Improved Impossible Differential Attack on 7-round Reduced ARIA-256

Xuan Shen* and Jun He
College of Information and Communication, National University of Defense Technology
Wuhan 430010, Hubei - P. R. China
[e-mail: shenxuan_08@163.com]
*Corresponding author: Xuan Shen

Received April 26, 2019; accepted June 9, 2019;
published November 30, 2019

Abstract

ARIA is an involutory SPN block cipher. Its block size is 128-bit and the master key sizes are 128/192/256-bit, respectively. Accordingly, they are called ARIA-128/192/256. As we all know, ARIA is a Korean Standard block cipher nowadays. This paper focuses on the security of ARIA against impossible differential attack. We firstly construct a new 4-round impossible differential of ARIA. Furthermore, based on this impossible differential, a new 7-round impossible differential attack on ARIA-256 is proposed in our paper. This attack needs 2^{118} chosen plaintexts and 2^{210} 7-round encryptions. Comparing with the previous best result, we improve both the data complexity and time complexity. To our knowledge, it is the best impossible differential attack on ARIA-256 so far.

Keywords: ARIA, impossible differential attack, data complexity, time complexity, early-abort technique

http://doi.org/10.3837/tiis.2019.11.027 **ISSN : 1976-7277**

1. Introduction

ARIA [1] was published by National Security Research Institute of Korea in 2003. One year later, it was selected as a Korean Standard block cipher. ARIA takes involution SPN structure. The block size of ARIA is 128-bit , while the master key sizes are 128/192/256-bit, respectively. We call them ARIA-128/192/256 accordingly. Moreover, the rounds of these three versions are 12/14/16, respectively. After ARIA was published, many cryptographers have analyzed ARIA from various security views, including differential cryptanalysis, linear cryptanalysis and so on [2]-[6].

Among kinds of cryptanalytic methods, impossible differential attack (short for IDA in our paper) is a very effective attack against many byte-oriented block ciphers [7]-[11]. It was first proposed to attack DEAL and Skipjack block ciphers by Knudsen [12] and Biham et al. [6],respectively. The main idea of this attack is exploiting an impossible differential (short for ID in our paper) to remove the wrong keys.

For ARIA, in 2006, Wu et al. [13] first constructed some nontrivial 4-round ID of ARIA, and attacked reduced to 6 rounds of ARIA-128 with 2^{121} data complexity and 2^{112} time complexity. Later, at ISA 2008, Li et al. [14] found a new ID of ARIA-128, and they improved the complexity for 6-round attack. After that, in 2010, Li et al. [15] further improved 5/6-round IDA on ARIA-128. At the same year, at CANS 2010, Du et al. [16] first proposed 7-round IDA on ARIA-256, the attack needs 2^{125} data complexity and 2^{238} time complexity. Then, in 2012, Su [17] improved 7-round IDA with 2^{120} data complexity and 2^{219} time complexity. Very recently, Xie et al. [18] constructed a new 4-round ID and further improved 7-round IDA with only half of the previous best complexity in 2018. The summary of IDA on ARIA is shown in **Table 1**.

Table 1. Summary of impossible differential attack on ARIA

Round	Data Complexity	Time Complexity	Source
6	2^{121}	2^{112}	[13]
6	2^{120}	2^{96}	[14]
6	2^{113}	$2^{121.6}$	[15]
7	2^{125}	2^{238}	[16]
7	2^{120}	2^{219}	[17]
7	2^{119}	2^{218}	[18]
7	2^{118}	2^{210}	Ours

In our paper, we first construct a new 4-round ID of ARIA. Then, based on this new ID of ARIA, a 7-round impossible differential attack is proposed. The data and time complexity of our attack is 2^{118} and 2^{210}, respectively. Comparing with the known IDAs on ARIA-256, our result is the best one.

Organization. In Section 2, we first give some notations that will be used in our paper, then show a description of ARIA and the principle of IDA. After that, we construct a new 4-round ID of ARIA in Section 3. Moreover, with this ID, a 7-round attack on ARIA-256 is shown in Section 4. At the end, we conclude our paper in Section 5.

2. Preliminary

2.1 Notations

In this section, we define some notations described in **Table 2**.

