0, 0, e_8, 0, 0, 0, 0, 0, 0, 0),$$

where e_1, e_4, e_5 and e_8 are all nonzero. The round key addition doesn't affect the value of the difference. After the next DL^{-1}, the difference is translated to

$$(e_4 \oplus e_8, e_5 \oplus e_8, e_4, e_5, e_5 \oplus e_8, e_1 \oplus e_4, 0, e_1 \oplus e_8, e_1 \oplus e_4,$$
$$e_1 \oplus e_5, e_5 \oplus e_8, e_4, e_1, e_8, e_4 \oplus e_5, e_1 \oplus e_4 \oplus e_5 \oplus e_8) \quad (7)$$

We denote the difference after the other SL^{-1} and round key addition, i.e., after the inverse of the last 2 rounds, as

$$(d_0^*, d_1^*, d_2^*, d_3^*, ..., d_{15}^*), \quad (8)$$

where $d_{11}^* \neq 0$ as $SL^{-1}(d_{11}^*) = e_4 \neq 0$. However, we know $d_6^* = 0$ from (7) easily. So we have $d_6^* \neq d_{11}^*$.

Then we get a contradiction from (6) and (8), so the property of the four rounds impossible differential (1) is right. The other properties such as (2) (3) (4) (5) can be proved similarly.

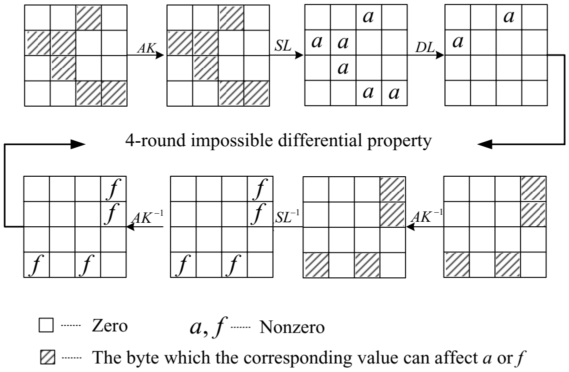
AK
SL
DL
a
4-round impossible differential property
AK^{-1}
SL^{-1}
f
□ Zero a, f Nonzero
▨ The byte which the corresponding value can affect a or f

Figure 2. Impossible differential cryptanalysis of ARIA reduced to six rounds

4 Impossible Differential Cryptanalysis of ARIA Reduced to Six Rounds

In this section, we propose an improved impossible differential cryptanalysis of ARIA reduced to six rounds. This attack is based on the four round impossible differential property with additional one round at the beginning and the end of it. The process is illustrated in the following in Fig. 2.

The procedure with 9 steps is described as follows in detail. In our attack, 10 bytes of round keys are needed to be guessed instead of 12 bytes in the previous one.

1. A structure is defined as a set of 2^{48} plaintexts which have fixed values in all but six bytes (1,5,6,8,11,15). Such a structure proposes $2^{48} \times 2^{48} \times \frac{1}{2} = 2^{95}$pairs of plaintexts.

2. Take 2^{71} structures, i.e., 2^{119} plaintexts, 2^{166} plaintexts pairs. Select pairs whose ciphertext pairs have zero difference at the twelve bytes (0,1,2,4,5,6,7,8,9,10,14,15). The expected number of such pairs is about $2^{166} \times 2^{-96} = 2^{70}$.

3. Guess a 4-byte value at bytes (3,11,12,13) of the last round key k_7.

4. For each ciphertext pair (C, C'), compute $C_5 \oplus C'_5 = SL^{-1}(C \oplus k_7) \oplus SL^{-1}(C' \oplus k_7)$ and choose pairs whose difference $C_5 \oplus C'_5$ is same at the four bytes (3,11,12,13). Since the probability is about $p = (2^{-8})^3 = 2^{-24}$, the expected number of the remaining pairs is $2^{70} \times 2^{-24} = 2^{46}$.

