New Impossible Differential Cryptanalysis of ARIA

Ruilin Li, Bing Sun, Peng Zhang and Chao Li

Department of Mathematics and System Sciences, Science College,
National University of Defense Technology,
Changsha, 410073, P.R.China,
securitylrl@gmail.com
{happy_come,cheetahzhp}@163.com
lichao_nudt@sina.com

Abstract. This paper studies the security of ARIA against impossible differential cryptanalysis. Firstly an algorithm is given to find many new 4-round impossible differentials of ARIA. Followed by such impossible differentials, we improve the previous impossible differential attack on 5/6-round ARIA. We also point out that the existence of such impossible differentials are due to the bad properties of the binary matrix employed in the diffusion layer.

Key Words: Block Cipher, Impossible Differential, ARIA

1 Introduction

ARIA[1] is a 128-bit block cipher designed by a group of Korean experts in 2003 which later was established as a Korean Standard by the Ministry of Commerce, Industry and Energy. ARIA supports key length of 128/192/256 bits, and the most interesting characteristic is its involution based on the special usage of neighbouring confusion layer and involutional diffusion layer[2].

The security of ARIA was initially analyzed by its designers, including differential cryptanalysis, linear cryptanalysis, truncated differential cryptanalysis, impossible differential cryptanalysis, higher order differential cryptanalysis, square attack and interpolation attack[1]. Later Alex Biryukov etc. performed an evaluation of ARIA, but they focused on truncated differential cryptanalysis and dedicated linear cryptanalysis[3]. Wu etc. firstly found a non-trivial 4-round impossible differential path which led to a 6-round attack of ARIA requiring about 2^{121} chosen plaintexts and about 2^{112} encryptions[4].

Impossible differential cryptanalysis, independently found by Knudsen[6] and Biham[7], uses one or more differentials with probability 0 called impossible differential. Unlike differential cryptanalysis[5] which recoveries the key through the obvious advantage of a high probability differential characteristic, impossible differential cryptanalysis is a sieving attack which excludes the candidate keys until only one key left using some impossible differential path. Since its emergence, impossible differential cryptanalysis has been applied to attack many well-known block ciphers such as AES[9–11], recently a newly designed block cipher CLEFIA[12–14] and so on.

Impossible differential is usually built in a miss-in-the-middle manner[8], i.e. given an input difference α, we can go forward with probabolity 1 to some difference γ, meanwhile from the output difference β, we can go backward with probability 1 to another difference δ, but then we get some contradictions between γ and δ, thus we get an impossible difference $\alpha \nrightarrow \beta$. In [7], some automated technique called *Shrinking* was introduced as an efficient algorithm to find impossible differential of a new block cipher, but such method relates to the structure of the block cipher at a large extent and doesn't focus too much on the detail of components in the round function.

In this paper we observe that due to some bad properties of the binary matrix used in the diffusion layer, we can find many new impossible differentials of ARIA, and the impossible differentials found in [4] are some special cases in ours. Based on such new impossible differentials and the *Early Abort Technique* introduced in [4, 5, 15], we mount an efficient attack on 5/6 reduced round of ARIA. Table 4 summaries our main cryptanalytic results compared with the previous impossible differential attack on ARIA.

The rest of the paper is organized as follows. In section 2 we briefly describe the block cipher ARIA. In section 3 we give some bad properties of the diffusion layer. In section 4, we present an algorithm to find many new 4-round impossible differential. Section 5 is our improved attack on the 5/6-reduced round ARIA. We concludes this paper in Section 6.

2 Preliminaries

2.1 Description of ARIA

ARIA is an SPN style block cipher, and the number of the rounds are 12/14/16 corresponding to key of 128/192/256 bit. In this paper the plaintext, as well as the input and output of the round function, the ciphertext are treated as 4×4 matrices over $GF(2^8)^{4\times 4}$ or a 16-byte vectors over $GF(2^8)^{16}$ and we call them states.

The round function of ARIA constitutes 3 basic operations: the Substitution Layer, the Diffusion Layer and the Round Key Addition. An N round ARIA firstly applies a Round Key Addition, then iterates the round function $N-1$ times, the last round is the same but excludes the diffusion layer. The whole structure is depicted in Fig. 1 and the 3 basic operations are as follows:

Round Key Addition(RKA): a 128-bit round key is simply XORed to the state. The round key is derived from the cipher key by means of the key schedule. For the detail of the key schedule, we refer to [1].

Substitution Layer(SL): a non-linear byte substitution operates on each byte of the state independently. In ARIA this is implemented by two S-boxes s_1 and s_2 defined by affine transformations of the inverse function over $GF(2^8)$.