Table 2. Some notations that will be used in this paper

Notations	Meanings
X_r^I	The input value of the r-th round
X_r^S	The value after the substitution layer of the r-th round
X_r^O	The output value of the r-th round
ΔX_r^*	The difference of X_r^*,where $*\in\{I,S,O\}$
K_r	The r-th round key
$K_{r,s}$	The s-th byte of K_r
R_r	The r-th round

2.2 Description of ARIA

The encryption process of ARIA block cipher is given in **Fig. 1**. Its 128-bit state is viewed as a 4×4 byte matrix described in **Fig. 2**. The iterative round function of ARIA is made up of three components:

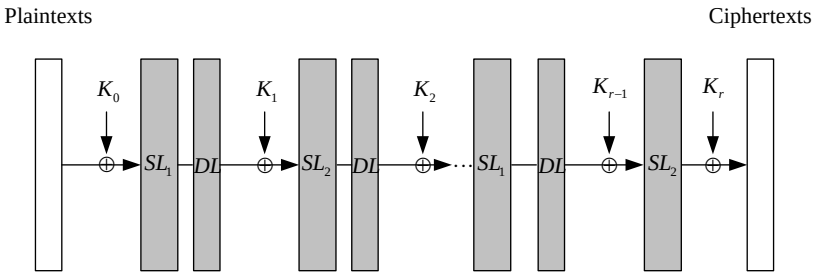

Fig. 1. Encryption process of ARIA

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

Fig. 2. 128-bit state of ARIA

- ***SL***: ARIA takes two kinds of Sboxes: S_1 and S_2. S_1^{-1} and S_2^{-1} denote the inverse of S_1 and S_2, respectively. Note that all of the sboxes in ARIA are 8-bit. In ARIA, SL_1/SL_2 are taken in the odd/ even rounds, respectively. They are given in **Fig. 3**.

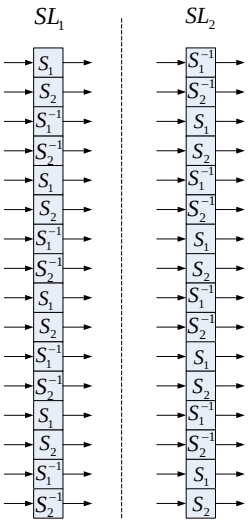

Fig. 3. Two types of substitution layers in ARIA

- ***DL***: After working by *SL*, a state is updated by a 16×16 involutory binary matrix. For a 128-bit state $X=(x_0, x_1, x_2, \cdots, x_{13}, x_{14}, x_{15})$, where $x_i(i=0,1,2, \cdots,13,14,15)$ is a byte, *DL* is presented by $Y=AX$, and *A* is a matrix given in **Fig. 4**.

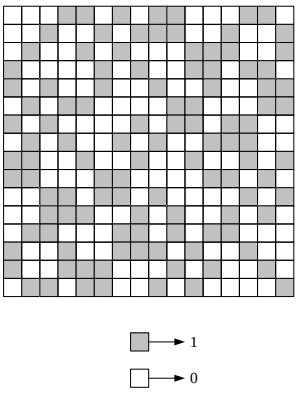

Fig. 4. Matrix of *DL* in ARIA

- ***RKA***: It is updated by XORing the round key with the middle states, where the round key is obtained by the key schedule of ARIA.

More details of ARIA that are not necessary for this paper can be referred to [1], we do not present them in our paper.

2.3 Principle of impossible differential attack

Impossible differential attack can be divided into two steps. Firstly, one needs to construct an impossible differential. In this step, the most popular method to find impossible differentials is using the miss-in-the-middle technique. With this technique, the contradictions are obtained in the middle matching parts from the encryption and decryption directions. The other step is exploiting the constructed impossible differential to remove the wrong keys.

As shown in **Fig. 5**, for a cipher E, the whole encryption could be divided into three parts: $E = E_2 \circ E_1 \circ E_0$, where E_1 is the encryption of the impossible differential, E_0 and E_2 are some rounds encryption added to E_1 at the beginning and at the end, respectively. Firstly, we construct an impossible differential $\Delta\alpha \rightarrow \Delta\beta$ in E_1. Then, if the round keys that need to be guessed in E_0 and E_2 are independent, we respectively guess the round keys to reduce the complexity. For example, choose a pair of plaintexts (P,P^*) and the corresponding pair of ciphertexts (C,C^*). We first guess the involved round keys κ_0 in E_0 for (P,P^*) and calculate the output difference of E_0. If it is equal to $\Delta\alpha$, we put the keys κ_0 into table A. With the same way, we guess the involved round keys κ_2 in E_2 for (C,C^*) and calculate the output difference of E_2. If it is equal to $\Delta\beta$, we put the keys κ_2 into table B. Finally, we only need to remove the candidate keys (κ_0, κ_2) in table A×B because the differential $\Delta\alpha \rightarrow \Delta\beta$ is impossible.

