Linear Cryptanalysis of ARIA Block Cipher

Zhiqiang Liu[1], Dawu Gu[1], Ya Liu[1], Juanru Li[1], and Wei Li[2,3]

[1] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
{ilu_zq,dwgu,liuya0611,jarod}@sjtu.edu.cn
[2] School of Computer Science and Technology,
Donghua University, Shanghai 201620, China
liwei.cs.cn@gmail.com
[3] Shanghai Key Laboratory of Integrate Administration Technologies
for Information Security, Shanghai 200240, China

Abstract. In this paper, we firstly present an approach to derive a kind of special linear characteristics for byte-oriented SPN block ciphers. Then based on this approach, we study the security of the block cipher ARIA against linear cryptanalysis and propose an attack on 7-round ARIA with 128/192/256-bit key size, an attack on 9-round ARIA with 192/256-bit key size as well as an attack on 11-round ARIA with 256-bit key size. The designers of ARIA expect that there isn't any effective attack on 8 or more rounds of ARIA with 128/192/256-bit key size by means of linear cryptanalysis. However, our work shows that such attacks do exist. Moreover, our cryptanalytic results are the best known cryptanalytic results of ARIA so far.

Keywords: Cryptanalysis, Linear cryptanalysis, Block cipher, ARIA.

1 Introduction

The block cipher ARIA [1,2] was presented at ICISC 2003 by a group of Korean experts, and it was later selected as a data encryption standard by the Korean Ministry of Commerce, Industry and Energy. As an involutional SPN structure block cipher, ARIA supports the block size of 128 bits and a variable key size of 128/192/256 bits. The number of rounds adopted in ARIA depends on the key size and 12/14/16 rounds will be used in ARIA v1.0 (the latest version of ARIA) with 128/192/256-bit key size respectively.

Up to now, the security of ARIA has already been analyzed by many cryptographists. In [1], the designers Kwon et al evaluated the security of ARIA by using the cryptanalytic methods such as differential cryptanalysis [3], linear cryptanalysis [4], truncated differential cryptanalysis [5], impossible differential cryptanalysis [6], integral cryptanalysis [7], and so on. In [8], Wu et al firstly found some 4-round impossible differential characteristics of ARIA which could lead to effective attacks on 6-round ARIA with 128/192/256-bit key size, and the cryptanalytic result was later improved by Li et al [9] and Du et al [10] respectively. In [11], Li et al presented some 3-round integral distinguishers of

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 242–254, 2011.

ARIA which could be used to attack 4/5/6-round ARIA with 128/192/256-bit key size, then based on this work, Li et al [12] demonstrated an integral attack on 7-round ARIA with 256-bit key size. In [13], Fleischmann et al proposed some attacks on 5/6-round ARIA with 128/192/256-bit key size and 7-round ARIA with 256-bit key size by means of boomerang attack [14]. In [15], Tang et al introduced some attacks on 5/6-round ARIA with 128/192/256-bit key size, 7-round ARIA with 192/256-bit key size and 8-round ARIA with 256-bit key size via meet-in-the-middle attack [16].

In this paper, we firstly present an approach to derive a kind of special linear characteristics for byte-oriented SPN block ciphers. Then according to this approach, we investigate the security of ARIA against linear cryptanalysis and propose an attack on 7-round ARIA with 128/192/256-bit key size, an attack on 9-round ARIA with 192/256-bit key size as well as an attack on 11-round ARIA with 256-bit key size. As a matter of fact, the designers of ARIA expect that there isn't any effective attack on 8 or more rounds of ARIA with 128/192/256-bit key size by means of linear cryptanalysis. However, our work shows that such attacks do exist. Furthermore, our cryptanalytic results are the best known cryptanalytic results of ARIA so far.

The remainder of this paper is organized as follows. Section 2 introduces the notations used throughout this paper, gives a brief description of ARIA as well as the method of linear cryptanalysis. Section 3 presents a kind of special linear characteristics for byte-oriented SPN block ciphers. Section 4 proposes several special 4-round linear characteristics of ARIA and demonstrates our attacks on reduced-round ARIA based on such linear characteristics. Finally, Section 5 summarizes the paper.

2 Preliminaries

The following notations are used throughout the paper.