Diffusion Layer(DL): a 16×16 involution binary matrix with branch number 8 was selected to improve the diffusion effect and increase efficiency in both hardware and software implementations.

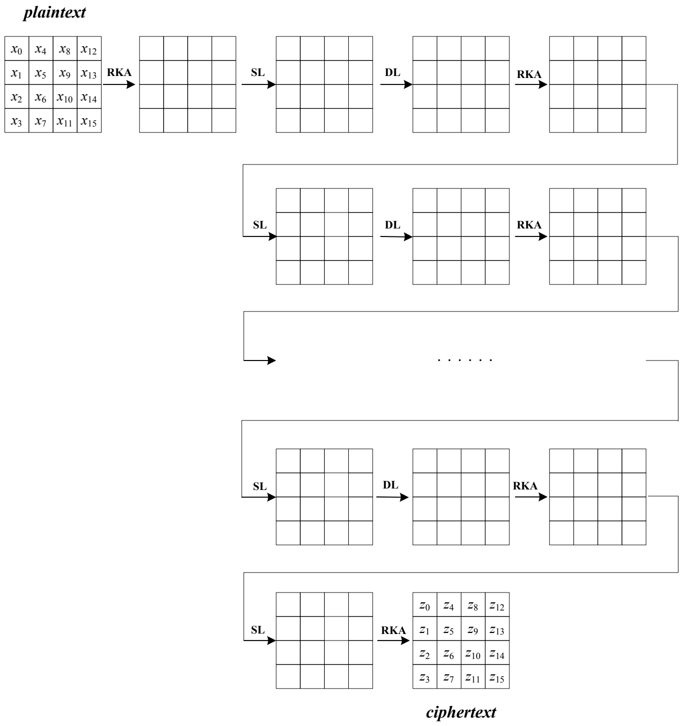


Fig. 1. Overall Structure of ARIA

2.2 Notions

In this paper, we will use the following notations:

P *or* P'	the 128-bit plaintext
C *or* C'	the 128-bit ciphertext
X	some 16-byte state denoted by $(x_0, \cdots, x_{15})$ where $x_i \in GF(2^8)$
ΔX	the XOR ($\oplus$) difference of X
$h(X)$	the number of non-zero byte in X
$X_i^I(X_i^O)$	the input (resp. output) of round i
$X_i^S(X_i^D)$	value after application of **SL**(resp. **DL**) of round i
$X_{i,j}^*$	the j-th byte of X_i^*, where $* \in \{I, O, S, D\}$

3 Some Observations On the Diffusion Layer of ARIA

In [2], the authors presented an excellent algorithm (implementation of A can be performed efficiently) to construct a binary matrix A satisfying the following conditions:

(1) the branch number of A is 8 which is the best when $A \in GF(2)^{16\times16}$;
(2) A is involution, i.e. $A^2 = I$, where I is identical transformation;
(3) resistance against truncated differential cryptanalysis;
(4) resistance against impossible differential cryptanalysis.

Such binary matrix A was later employed as the diffusion layer in ARIA. In this section, we will use X to denote the input to the **DL**, and Y to denote the output of the **DL**. Both X and Y can be treated as 16-byte vectors, then A can be seen as a linear map from $GF(2^8)^{16}$ to $GF(2^8)^{16}$, we denote such transformation by $Y = AX$ as follow.

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\,0\,1\,1\,0 \\ 0\,0\,1\,0\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0\,1 \\ 0\,1\,0\,0\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,0\,1 \\ 1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,0\,1\,1\,0 \\ 1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1 \\ 0\,1\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1 \\ 1\,0\,1\,0\,0\,0\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0 \\ 0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,0\,0 \\ 1\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,1 \\ 1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,0\,1\,1\,0\,1\,0\,0\,0\,0\,1\,0\,1 \\ 0\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0 \\ 0\,1\,1\,0\,0\,0\,1\,1\,0\,1\,0\,1\,1\,0\,0\,0 \\ 1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,0\,0 \\ 1\,0\,0\,1\,1\,1\,0\,0\,0\,1\,0\,1\,0\,0\,1\,0 \\ 0\,1\,1\,0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1 \end{pmatrix} \times \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}$$

Let $\Lambda_i = \{t | 0 \le t \le 15, A_{i,t} = 1\} (0 \le i \le 15)$. It is obviously that Λ_i is a good description of the dependency between output y_i and the input byte positions of X. After pondering such Λ_i's in table 1 thoroughly, we can get the following propositions:

Proposition 1. *Let A be defined as above, then, for any $0 \le i \ne j \le 15$, there exits $\mathcal{E}^{(i,j)} \subset GF(2^8)^{16}$ such that for any $X \in \mathcal{E}^{(i,j)}$, $y_i = 0$ and $y_j \ne 0$.*

Proof. From table 1, for any $0 \le i \ne j \le 15$, $\Lambda_{ij} \triangleq \Lambda_j - \Lambda_i \ne \emptyset$. Chose an arbitrary element of Λ_{ij}, say k, then for $l = 0, 1, \cdots 15$, let

$$x_l = \begin{cases} \alpha & \text{if } l = k, \text{where } 0 \ne \alpha \in GF(2^8) \\ 0 & \text{if } l \in \Lambda_i \cup \Lambda_j, l \ne k \\ \beta & \text{others, where } \beta \in GF(2^8)\ . \end{cases}$$

Table 1. The dependency between output y_i and input byte positions of X

Λ_0	{3,4,6,8,9,13,14}	Λ_8	{0,1,4,7,10,13,15}
Λ_1	{2,5,7,8,9,12,15}	Λ_9	{0,1,5,6,11,12,14}
Λ_2	{1,4,6,10,11,12,15}	Λ_{10}	{2,3,5,6,8,13,15}
Λ_3	{0,5,7,10,11,13,14}	Λ_{11}	{2,3,4,7,9,12,14}
Λ_4	{0,2,5,8,11,14,15}	Λ_{12}	{1,2,6,7,9,11,12}
Λ_5	{1,3,4,9,10,14,15}	Λ_{13}	{0,3,6,7,8,10,13}
Λ_6	{0,2,7,9,10,12,13}	Λ_{14}	{0,3,4,5,9,11,14}
Λ_7	{1,3,6,8,11,12,13}	Λ_{15}	{1,2,4,5,8,10,15}

and let

$$\mathcal{E}_k^{(i,j)} = \{X | X = (x_0, \cdots, x_{15})\},$$

then, $\mathcal{E}^{(i,j)} = \bigcup_{k \in \Lambda_{ij}} \mathcal{E}_k^{(i,j)}$ satisfies all the conditions in Proposition 1. □

Proposition 2. *For 2 consecutive rounds of ARIA, there exits* $\mathcal{D} \triangleq \{(r, s, u, v) | 0 \le r, s, u, v \le 15, r < s, u < v\}$*, such that for any* $(r, s, u, v) \in \mathcal{D}$*,*

$$(\Delta X_{i,r}^I, \Delta X_{i,s}^I) \neq (0, 0); \quad \Delta X_{i,l}^I = 0, \text{ while } l \neq r, s;$$

and

$$\Delta X_{i+1,u}^O = \Delta X_{i+1,v}^O.$$

Proof. The existence of $\mathcal{D}$ can be verified by algorithm 1 and the searched results are listed in table 2. We only give the proof when $(r, s, u, v) = (0, 5, 11, 14)$ as depicted in Fig 2, other cases are similar.

Algorithm 1: Finding the Set $\mathcal{D}$
for $u = 0$ to 15
  for $v = u + 1$ to 15
    Set T:=$\Lambda_u \cup \Lambda_v - \Lambda_u \cap \Lambda_v$
    Let $\Gamma_{u,v} := \{0, \cdots, 15\} - \bigcup_{k \in T} \Lambda_k$
    print $\{\Gamma_{u,v}, u, v\}$
  end for
end for

Results of Algorithm 1 show that for any $0 \le u < v \le 15$, $|\Gamma_{u,v}|$=0 or 2.

Suppose that the input difference of round i is $\Delta X_i^I = (a_0, 0, 0, 0, 0, a_5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ as depicted in Fig 2, where $(a_0, a_5) \neq (0, 0)$. Such difference propagates in round i as follows:

After **SL**: $\Delta X_i^S = (b_0, 0, 0, 0, 0, b_5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.
After **DL**: $\Delta X_i^D = (0, c_1, 0, c_3, c_4, 0, c_6, 0, c_8, c_9, c_{10}, 0, 0, c_{13}, c_{14}, c_{15})$.
After **RKA**: $\Delta X_i^O = (0, c_1, 0, c_3, c_4, 0, c_6, 0, c_8, c_9, c_{10}, 0, 0, c_{13}, c_{14}, c_{15})$.