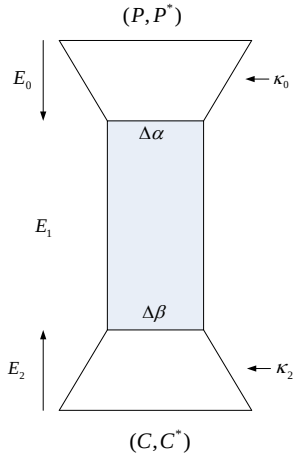

Fig. 5. Whole frame of impossible differential attack

We denote l_0, l_2 by the bit number of guessed keys in E_0 and E_2,respectively. Moreover, if the probability that the random key can be remained through a pair of plaintexts (P,P^*) is $1\text{-}2^{-c}$, where c denotes the total bit number of the matched conditions, the probability that the random key can be remained through N pairs of plaintexts is

$$Pr = (1-2^{-c})^N \approx e^{-N/2^c}.$$

Then, choose different probability Pr, the complexity of the attack can be different. For example, if all wrong keys are requested to remove, N needs to satisfy the following inequation:

$$Pr = (1-2^{-c})^N \le 2^{-(l_0+l_2)} \Rightarrow N \ge (l_0+l_2) \times \ln 2 \times 2^c.$$

If N needs to satisfy $Pr = (1-2^{-c})^N \le 2^{-1}$, which means only half of all wrong keys are requested to remove at least, N only needs to satisfy $N \ge \ln 2 \times 2^c$.

Note that all wrong keys are requested to remove in the previous best result [18]. However, we will take much appropriate Pr in this paper such that the complexity can be improved comparing with the previous one.

3. The 4-round impossible differential of ARIA

We mainly construct a 4-round impossible differential of ARIA in this section.

Proposition 1. For ARIA, the following 4-round differential is impossible:

$$(a_0,0,0,0,0,\ a_5,0,0,0,0,0,0,0,0,0,0)\rightarrow(f,f,0,0,0,0,f,0,0,0,0,0,0,0,f,0)$$

where all of a_0, a_5 and f denote non-zero byte.

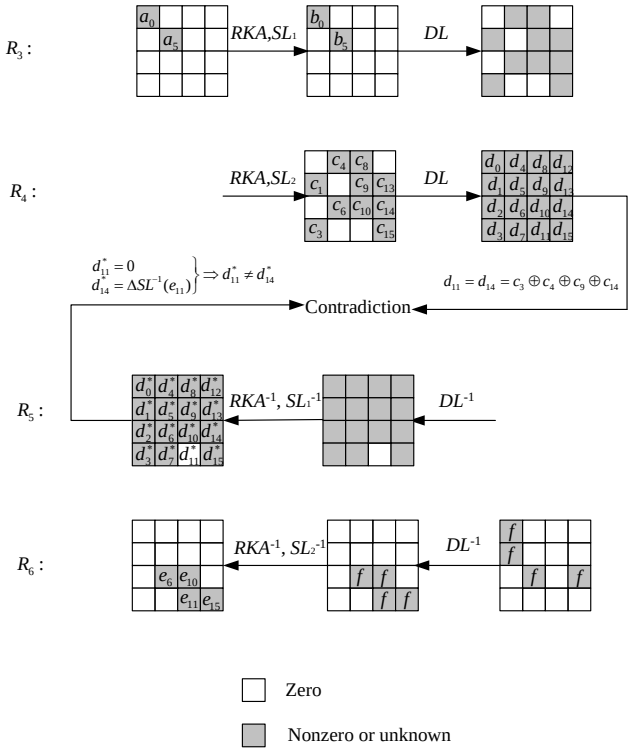

Fig. 6. The 4-round impossible differential of ARIA

Proof. It should be pointed out that the difference does not change through the *RKA* and RKA^{-1}. As shown in **Fig. 6**, we first give the 2-round differential from the encryption direction as follows:

Since $\Delta X_3^I = (a_0,0,0,0,0,\ a_5,0,0,0,0,0,0,0,0,0,0)$, after *RKA* and SL_1 of R_3, the difference is $\Delta X_3^S = (b_0,0,0,0,0,b_5,0,0,0,0,0,0,0,0,0,0)$, where both b_0 and b_5 are unknown non-zero bytes. Then, after *DL* of R_3,*RKA* and SL_2 of R_4, ΔX_4^S become $(0,c_1,0,\ c_3,\ c_4,\ 0,\ c_6,0,\ c_8,\ c_9,\ c_{10},0,0,\ c_{13},\ c_{14},\ c_{15})$. Moreover, after *DL* of R_4, the difference is $\Delta X_4^O = (d_0,d_1,\ d_2,\cdots,d_{14},d_{15})$, where

$$d_{11}= d_{14}= c_3\oplus\ c_4\oplus\ c_5\oplus\ c_{14}.$$

Thus, the difference ΔX_3^I evolves into ΔX_4^O with probability 1, and the 11-th byte and 14-th byte values of ΔX_4^O are the same.