- $\oplus$ denotes bitwise exclusive OR (XOR).
- $\bullet$ denotes bitwise inner product.
- $|x|$ denotes absolute value of a real number x.
- $\circ$ denotes the composition operation.
- $\#S$ denotes the cardinality of a set S.
- 0x denotes the hexadecimal notation.
- $\|$ denotes the concatenation operation.
- For a real number x, $\lceil x \rceil$ denotes the integer such that $x \leq \lceil x \rceil < x + 1$.

2.1 Description of ARIA

ARIA is a 128-bit block cipher with an involutional SPN structure. It accepts keys of 128, 192 or 256 bits and the number of rounds is 12, 14 or 16 respectively. The input and output of each round of ARIA are treated as 16-byte vectors, and each byte within the vectors could be regarded as an element in $GF(2^8)$.

The round function of ARIA applies following three basic operations subsequently:

Round Key Addition (RKA): This is done by XORing the 128-bit round key. All round keys are derived from the master key by means of the key schedule.

Substitution Layer (SL): Apply 16 non-linear 8×8-bit S-boxes to the 16 bytes of the intermediate 16-byte vector respectively. ARIA adopts four distinct S-boxes, i.e., S_1, S_2 and their inverses S_1^{-1}, S_2^{-1}. In addition, ARIA has two types of substitution layers as shown in Fig. 1, where type 1 is used in the odd rounds and type 2 is used in the even rounds.

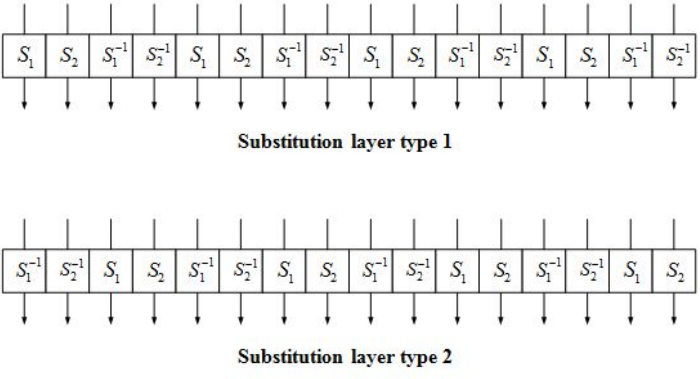

Fig. 1. The two types of substitution layers in ARIA

Diffusion Layer (DL): An involutional linear transformation $P : GF(2^8)^{16} \rightarrow GF(2^8)^{16}$ is performed on the intermediate 16-byte vector. The transformation P is defined as

$$(x_0, x_1, \ldots, x_{15}) \rightarrow (y_0, y_1, \ldots, y_{15}),$$

where

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

Note that in the last round of ARIA, the DL operation is replaced by an additional RKA operation. Please refer to [2] for detailed information about the S-boxes S_1, S_2, S_1^{-1}, S_2^{-1} and the key schedule algorithm.

2.2 Linear Cryptanalysis

Linear cryptanalysis [4] analyzes a block cipher E by investigating a correlation between the inputs and outputs of E and then obtains a linear approximation (also called linear characteristic and denoted as $\Gamma_P \rightarrow \Gamma_C$) of E with following type:

$$\Gamma_P \bullet P \oplus \Gamma_C \bullet C = \Gamma_K \bullet K, \tag{1}$$

where P, C and K denote plaintext, ciphertext and master key of E respectively, Γ_P, Γ_C and Γ_K stand for the masks of P, C and K respectively.

If equation (1) holds with probability $p \neq 1/2$, we call it an effective linear approximation of the block cipher E, and the linear approximation can be used to distinguish E from a random permutation since equation (1) holds with probability $1/2$ for a random permutation. Let $\varepsilon = p - 1/2$ be the bias of the linear approximation given in equation (1), then the greater $|\varepsilon|$ is, the more effective the linear approximation will be. Moreover, based on the above linear approximation, an adversary can mount a key recovery attack on $E' = E_1 \circ E$ by means of guessing part of round keys used in E_1, where E_1 represents the last few rounds of the cipher E'. Following the technique introduced in [4], the number of plaintext-ciphertext pairs required in the key recovery attack can be estimated as $c_N \times \frac{1}{\varepsilon^2}$, where the coefficient c_N, which is closely related to the number of guessed round key bits and the desired success rate of the attack, can be measured by using the approach given in [17].