Since the output difference of round i is equal to the input difference of round $i+1$, we have $\Delta X^I_{i+1} = (0, c_1, 0, c_3, c_4, 0, c_6, 0, c_8, c_9, c_{10}, 0, 0, c_{13}, c_{14}, c_{15})$, then such difference propagates in round $i+1$ as follows:

After **SL**: $\Delta X^S_{i+1} = (0, d_1, 0, d_3, d_4, 0, d_6, 0, d_8, d_9, d_{10}, 0, 0, d_{13}, d_{14}, d_{15})$.
After **DL**: $\Delta X^D_{i+1} = (e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}, e_{13} e_{14}, e_{15})$.
After **RKA**: $\Delta X^O_{i+1} = (e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}, e_{13}, e_{14}, e_{15})$.

Through the binary matrix A, we can express e_{11} and e_{14} as follows:

$$e_{11} = d_3 \oplus d_4 \oplus d_9 \oplus d_{14}$$
$$e_{14} = d_3 \oplus d_4 \oplus d_9 \oplus d_{14}$$

thus $e_{11} = e_{14}$, which means that $\Delta X^O_{i+1,11} = \Delta X^O_{i+1,14}$. □

Table 2. $\mathcal{D}$ Searched By Algorithm 1

(r,s,u,v)	(r,s,u,v)	(r,s,u,v)	(r,s,u,v)
(0,5,11,14)	(2,5,8,15)	(4,9,3,14)	(7,9,2,12)
(0,7,10,13)	(2,7,9,12)	(4,10,1,15)	(7,10,0,13)
(0,10,7,13)	(2,8,5,15)	(4,14,3,9)	(7,12,2,9)
(0,11,5,14)	(2,9,7,12)	(4,15,1,10)	(7,13,0,10)
(0,13,7,10)	(2,12,7,9)	(5,8,2,15)	(8,13,3,6)
(0,14,5,11)	(2,15,5,8)	(5,11,0,14)	(8,15,2,5)
(1,4,10,15)	(3,4,9,14)	(5,14,0,11)	(9,12,2,7)
(1,6,11,12)	(3,6,8,13)	(5,15,2,8)	(9,14,3,4)
(1,10,4,15)	(3,8,6,13)	(6,8,3,13)	(10,13,0,7)
(1,11,6,12)	(3,9,4,14)	(6,11,1,12)	(10,15,1,4)
(1,12,6,11)	(3,13,6,8)	(6,12,1,11)	(11,12,1,6)
(1,15,4,10)	(3,14,4,9)	(6,13,3,8)	(11,14,0,5)

Proposition 2 shows that in ARIA there exits input difference of which 1 or 2 bytes can have nonzero difference, after applying 2 consecutive rounds, some 2 bytes of output difference are identical. This fact is useful to find new 4-round impossible differentials as depicted in section 4.

4 New 4-Round Impossible Differentials

In this section, we present an algorithm to find many new 4-round impossible differentials of ARIA.

Algorithm 2: Finding 4-Round Impossible Differentials of ARIA

Choose an element $(r, s, u, v) \in \mathcal{D}$
Construct $\mathcal{E}^{(u,v)}$ and $\mathcal{E}^{(v,u)}$
Let $\Delta X_i^I = (0, \cdots, 0, a_r, 0, \cdots, 0, a_s, 0, \cdots, 0)$, where $(a_r, a_s) \neq (0, 0)$
Let $\Delta X_{i+3}^S \in \mathcal{E}^{(u,v)} \cup \mathcal{E}^{(v,u)}$
Output:$(\Delta X_i^I, \Delta X_{i+3}^O)$, where $\Delta X_{i+3}^O = A \cdot \Delta X_{i+3}^S$.

The impossible differentials found by Algorithm 2 are explained as follows: Since $(r, s, u, v) \in \mathcal{D}$ and $\Delta X_i^I = (0, \cdots, 0, a_r, 0, \cdots, 0, a_s, 0, \cdots, 0)$, from proposition 2 we know that

$$\Delta X_{i+1,u}^O = \Delta X_{i+1,v}^O. \tag{1}$$

Meanwhile, if

$$\Delta X_{i+3}^S \in \mathcal{E}^{(u,v)} \cup \mathcal{E}^{(v,u)}, \tag{2}$$

then

$$\Delta X_{i+3}^I \in \mathcal{E}^{(u,v)} \cup \mathcal{E}^{(v,u)}, \tag{3}$$

Note that

$$\Delta X_{i+2}^S = A^{-1} \cdot \Delta X_{i+2}^D \text{ and } \Delta X_{i+2}^D = \Delta X_{i+2}^O = \Delta X_{i+3}^I, \tag{4}$$

and since A is involutional, from (3)(4) we get

$$X_{i+2}^S = A \cdot \Delta X_{i+2}^D \text{ and } \Delta X_{i+2}^D \in \mathcal{E}^{(u,v)} \cup \mathcal{E}^{(v,u)}. \tag{5}$$