5. For a plaintext pair (P, P') with such ciphertext pairs and 6-byte value at the bytes (1,5,6,8,11,15) of the initial key k_1, calculate $SL(P \oplus k_1) \oplus SL(P' \oplus k_1)$ and choose pairs whose difference are same at the six bytes

Table 1. Comparison of impossible differential cryptanalysis of ARIA

Rounds	Chosen Plaintexts	# Encryptions	Source
6	2^{121}	2^{112}	Ref. [9]
6	2^{120}	2^{96}	This paper

(1,5,6,8,11,15) after SL transformation. The probability is about 2^{-40}.

6. Since such a difference is impossible, every key that proposes such difference is a wrong key. After analyzing 2^{46} ciphertext pairs, there remain only about $2^{48} \times (1 - 2^{-40})^{2^{46}} = 2^{-44}$ wrong values of the six bytes of k_0.
7. Unless the initial assumption on the final round key k_7 is correct, it is expected that we can get rid of the whole 48-bit value of k_1 for each 32-bit value of k_7 since the wrong value (k_1, k_7) remains with the probability 2^{-12}. Hence if there remains a value of k_1, we can assume the key k_7 is a right key.
8. In step 4, we compute the 3rd and 11th byte of $C_5 \oplus C'_5$ and judge whether they are equal. If yes, continue computing the other bytes. So this step requires about $2^{16} \times 2^{70} + 2^{24} \times 2^{62} + 2^{32} \times 2^{54} = 3 \times 2^{86}$ one round operations. Similarly, Step 5 requires about $2^{32} \times (2^{16} \times 2^{47} + 2^{24} \times 2^{39} + ... + 2^{48} \times 2^{15}) = 5 \times 2^{95}$ one round operations.
9. Repeat the above Steps after changing the impossible differential characters, we can get the whole value of k_1. Consequently, this attack requires about 2^{120} chosen plaintexts and 2^{96} encryptions of ARIA reduced to six rounds.

5 Conclusion

We presented an impossible differential attack against ARIA reduced to six rounds. This attack needs 2^{120} chosen plaintexts and 2^{96} encryptions. Our results are better than previous impossible differential cryptanalysis results on the ARIA as far as we know to date. In Table 1, we briefly presented a comparison of our attacks with previous impossible differential cryptanalysis of the ARIA.

Acknowledgments

The authors would like to thank Professor Xiaoyun Wang for her invaluable discussions and suggestions. The authors also thank Haina Zhang and Wei Wang for their helpful comments.

References

[1] Alex Biryukov, Christophe De Canniere et al. Secruity and performance analysis of ARIA. http://homes.esat.kuleuven.be/ abiryuko/ARIA-COSICreport.pdf.

[2] Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, SungWoo. Kang. Improved impossible differential cryptanalysis of Rijndael and Crypton. *3rd International Conference on Information Security and Cryptology (ICISC 2001), LNCS 2288*, pp. 39-49, Springer-Verlag, Berlin, 2001.

[3] Vincent Rijmen, Joan Daemen. AES Proposal: Rijndael. http://csrc.nist.gov/envryption/aes/rijndael.

[4] Goce Jakimoski, Yvo Desmedt. Related-key differential cryptanalysis of 192-bit key AES variants. *Selected Areas in Cryptography (SAC'2003), LNCS 3006*, pp. 208-221 Springer-Verlag, 2003.

[5] Daesung Kwon, Jaesung Kim, Sangwoo Park, et al. New Block Cipher: ARIA. *Information Security and Cryptology (ICISC'03), LNCS 2971*, pp. 432-445, Springer-Verlag 2004.

[6] National Security Research Institute, Specification of ARIA, Version 0.8, August, 2003.

[7] National Security Research Institute, Specification of ARIA, Version 1.0, Janaulary 2005. 0.8 http://www.nsri.re.kr/ARIA/doc/ARIA-specification-e.pdf

[8] Raphael Chung-Wei Phan. Impossible Differential Cryptanalysis of 7-round AES. *Information Processing Letters, Vol. 91, Number 1*, pp. 33-38, 2004.

[9] Wenling Wu, Wentao Zhang, Dengguo Feng. Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. *J. Comput. Sci. Technol, Vol. 22, No.3*, pp. 453-460, 2007.