3 A Kind of Special Linear Characteristics for Byte-Oriented SPN Block Ciphers

Let E be an n-round byte-oriented SPN block cipher with m-byte block size. Let I^i, O^i, K^i be the input, output and round key of the i-th ($1 \leq i \leq n$) round of E respectively. Let X^i, Y^i be the input and output of the substitution layer of the i-th round respectively. Then I^i, O^i, K^i, X^i and Y^i can be treated as m-byte vectors. The round function of the i-th round of E is depicted in Fig. 2,

where the round key addition is done by XORing K^i, S_j^i ($1 \leq j \leq m$) is a non-linear byte permutation which operates on the j-th byte of X^i, and the diffusion layer is essentially a linear transformation $P : GF(2^8)^m \rightarrow GF(2^8)^m$ which is performed on Y^i.

Let $(a_1, a_2, \ldots, a_m)$, $(b_1, b_2, \ldots, b_m) \in GF(2^8)^m$ be the input and output of the diffusion layer respectively. We firstly find that if there is subscript set Λ such that

$$\oplus_{\lambda \in \Lambda} a_\lambda = \oplus_{\lambda \in \Lambda} b_\lambda,$$

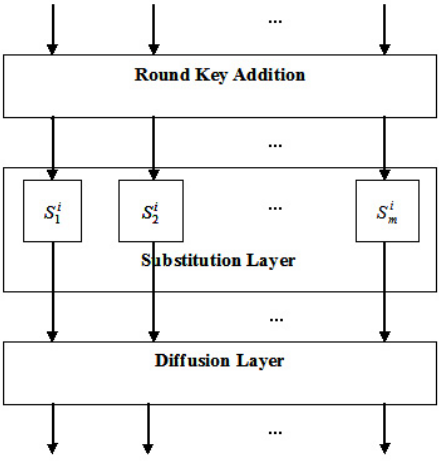

Fig. 2. The round function of the i-th round of E

special linear characteristics for t $(2 \leq t < n)$ consecutive rounds of E can be constructed as below (without loss of generality, linear characteristics for the first t rounds of E will be derived):

Step 1. For the first round of E, investigate the linear distribution tables of the S-boxes $\{S^1_\lambda\}_{\lambda \in \Lambda}$ and find all possible linear characteristics with the following form:

$$\oplus_{\lambda \in \Lambda}(\Gamma X^1_\lambda \bullet X^1_\lambda \oplus \Gamma Y^1_\lambda \bullet Y^1_\lambda) = 0,$$

where X^1_λ, Y^1_λ are the input and output of S^1_λ respectively, ΓX^1_λ, ΓY^1_λ are the masks of X^1_λ and Y^1_λ respectively, ΓY^1_λ keeps constant for any $\lambda \in \Lambda$ and is denoted as ΓY^1. Then extend the above linear characteristics for the S-boxes $\{S^1_\lambda\}_{\lambda \in \Lambda}$ to the linear approximations of the first round described as follows:

$$\oplus_{\lambda \in \Lambda}(\Gamma X^1_\lambda \bullet I^1_\lambda \oplus \Gamma Y^1 \bullet O^1_\lambda) = \oplus_{\lambda \in \Lambda}(\Gamma X^1_\lambda \bullet K^1_\lambda),$$

where I^1_λ, O^1_λ, K^1_λ are the λ-th bytes of I^1, O^1 and K^1 respectively.

Step 2. For the i-th $(2 \leq i \leq t)$ round of E, study the the linear distribution tables of the S-boxes $\{S^i_\lambda\}_{\lambda \in \Lambda}$ and get all possible linear characteristics with the following form:

$$\oplus_{\lambda \in \Lambda}(\Gamma X^i_\lambda \bullet X^i_\lambda \oplus \Gamma Y^i_\lambda \bullet Y^i_\lambda) = 0,$$

where X^i_λ, Y^i_λ are the input and output of S^i_λ respectively, ΓX^i_λ, ΓY^i_λ are the masks of X^i_λ and Y^i_λ respectively, ΓX^i_λ is the same for any $\lambda \in \Lambda$ and is denoted as ΓX^i, ΓY^i_λ remains unchanged for any $\lambda \in \Lambda$ and is denoted as ΓY^i. Then

based on the above linear characteristics for the S-boxes $\{S_\lambda^i\}_{\lambda\in\Lambda}$, generate the linear approximations of the i-th round as shown below:

$$\oplus_{\lambda\in\Lambda}(\Gamma X^i \bullet I_\lambda^i \oplus \Gamma Y^i \bullet O_\lambda^i) = \oplus_{\lambda\in\Lambda}(\Gamma X^i \bullet K_\lambda^i),$$

where I_λ^i, O_λ^i, K_λ^i are the λ-th bytes of I^i, O^i and K^i respectively.