According to proposition 1 and (5) we have

$$\begin{cases} \Delta X_{i+2,u}^S = 0 \\ \Delta X_{i+2,v}^S \neq 0 \end{cases} \quad \text{or} \quad \begin{cases} \Delta X_{i+2,u}^S \neq 0 \\ \Delta X_{i+2,v}^S = 0 \end{cases}$$

which implies that

$$\Delta X_{i+2,u}^S \neq \Delta X_{i+2,v}^S,$$

thus

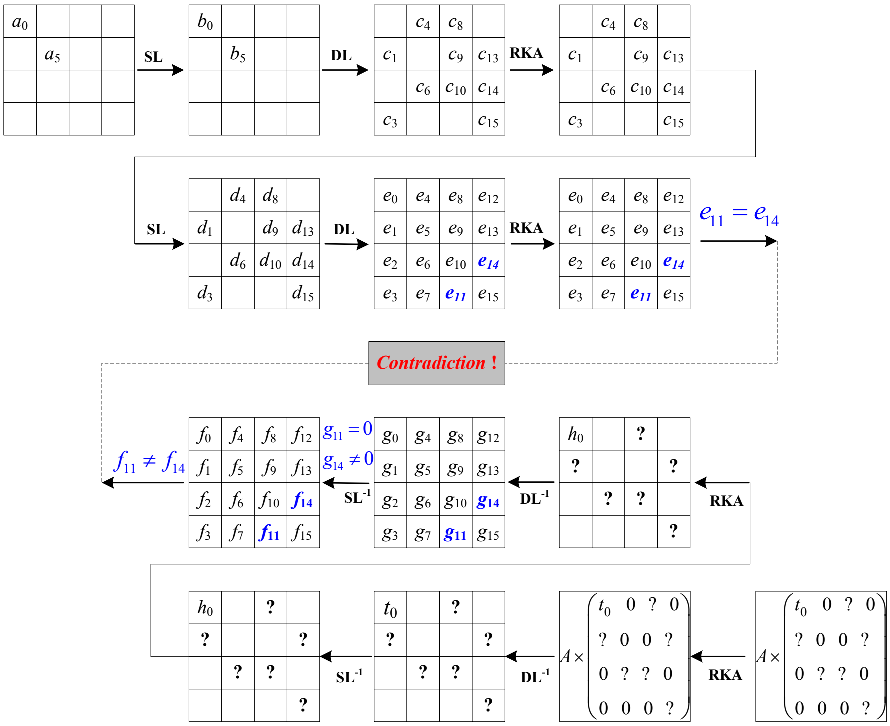
$$\Delta X_{i+2,u}^I \neq \Delta X_{i+2,v}^I.$$

which is contradicted with (1), so these differentials are impossible.

One kind of the above impossible differentials are depicted in Fig 2. Note that these impossible differentials are based on $(0, 5, 11, 14) \in \mathcal{D}$, but they don't use the whole set $\mathcal{E}^{(11,14)} \cup \mathcal{E}^{(14,11)}$ (only use the set $\mathcal{E}_0^{(11,14)}$ as constructed in the proof of Proposition 1).

As shown in Fig.2, the input difference of round i can only have 1 or 2 non-zero bytes, i.e. $h(\Delta X_i^I) = 1$ or 2, but the output difference of round $i + 3$, i.e. ΔX_{i+3}^O, can have many situations depending on the combinations of question mark(?) in ΔX_{i+3}^S. Since

$$\Delta X_{i+3}^S = (t, ?, ?, ?, 0, 0, ?, 0, ?, 0, ?, 0, 0, ?, 0, ?),$$



$(a_0, a_5) \neq (0,0)$ $t_0 \neq 0$? *arbitrary* □ 0

Fig. 2. New 4-Round Impossible Differential

if now ? is confined to $\{0, t\}$, some concrete output difference after the **DL** can be given. In fact, there will be $2^6 = 64$ total output differences and $4 \leq h(\Delta X_{i+3}^O) \leq 13$. Table 3 lists 6 of them satisfying $h(\Delta X_{i+3}^O) = 4, 5$, where the first 2 correspond to the output difference of our chosen impossible differential as ID-I, ID-II, ID-III, ID-IV in Fig. 3, the next 4 denote the output difference of the impossible differential in Ref. [4].