From the decryption direction, we show the 2-round differential propagation (R_5 and R_6). Given that $\Delta X_6^O=(\ f,f,0,0,0,0,f,0,0,0,0,0,0,0,f,0)$, we get that $\Delta X_5^S =(0,0,0,0,0,0,f,0,0,0,f,$ $f,0,0,0,f)$ through $DL^{-1}$of R_6. Moreover, after SL_2^{-1} and $RKA^{-1}$of R_6, the difference is $\Delta X_6^I = (0,0,0,0,0,0,e_6,0,0,0,e_{10},e_{11},0,0,0,e_{15})$, where all of e_6,e_{10},e_{11},e_{15} are unknown non-zero bytes. Moreover, after DL^{-1},SL_1^{-1},RKA^{-1} of R_5, the difference is $\Delta X_5^I=(d_0^*,\ d_1^*,\ d_2^*,\cdots,\ d_{14}^*,\ d_{15}^*)$ where

$$d_{11}^{*}=0,\ d_{14}^{*}=\Delta SL^{-1}(e_{11}).$$

Given that $e_{11}=\Delta SL^{-1}(f)\neq 0$, $d_{14}^{*}=\Delta SL^{-1}(e_{11})\neq 0$, thus, we have $d_{11}^{*}\neq d_{14}^{*}$, which contradicts $d_{11}=d_{14}$ in the former 2-round differential. So, this 4-round impossible differential is constructed. □

4. The 7-round impossible differential attack on ARIA−256

In this section, with the above impossible differential, we propose the 7-round impossible differential attack on ARIA-256 whose data/time complexity is $2^{118}/2^{210}$. Comparing with the previous known results, the better threshold value of *Pr* will be taken and our attack can get better results.

The 7-round impossible differential attack on ARIA-256 is described in **Fig. 7**. Before giving the procedure of this attack, we first present the following proposition which will be used to calculate the complexity.

Proposition 2. In **Fig. 7**, when the following four equations hold,

$$\begin{cases} c_1 = c_4; \\ c_3 = c_6; \\ c_9 = c_{12}; \\ c_2 \oplus c_7 \oplus c_8 \oplus c_{10} \oplus c_{13} \oplus c_{15} = 0, \end{cases}$$

the probability that making ΔX_1^{S} become ΔX_1^{O} whose 10 byte differences (0,2,3,4,5,7,9, 11,12,14) are zero is 2^{-32}.