Step 3. Denote the first t rounds of E as E_t. Obtain linear characteristics of E_t with the following form by concatenating t linear approximations on each round of E_t respectively which satisfy $\Gamma Y^{i-1} = \Gamma X^i$ $(2 \le i \le t)$:

$$\begin{aligned} &\oplus_{\lambda\in\Lambda}(\Gamma X_\lambda^1 \bullet I_\lambda^1 \oplus \Gamma Y^t \bullet O_\lambda^t) \\ &= \oplus_{\lambda\in\Lambda}(\Gamma X_\lambda^1 \bullet K_\lambda^1) \oplus_{i=2}^t \oplus_{\lambda\in\Lambda}(\Gamma X^i \bullet K_\lambda^i). \end{aligned} \tag{2}$$

Let E_s denote the first s $(t < s \le n)$ rounds of E. With the help of the linear characteristic for E_t given in equation (2), an adversary can mount an effective key recovery attack on E_s. Note that the smaller $\#\Lambda$ is, the more effective the above linear characteristic will be. We will demonstrate the effectiveness of such kind of linear characteristics by proposing some attacks on reduced-round ARIA in Section 4.

4 Attacking Reduced-Round ARIA

In this section, we firstly present some special 4-round linear characteristics of ARIA by using the approach mentioned in Section 3. Then based on the 4-round linear characteristics, we mount an attack on 7-round ARIA with 128/192/256-bit key size, an attack on 9-round ARIA with 192/256-bit key size as well as an attack on 11-round ARIA with 256-bit key size.

Let I^i, O^i, K^i be the input, output and round key of the i-th $(1 \le i \le n$, where n depends on the key size) round of ARIA respectively. Let X^i, Y^i be the input and output of the substitution layer of the i-th round respectively. Let I_j^i, O_j^i, K_j^i, X_j^i, Y_j^i denote the $(j+1)$-th $(0 \le j \le 15)$ bytes of I^i, O^i, K^i, X^i and Y^i respectively. As a matter of fact, the diffusion layer adopted in ARIA has the following property:

$$a_0 \oplus a_3 \oplus a_{12} \oplus a_{15} = b_0 \oplus b_3 \oplus b_{12} \oplus b_{15},$$

where $(a_0, a_1, \ldots, a_{15})$, $(b_0, b_1, \ldots, b_{15}) \in GF(2^8)^{16}$ are the input and output of the diffusion layer respectively. Thus according to the method given in Section 3, we construct several linear characteristics for the first 4 rounds of ARIA described as below:

$$\begin{aligned} &\text{0x17} \bullet (I_0^1 \oplus I_{12}^1) \oplus \text{0x10} \bullet (I_3^1 \oplus I_{15}^1) \\ &\oplus \text{0x4}D \bullet (O_0^4 \oplus O_3^4 \oplus O_{12}^4 \oplus O_{15}^4) \\ &= \text{0x17} \bullet (K_0^1 \oplus K_{12}^1) \oplus \text{0x10} \bullet (K_3^1 \oplus K_{15}^1) \\ &\oplus \text{0x17} \bullet (K_0^2 \oplus K_3^2 \oplus K_{12}^2 \oplus K_{15}^2) \\ &\oplus \text{0x4}D \bullet (K_0^3 \oplus K_3^3 \oplus K_{12}^3 \oplus K_{15}^3) \\ &\oplus \text{0x17} \bullet (K_0^4 \oplus K_3^4 \oplus K_{12}^4 \oplus K_{15}^4), \end{aligned} \tag{3}$$

$$\begin{aligned}
&0\text{x}0E \bullet (I_0^1 \oplus I_{12}^1) \oplus 0\text{x}15 \bullet (I_3^1 \oplus I_{15}^1) \\
&\oplus 0\text{x}B1 \bullet (O_0^4 \oplus O_3^4 \oplus O_{12}^4 \oplus O_{15}^4) \\
=\ &0\text{x}0E \bullet (K_0^1 \oplus K_{12}^1) \oplus 0\text{x}15 \bullet (K_3^1 \oplus K_{15}^1) \\
&\oplus 0\text{x}09 \bullet (K_0^2 \oplus K_3^2 \oplus K_{12}^2 \oplus K_{15}^2) \\
&\oplus 0\text{x}B1 \bullet (K_0^3 \oplus K_3^3 \oplus K_{12}^3 \oplus K_{15}^3) \\
&\oplus 0\text{x}09 \bullet (K_0^4 \oplus K_3^4 \oplus K_{12}^4 \oplus K_{15}^4),
\end{aligned} \tag{4}$$