Table 3. Some Concrete ΔX_{i+3}^O while ? is confined to $\{0, t\}$

ΔX_{i+3}^S	$h(\Delta X_{i+3}^S)$	ΔX_{i+3}^O	$h(\Delta X_{i+3}^O)$
$t00000t0t0t00000$	4	$0t000t000000t0t0$	4
$tt00000000000t0t$	4	$tt0000000000t0t0$	4
$t000000000t0000t$	3	$0t000000ttt000t0$	5
$t0000000t0000t00$	3	$0t0000000t000ttt$	5
$t00000t000000t00$	3	$00t0t0000000ttt0$	5
$tt00000000t00000$	3	$0000t00tt000t0t0$	5

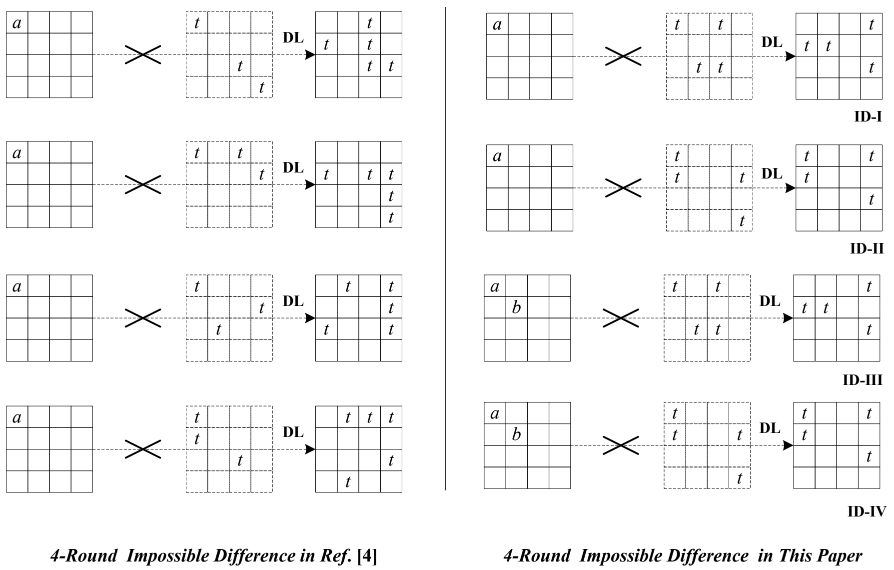


Fig. 3. Comparision of 4 Round Impossible Differential of ARIA

5 Impossible Differential Attack on Reduced Round ARIA

In this section, we improve all the previous impossible differential cryptanalysis of ARIA reduced to six rounds. The 6 round attack is based on the new four round impossible differential with additional one round at each of the beginning and the end. We only give our improved attack based on ID-III as in Fig 4, others are similar and the results are summarized in table 4.

The procedure is as follow:

1. A structure is defined as a set of plaintexts which have certain fixed values in all but the ten bytes(1,3,4,6,8,9,10,13,14,15). One such structure consists of 2^{80} plaintexts and proposes $2^{80} \times (2^{80}-1) \times \frac{1}{2} \approx 2^{159}$ pairs of plaintexts.
2. Take 2^{32} structures(2^{112} plaintexts, 2^{191} plaintext pairs). Choose pairs whose ciphertext pairs have zero difference at the twelve bytes (0,2,3,4,6,7,8,9,10,11, 13,15). The expected number of such pairs is $2^{191} \times 2^{-96} = 2^{95}$.
3. Assuming a 32-bit value k_7 at the four byte(1,5,12,14), repeat Step 4 and Step 5.
4. For every remaining ciphertext pair(C, C^*) from Step 2, compute $C_5 = SL^{-1}(C \oplus k_6)$, $C_5^* = SL^{-1}(C^* \oplus k_6)$ and choose pairs whose difference $C \oplus C^*$ are the same at the four bytes(1,5,12,14). The probability is about $(2^{-8})^3 = 2^{-24}$, thus the expected number of the remaining pairs is about $2^{95} \times 2^{-24} = 2^{71}$.
5. For every remaining ciphertext pair(C, C^*) from Step 4, considering the corresponding plaintext pair (P, P^*), guess ten bytes of the key k_1 at (1,3,4,6,8,9, 10,13,14,15), calculate $SL(P \oplus k_1) \oplus SL(P^* \oplus k_1)$ and check whether such difference satisfy the conditions at (1,10,15)(6,8,13),(3,4,9,14) as depicted in Fig 4. The probability is $(2^{-8})^2 \times (2^{-8})^2 \times (2^{-8})^4 = 2^{-64}$.
6. Since such a difference is impossible, every key that proposes such a difference is wrong key. After analyzing 2^{71} ciphertext pairs, there remain only about $2^{80}(1-2^{-64})^{2^{71}} \approx 2^{-104}$ wrong values of the ten bytes of k_1.
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 ten bytes of k_1 for each 32-bit value of k_7 since the wrong key value (k_1, k_7) remains with probability $\sum_{j,j \text{ is a wrong key}} 2^{-104} = (2^{32}-1) \times (2^{-104}) \approx 2^{-72}$. Hence if there remains a value of k_1, we can assume that value of k_7 is right.