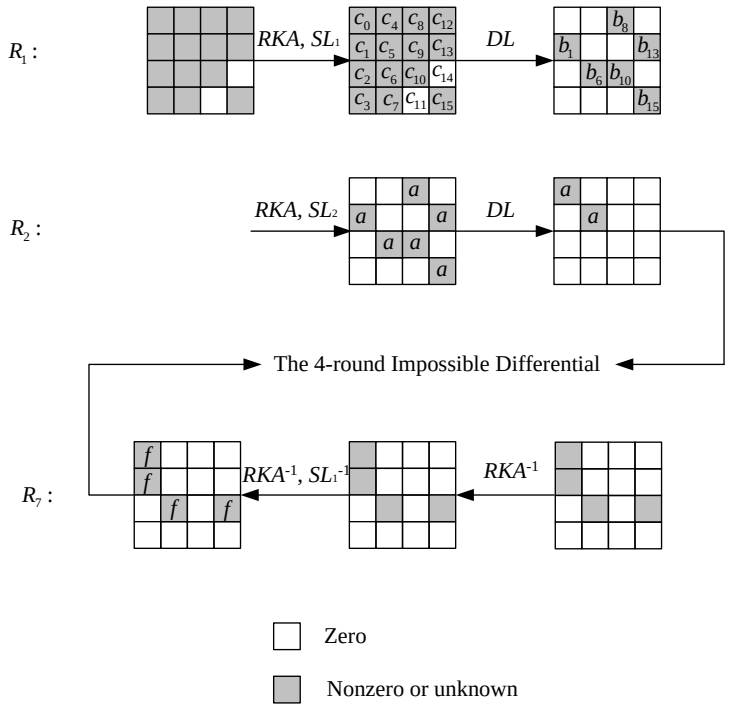

Fig. 7. The 7-round impossible differential attack on ARIA-256

Proof . We define a state structure that the (0,2,3,4,5,7,9,11,12,14)-byte differences are zero, the other 8 byte differences are nonzero. Then, one structure has 2^{48} states. In **Fig. 7**, after DL^{-1} of R_1, we can get that $c_1=b_8 \oplus b_{15}$,$c_4=b_8 \oplus b_{15}$. So, $c_1=c_4$ with the probability 1 no matter what b_8 and b_{15} are. With the same method, we have

$$\begin{cases} c_3 = c_6 = b_{10} \oplus b_{13}; \\ c_9 = c_{12} = b_1 \oplus b_6. \end{cases}$$

Since

$$\begin{cases} c_2 = b_1 \oplus b_6 \oplus b_{10} \oplus b_{15}; \\ c_7 = b_1 \oplus b_6 \oplus b_8 \oplus b_{13}; \\ c_8 = b_1 \oplus b_{10} \oplus b_{13} \oplus b_{15}; \\ c_{10} = b_6 \oplus b_8 \oplus b_{13} \oplus b_{15}; \\ c_{13} = b_6 \oplus b_8 \oplus b_{10} \oplus b_{13}; \\ c_{15} = b_1 \oplus b_8 \oplus b_{10} \oplus b_{15}, \end{cases}$$

we have $c_2 \oplus c_7 \oplus c_8 \oplus c_{10} \oplus c_{13} \oplus c_{15}=0$. Thus, all of the four equations hold with probability 1. However, one of them holds with the probability 2^{-8} randomly. Therefore, the number of ΔX_1^S is $2^{112}\times(2^{-8})^4=2^{80}$. Given that DL is the linear transformation and the number of ΔX_1^O is 2^{48}, the probability that making ΔX_1^S become ΔX_1^O in **Fig. 7** is $2^{48}/2^{80}=2^{-32}$. □

Note that the probability that ΔX_1^O satisfies 10 byte differences (0,2,3,4,5,7,9,11,12, 14) are zero randomly is $(2^{-8})^{10}=2^{-80}<2^{-32}$.

Our key recovery procedure for 7-round ARIA-256 is given below.

Step 1: Choose structures of 2^{112} plaintexts that they are different at the 14 bytes (0,1,2,3,4,5,6,7,8,9,10,12,13,15), and taking all values in the above 14 bytes. Thus, every structure can proposes $2^{112}\times2^{112}\times1/2 = 2^{223}$ pairs of plaintexts.

Step 2: Take 2^n structures (2^{n+112} plaintexts and 2^{n+223} pairs of plaintexts). We only retain the pairs that the corresponding ciphertext pairs are zero difference at the 12 bytes (2,3,4,5,7,8,9,10,11,12,13,15). So, about $2^{n+223}\times2^{-8\times12}=2^{n+127}$ pairs can be remained.

Since the guessed round keys in the encryption and decryption can be viewed independently, we will get the candidate round keys that belong to table A and table B, respectively.

Step 3: Guess the 112-bit value of K_1.

Step 3.1: For every remaining plaintext pair (P,P^*), guess the candidates of $(K_{1,1},K_{1,4})$, calculate $SL_1(P \oplus K_1) \oplus SL_1(P^* \oplus K_1)$, and check if the values of two bytes (1,4) are same. If yes, remain the plaintext pair. Consider that the probability is 2^{-8}, $2^{n+127}\times2^{-8} = 2^{n+119}$ pairs can be remained.

Step 3.2: Similarly, for every remaining pair (P,P^*), guess the candidates of $(K_{1,3},K_{1,6})$, calculate $SL_1(P \oplus K_1) \oplus SL_1(P^* \oplus K_1)$, and check if the values of two bytes (3,6) are same. If yes, remain the plaintext pair. Consider that the probability is 2^{-8}, $2^{n+119}\times2^{-8} = 2^{n+111}$ pairs can be remained.

Step 3.3: Guess the candidates of $(K_{1,9},K_{1,12})$, calculate $SL_1(P \oplus K_1) \oplus SL_1(P^* \oplus K_1)$, and check if the values of two bytes (9,12) are same. If yes, remain the plaintext pair. Consider that the probability is 2^{-8}, $2^{n+111}\times 2^{-8} = 2^{n+103}$ pairs can be remained.