$$\begin{aligned}
&0\text{x}40 \bullet (I_0^1 \oplus I_{12}^1) \oplus 0\text{x}1B \bullet (I_3^1 \oplus I_{15}^1) \\
&\oplus 0\text{x}ED \bullet (O_0^4 \oplus O_3^4 \oplus O_{12}^4 \oplus O_{15}^4) \\
=\ &0\text{x}40 \bullet (K_0^1 \oplus K_{12}^1) \oplus 0\text{x}1B \bullet (K_3^1 \oplus K_{15}^1) \\
&\oplus 0\text{x}08 \bullet (K_0^2 \oplus K_3^2 \oplus K_{12}^2 \oplus K_{15}^2) \\
&\oplus 0\text{x}ED \bullet (K_0^3 \oplus K_3^3 \oplus K_{12}^3 \oplus K_{15}^3) \\
&\oplus 0\text{x}08 \bullet (K_0^4 \oplus K_3^4 \oplus K_{12}^4 \oplus K_{15}^4),
\end{aligned} \tag{5}$$

and

$$\begin{aligned}
&0\text{x}B4 \bullet (I_0^1 \oplus I_{12}^1) \oplus 0\text{x}D9 \bullet (I_3^1 \oplus I_{15}^1) \\
&\oplus 0\text{x}4A \bullet (O_0^4 \oplus O_3^4 \oplus O_{12}^4 \oplus O_{15}^4) \\
=\ &0\text{x}B4 \bullet (K_0^1 \oplus K_{12}^1) \oplus 0\text{x}D9 \bullet (K_3^1 \oplus K_{15}^1) \\
&\oplus 0\text{x}03 \bullet (K_0^2 \oplus K_3^2 \oplus K_{12}^2 \oplus K_{15}^2) \\
&\oplus 0\text{x}4A \bullet (K_0^3 \oplus K_3^3 \oplus K_{12}^3 \oplus K_{15}^3) \\
&\oplus 0\text{x}03 \bullet (K_0^4 \oplus K_3^4 \oplus K_{12}^4 \oplus K_{15}^4),
\end{aligned} \tag{6}$$

where each of the above 4-round linear characteristics holds with probability $1/2 - 2^{-50.15}$ approximately. Next, we will demonstrate some effective key recovery attacks on reduced-round ARIA in terms of the linear characteristic given in equation (3).

4.1 Key Recovery Attacks on 7-Round ARIA, 9-Round ARIA and 11-Round ARIA

Let E denote the first s rounds of ARIA and $s = 7$. We now propose our key recovery attack on E. First of all, the linear characteristic described in equation (3) can be rewritten as follows:

$$\begin{aligned}
&0\text{x}17 \bullet (I_0^1 \oplus I_{12}^1) \oplus 0\text{x}10 \bullet (I_3^1 \oplus I_{15}^1) \\
&\oplus 0\text{x}4D \bullet (X_0^5 \oplus X_3^5 \oplus X_{12}^5 \oplus X_{15}^5) \\
=\ &0\text{x}17 \bullet (K_0^1 \oplus K_{12}^1) \oplus 0\text{x}10 \bullet (K_3^1 \oplus K_{15}^1) \\
&\oplus 0\text{x}17 \bullet (K_0^2 \oplus K_3^2 \oplus K_{12}^2 \oplus K_{15}^2) \\
&\oplus 0\text{x}4D \bullet (K_0^3 \oplus K_3^3 \oplus K_{12}^3 \oplus K_{15}^3) \\
&\oplus 0\text{x}17 \bullet (K_0^4 \oplus K_3^4 \oplus K_{12}^4 \oplus K_{15}^4) \\
&\oplus 0\text{x}4D \bullet (K_0^5 \oplus K_3^5 \oplus K_{12}^5 \oplus K_{15}^5).
\end{aligned} \tag{7}$$

Then we mount an attack on E based on the linear characteristic depicted in equation (7). The detailed description of our attack is given as below:

Step 1. Collect N pairs (P_μ, C_μ) $(1 \le \mu \le N)$, where P_μ, C_μ are the plaintext and ciphertext of E respectively. Let X_μ^i, Y_μ^i $(1 \le i \le s)$ denote the intermediate