The time complexity of the above attack is calculated as follow: the naive approach as in [10, 11] will require about $2 \times 2^{32} \times 2^{95} + 2^{32} \times 2 \times 2^{80} \times \{1 + (1 - 2^{-64}) + (1-2^{-64})^2 + \cdots + (1-2^{-64})^{2^{71}}\}$ one round operations, thus the time is longer than exhaustive search. To avoid this, we use the *Early Abort Technology* method [4, 5, 15], i.e. at Step 4 we don't guess the whole four byte of k_7 each time for discarding unuseful pairs, instead we first guess $k_{7,1}$ and $k_{7,5}$ to discard $2^{95}(1-2^{-8})$ pairs, then add another guessing key byte $k_{7,12}$ for further filtering, thus discard $2^{87}(1-2^{-8})$ pairs, then guess $k_{7,15}$ to discard $2^{79}(1-2^{-8})$ pairs.

At last, about $2^{95} - 2^{95}(1 - 2^{-8}) - 2^{87}(1 - 2^{-8}) - 2^{79}(1 - 2^{-8}) = 2^{71}$ pairs are left for the next step. The same procedure can also be performed at Step 5. So the time complexity can be calculated as follow:

1. Step 4 requires about $2^{16} \times 2 \times 2^{95} + 2^{24} \times 2 \times 2^{87} + 2^{32} \times 2 \times 2^{79} = 3 \times 2^{112}$ one round operations.
2. Step 5 requires about $2^{32} \times (2^{16} \times 2 \times 2^{71} + 2^{24} \times 2 \times 2^{63} + 2^{32} \times 2 \times 2^{55} + \cdots + 2^{80} \times 2 \times 2^{7}) = 9 \times 2^{120}$ one round operations.

Choose another impossible differential, we can derive other key bytes of k_7 and k_1, so the total time complexity is about $2^{121.6}$ encryptions of ARIA reduced to 6 rounds.

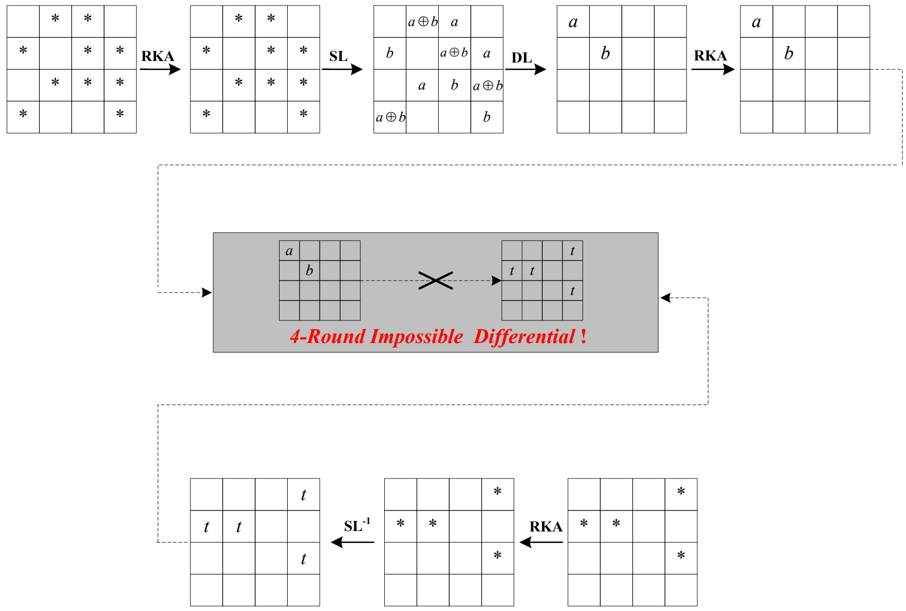


Fig. 4. 6-Round Impossible Differential Attack Based On ID-III

For the attack of 5 round ARIA, the following 4 round impossible differential is chosen:

$$(*, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) \nrightarrow (*, *, 0, 0, 0, 0, *, 0, *, 0, *, 0, 0, *, 0, *),$$

where * denotes non-zero byte. Note that such 4-round impossible differential is from round 2 to round 5 and round 5 doesn't contain the diffusion layer. The data and time complexity are $2^{71.3}$ and $2^{71.6}$ respectively.