Step 3.4: Guess the candidates of $(K_{1,2},K_{1,7},K_{1,8},K_{1,10},K_{1,13},K_{1,15})$, calculate $SL_1(P \oplus K_1) \oplus SL_1(P^* \oplus K_1)$, and check if the XOR sum of the six bytes (2,7,8,10,13,15) is zero. If yes, remain the plaintext pair. Consider that the probability is 2^{-8}, $2^{n+103}\times 2^{-8} = 2^{n+95}$ pairs can be remained.

Step 3.5: Guess the candidates of $(K_{1,0},K_{1,5})$, calculate the two bytes (0,5) of $SL_1(P \oplus K_1) \oplus SL_1(P^* \oplus K_1)$.

Step 3.6: For the remaining pairs, calculate ΔX_1^O and check if all of the 10 bytes (0,2,3,4,5,7,9,11,12,14) are zero. If yes, remain the pairs. According to proposition 2, the probability is 2^{-32}, $2^{n+95}\times 2^{-32} = 2^{n+63}$ pairs can be remained.

Step 4: For every remaining pair (P,P^*), guess the candidates of $(K_{2,1},K_{2,6},K_{2,8},K_{2,10},K_{2,13},K_{2,15})$, calculate $SL_2(P \oplus K_2) \oplus SL_2(P^* \oplus K_2)$, and check if the values of six bytes (1,6,8,10,13,15) are same. If yes, remain the plaintext pair. Consider that the probability is $2^{-8\times 5}$, $2^{n+63}\times 2^{-8\times 5}=2^{n+23}$ pairs can be remained.

Step 5: In the decryption direction, for every remaining pair (C,C^*) after step 2, guess the candidates of $(K_{8,0},K_{8,1},K_{8,6},K_{8,14})$, calculate $SL_1(C \oplus K_8) \oplus SL_1(C^* \oplus K_8)$, and check if the values of four bytes (0,1,6,14) are same. If yes, remain the plaintext pair. Consider that the probability is $2^{-8\times 3}$, $2^{n+127}\times 2^{-8\times 3}=2^{n+103}$ pairs can be remained.

Complexity analysis: The data complexity is 2^{n+112} chosen plaintexts. We mainly calculate the time complexity presented in **Table 3**. Note that one round encryption of ARIA is made up of *SL*, *DL*, and *RKA* (*DL* is omitted in the last round), every encryption of *SL*, *DL*, and *RKA* is equal to 1/3 one round encryption.

- Step 3.1 needs guess 2^{16} candidate keys and only 2 sboxes (total 16 sboxes in *SL*) are involved. Then, its time complexity is $2^{n+127}\times 2^{16}\times 2\times 2/16\times 2/3=1/3\times 2^{n+142}$one round encryption.
- Step 3.2 needs guess 2^{16} candidate keys and only 2 sboxes are involved. Then, its time complexity is $2^{16}\times 2^{n+119}\times 2^{16}\times 2\times 2/16\times 2/3=1/3\times 2^{n+150}$ one round encryption.
- Step 3.3 needs guess 2^{16} candidate keys and only 2 sboxes are involved. Then, its time complexity is $2^{32}\times 2^{n+111}\times 2^{16}\times 2\times 2/16\times 2/3 =1/3\times 2^{n+158}$one round encryption.
- Step 3.4 needs guess 2^{48} candidate keys and only 6 sboxes are involved. Then, its time complexity is $2^{48}\times 2^{n+103}\times 2^{48}\times 2\times 6/16\times 2/3 =2^{n+198}$one round encryption.
- Step 3.5 needs guess 2^{16} candidate keys and only 6 sboxes are involved. Then, its time complexity is $2^{96}\times 2^{n+95}\times 2^{16}\times 2\times 2/16\times 2/3=1/3\times 2^{n+206}$ one round encryption.
- Step 3.6 does not need guess any candidate keys and calculate *DL* encryption of R_1. Then, its time complexity is $2^{112}\times 2^{n+95}\times 2\times 1/3= 1/3\times 2^{n+208}$one round encryption.
- Step 4 needs guess 2^{48} candidate keys. Note that the early-abort technique [19] is applied in this step. It can be used to reduce the time complexity. Firstly, check whether the two bytes (1,6) of ΔX_2^S are the same, If yes, go on checking the two bytes (6,8) of ΔX_2^S ,and so on. Then, its time complexity is

  $$2^{112}\times(2^{n+63}\times 2^{16}+2^{n+55}\times 2^{24}+2^{n+47}\times 2^{32}+2^{n+39}\times 2^{40}+2^{n+31}\times 2^{48})\times 2\times 6/16\times 2/3 =5\times 2^{n+190}$$

  one round encryption.

- Step 5 needs guess 2^{32} candidate keys. The early-abort technique is also applied in this step. Then, its time complexity is

$$(2^{n+127}\times 2^{16}+2^{n+119}\times 2^{24}+2^{n+111}\times 2^{32})\times 2\times 4/16=3\times 2^{n+142}$$

one round encryption.

Table 3. Complexity analysis of 7-round impossible differential attack

Step	Guessed round key	Ngk (bit)	Nmc (bit)	Remaining pairs (pair)	TC (one round encryption)
3.1	$K_{1,1},K_{1,4}$	16	8	$2^{n+127-8}=2^{n+119}$	$1/3\times 2^{n+142}$
3.2	$K_{1,3},K_{1,6}$	16	8	$2^{n+119-8}=2^{n+111}$	$1/3\times 2^{n+150}$
3.3	$K_{1,9},K_{1,12}$	16	8	$2^{n+111-8}=2^{n+103}$	$1/3\times 2^{n+158}$
3.4	$K_{1,2},K_{1,7}$, $K_{1,8},K_{1,10}$, $K_{1,13}$, $K_{1,15}$	48	8	$2^{n+103-8}=2^{n+95}$	2^{n+198}
3.5	$K_{1,0},K_{1,5}$	16	0	$2^{n+95-0}=2^{n+95}$	$1/3\times 2^{n+206}$
3.6			32	$2^{n+95-32}=2^{n+63}$	$1/3\times 2^{n+208}$
4	$K_{2,1},K_{2,6}$, $K_{2,8},K_{2,10}$, $K_{2,13}$, $K_{2,15}$	48	40	$2^{n+63-40}=2^{n+23}$	$5\times 2^{n+190}$
5	$K_{8,0}$, $K_{8,1}$, $K_{8,6}$, $K_{8,14}$	32	24	$2^{n+127-24}=2^{n+103}$	$3\times 2^{n+142}$

Ngk: Number of guessed round key;

Nmc: Number of the matched condition;

TC: Time Complexity.

Combining with the above steps, the time complexity of our attack is

$$1/3\times 2^{n+142}+1/3\times 2^{n+150}+1/3\times 2^{n+158}+2^{n+198}+1/3\times 2^{n+206}+1/3\times 2^{n+208}+5\times 2^{n+190}+3\times 2^{n+142}\approx$$

$$5/12\times 2^{n+208}\text{ (one round encryption).}$$

It is about $1/7\times 5/12\times 2^{n+208}\approx 2^{n+201.61}$ 7-round encryption of ARIA-256.

Note that the total number of the matched condition is (8+8+8+8+32+40+24)=128 bits, it means that the probability which the random key can be remained through a pair of plaintexts (P,P^*) is $1-2^{-128}$. For the whole 256-bit master key, there exist 192-bit key in our attack. Moreover, for the 192-bit key, we can reduce it from 2^{192} candidates to

$$(2^{192}-1)\times(1-2^{-128})^{2^{n+127}}\approx 2^{192}\times e^{-2^{n-1}}\approx 2^{192-1.44\times 2^{n-1}}.$$

Considering the candidate keys which are remained after our attack and 256-192=64 bit keys which are not involved in our attack, the time complexity for recovering the whole 256-bit master key is

$$2^{n+201.61}+2^{192-1.44\times 2^{n-1}}\times 2^{64}=2^{n+201.61}+2^{256-1.44\times 2^{n-1}}\text{ (7-round encryption).}$$

Note that the best result of ARIA-256 known so far is given in [18] which the time complexity is 2^{218} 7-round encryptions, thus we need

$$2^{n+201.61}+2^{256-1.44\times 2^{n-1}}<2^{218}.$$

When we take n=6, the total time complexity for recovering the 256-bit master key is

$$2^{6+201.61} + 2^{256-1.44\times 2^{6-1}} \approx 2^{207.61} + 2^{210} \approx 2^{210} \text{ (7-round encryption).}$$

Meanwhile, for the data complexity, $2^{n+112}=2^{6+112}=2^{118}$ chosen plaintexts are needed for our attack, it is only half of the data complexity presented in [18].