6 Conclusion

This paper study the impossible differential property of ARIA. We firstly point out many bad properties of the binary matrix in the diffusion layer, then we present an algorithm to find many new 4-round impossible differentials. For the attack of 5 round ARIA, the data complexity is $2^{71.3}$ and the time complexity is $2^{71.6}$. For the 6-round ARIA, we mount 2 kinds of impossible differential attack. One is for reducing the time complexity and the corresponding data (resp. time) complexity is $2^{120.5}$(reps. $2^{104.5}$). The other is for reducing the data complexity and the corresponding data (resp. time) complexity is 2^{113}(resp. $2^{121.6}$). Table 4 summaries our main cryptanalytic results of ARIA.

Even if we can improve the previous impossible differential attack of reduced round ARIA, our new impossible differential could't lead to a successful attack on more than 6 rounds now. The main handicap is the absence of enough pairs for filtering wrong keys. Further research should be focused on more than 4 round properties of ARIA, eg. it is very interesting to find some new impossible differential other than ours in this paper and some new cryptanalysis technology combined with the key schedule is welcome for attacking more rounds of ARIA.

Table 4. Summary of Impossible Differential Attacks on Reduced ARIA

Round Number	Data	Time	Paper	Weight of ID
5	$2^{71.3}$	$2^{71.6}$	ID in this paper	(1,7)
6	2^{121}	2^{112}	Ref.[4]	(1,5)
6	$2^{120.5}$	$2^{104.5}$	ID-I in this paper	(1,4)
6	2^{113}	$2^{121.6}$	ID-III in this paper	(2,4)

Acknowledgments

The work in this paper is supported by the Natural Science Foundation of China. (No:60573028)

References

1. Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung etc. New Block Cipher: ARIA. In J.I.Lim and D.H.Lee(Eds.), ICISC 2003, LNCS 2971, pp.432-445, 2004.
2. Bon Wook Koo, Hwan Seok Jang, and Jung Hwan Song, Constructing and Cryptanalysis of a 16×16 Binary Matrix as a Diffusion Layer. In K. Chae and M. Yung (Eds.): WISA 2003, LNCS 2908, pp.489-503, 2004.
3. Alex Biryukov, Christophe De Canniere, Joseph Lano, Siddika Berna Ors and Bart Preneel. Security and Performance Analysis of Aria. Version 1.2. Jan 7, 2004.

4. Wenling Wu, Wentao Zhang and Dengguo Feng. Impossible differential cryptanalysis of ARIA and Camellia. In Journal of Compute Science and Technology, 2007.
5. Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, Vol 3, pp.3-72, 1991.
6. Lars R. Knudsen. DEAL—A 128-bit Block Cipher. Technical Report 151, Department of Informatics, University of Bergen, Bergen, Norway, Feb. 1998.
7. E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. Advances in Cryptology-EUROCRYPT'99, LNCS 2595, pp.12-23, Springer-Verlag 1999.
8. Eli Biham, Alex Biryukov and Adi Shamir. Miss in the Middle Attacks on IDEA and Khufu. FSE'99, LNCS 1636, pp. 124-138, Springer-Verlag 1999.
9. E. Biham and N. Keller. Cryptanalysis of Reduced Variants of Rijndael. 3rd AES Conference, 2000.
10. Jung Hee Cheon, Munju Kim, Kwangjo Kim, et al. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton. International Conference on Information Security and Cryptology-ICISC'01, LNCS 2288, pp.39-49, Springer-Verlag 2002.
11. Raphael Chung-Wei Phan. Impossible Differential Cryptanalysis of 7-round AES. Information Processing Letters, Vol.91, Number 1, pp.33-38, Elsevier, 2004.
12. Wei Wang and Xiaoyun Wang. Improved Impossible differential cryptanalysis of CLEFIA. Avaiable through: http://www.eprint/2007/466.pdf
13. Y. Tsunoo, E. Tsujihara, M. Shigeri, T. Saito, T. Suzaki, and H. Kubo. Impossible Differential Cryptanalysis of CLEFIA. To be appeared in FSE2008.
14. Bing Sun, Ruilin Li, Mian Wang, Ping Li and Chao Li. Impossible Differential Cryptanalysis of CLEFIA. Avaiable through: http://www.eprint/2008/151.pdf.
15. Jiqiang Lv, Jongsung Kim, Nathan Keller and Orr Dunkelman. Improving the efficiency of impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. CT-RSA 2008, LNCS 4904, pp. 370-386, 2008.