4. Conclusion

With the new 4-round impossible differential constructed in this paper, we gave the 7-round impossible differential attack on ARIA-256. Different from the previous impossible differential attacks on ARIA-256, we carefully chose the threshold value of the probability that the random key can be remained through some pairs of plaintexts. By this method, the complexity of our attack can be improved than the previous known results. Specifically, the data complexity is 2^{118} which is only half of the known best one, while the time complexity is 2^{210} which is reduced by 2^8 times compared with the known best one.

References

[1] Kwon D, Kim J, Park S, et al., "New block cipher: ARIA," in *Proc. of 6-th International Conference on Information Security and Cryptology-ICISC 2003*, 2971, 432-445, 2003. Article (CrossRef Link).

[2] Biham E, Shamir A, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, 4(1), 3-72, 1991. Article (CrossRef Link).

[3] Matsui M, "Linear cryptanalysis method for DES cipher," in *Proc. of Advances in Cryptology -EUROCRYPT 1993*, 386-397,1994. Article (CrossRef Link).

[4] Knudsen L R, Wagner D, "Integral cryptanalysis," *Fast Software Encryption-FSE 2002*, pp. 112-127, 2002. Article (CrossRef Link).

[5] Knudsen L R, "Truncated and higher order differentials," *Fast Software Encryption-FSE 1994*, 196-211,1995. Article (CrossRef Link).

[6] Biham E, Biryukov A, Shamir A, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," in *Proc. of Advances in Cryptology-EUROCRYPT 1999*, 12-23, 1999. Article (CrossRef Link).

[7] Zhang K, Guan J, Hu B, "Impossible differential cryptanalysis on DVB-CSA," *KSII Transactions on Internet and Information Systems*, 10(4), 1944-1956, 2016. Article (CrossRef Link).

[8] Han G Y, Zhang W Y, Zhao, H L, "An upper bound of the longest impossible differentials of several block ciphers," *KSII Transactions on Internet and Information Systems*, 13(1), 435-451, 2019. Article (CrossRef Link).

[9] Cui T, Jin C H, "Finding impossible differentials for Rijndael-like and 3D-like structures," *KSII Transactions on Internet and Information Systems*, 7(3), 509-520, 2013. Article (CrossRef Link).

[10] Shen X, Liu G Q, Li C, et al., "Impossible differential cryptanalysis of Fantomas and Robin" *IEICE Trans. Fundamentals*, E101-A(5), 863-866, 2018. Article (CrossRef Link).

[11] Shen X, Liu G Q, Sun B, et al., "Impossible differentials of SPN ciphers," *INSCRYPT 2016*, 47-63, 2016. Article (CrossRef Link).

[12] Knudsen, L R, "DEAL-A 128-bit block cipher," *Technical Report*, 1998.

[13] Wu W L, Zhang W T, Feng D G, "Impossible differential cryptanalysis of reduced-round ARIA and Camellia," *Journal of Computer Science and Technology*, 22(3), 449-456, 2007. Article (CrossRef Link).

[14] Li S H, Song C Y, "Improved impossible differential cryptanalysis of ARIA," in *Proc. of 2008 International Conference on Information Security and Assurance-ISA 2008*, 129-132, 2008. Article (CrossRef Link).

[15] Li R L, Sun B, Zhang P, et al., "New impossible differential cryptanalysis of ARIA," *http://eprint.iacr.org/2010/307.pdf*, 2010. Article (CrossRef Link).

[16] Du C H, Chen J Z, "Impossible differential cryptanalysis of ARIA reduced to 7 rounds," in *Proc. of the 9th International Workshop on Cryptology and Network Security- CANS 2010*, 20-30, 2010. Article (CrossRef Link).
[17] Su C M, "New impossible differential attack on 7-round reduced ARIA," *Journal of Computer Applications*, 32(1), 45-48, 2012. Article (CrossRef Link).
[18] Xie G Q, Wei H R, "Impossible differential attack of block cipher ARIA," *Journal of Computer Reseach and Development*, 55(6), 1201-1210, 2018. Article (CrossRef Link).
[19] Lu J, Kim J, Keller N, et al., "Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1," *CT-RSA 2008*, 1592, 370-386, 2008. Article (CrossRef Link).

Xuan Shen received his PH.D. degree in College of Liberal Arts and Sciences from National University of Defense Technology, Changsha, Hunan, P. R. China, in December 2018. He is now a lecturer of College of Information and Communication from National University of Defense Technology. His current research interests include design and cryptanalysis of symmetric ciphers.

Jun He received his PH.D. degree in PLA University of Science and Technology, Nanjing, Jiangsu, P. R. China, in 2007. He is now a professor of College of Information and Communication from National University of Defense Technology. His current research interests include cryptography and network security.