16-byte vectors X^i and Y^i respectively which are relevant to the pair (P_μ, C_μ). Let $P_{\mu,j}$, $C_{\mu,j}$, $X^i_{\mu,j}$, $Y^i_{\mu,j}$ denote the $(j+1)$-th $(0 \le j \le 15)$ bytes of P_μ, C_μ, X^i_μ and Y^i_μ respectively. Derive $Y^s_{\mu,0}$, $Y^s_{\mu,3}$, $Y^s_{\mu,12}$ and $Y^s_{\mu,15}$ from the following expressions:

$$\begin{aligned}
Y^s_{\mu,0} &= C_{\mu,3} \oplus C_{\mu,4} \oplus C_{\mu,6} \oplus C_{\mu,8} \oplus C_{\mu,9} \oplus C_{\mu,13} \oplus C_{\mu,14},\\
Y^s_{\mu,3} &= C_{\mu,0} \oplus C_{\mu,5} \oplus C_{\mu,7} \oplus C_{\mu,10} \oplus C_{\mu,11} \oplus C_{\mu,13} \oplus C_{\mu,14},\\
Y^s_{\mu,12} &= C_{\mu,1} \oplus C_{\mu,2} \oplus C_{\mu,6} \oplus C_{\mu,7} \oplus C_{\mu,9} \oplus C_{\mu,11} \oplus C_{\mu,12},\\
Y^s_{\mu,15} &= C_{\mu,1} \oplus C_{\mu,2} \oplus C_{\mu,4} \oplus C_{\mu,5} \oplus C_{\mu,8} \oplus C_{\mu,10} \oplus C_{\mu,15}.
\end{aligned}$$

Initialize 2^{32} counters $\{T_l\}_{0 \le l \le 2^{32}-1}$ (the size of each counter could be set to $\lceil \log_2^N \rceil$ bits), where T_l corresponds to l which represents the possible value of $Y^s_{\mu,0} \| Y^s_{\mu,3} \| Y^s_{\mu,12} \| Y^s_{\mu,15}$. For each pair (P_μ, C_μ), increase (or decrease) the counter T_l by 1 if the parity of

$$0\text{x}17 \bullet (P_{\mu,0} \oplus P_{\mu,12}) \oplus 0\text{x}10 \bullet (P_{\mu,3} \oplus P_{\mu,15})$$

is 0 (or 1) as well as the value of $Y^s_{\mu,0} \| Y^s_{\mu,3} \| Y^s_{\mu,12} \| Y^s_{\mu,15}$ is equal to l.

Step 2. Let K^{s-1}_g, K^s_g denote $K^{s-1}_0 \oplus K^{s-1}_3 \oplus K^{s-1}_{12} \oplus K^{s-1}_{15}$ and $K^s_0 \oplus K^s_3 \oplus K^s_{12} \oplus K^s_{15}$ respectively. Let θ_1, θ_2, ξ denote $Y^{s-1}_{\mu,0} \| Y^{s-1}_{\mu,3} \| Y^{s-1}_{\mu,12} \| Y^{s-1}_{\mu,15}$, $Y^{s-2}_{\mu,0} \| Y^{s-2}_{\mu,3} \| Y^{s-2}_{\mu,12} \| Y^{s-2}_{\mu,15}$ and $K^{s-1}_g \| K^s_g \| \theta_1 \| \theta_2$ respectively. Initialize 2^{80} counters $\{T'_\xi\}_{0 \le \xi \le 2^{80}-1}$ (the size of each counter could be set to $\lceil \log_2^N \rceil$ bits), where T'_ξ corresponds to ξ. For each possible value of $K^{s-1}_g \| K^s_g$, do the following:
(I). For each possible vaule of l, calculate $X^s_{\mu,0}$, $X^s_{\mu,3}$, $X^s_{\mu,12}$ and $X^s_{\mu,15}$ according to the corresponding S-boxes. Then compute the value of $Y^{s-1}_{\mu,0} \oplus Y^{s-1}_{\mu,3} \oplus Y^{s-1}_{\mu,12} \oplus Y^{s-1}_{\mu,15}$ and denote the value as v^{s-1}. Go to (II).

(II). For any of the 2^{24} possible values of θ_1 satisfying $Y^{s-1}_{\mu,0} \oplus Y^{s-1}_{\mu,3} \oplus Y^{s-1}_{\mu,12} \oplus Y^{s-1}_{\mu,15} = v^{s-1}$, derive $X^{s-1}_{\mu,0}$, $X^{s-1}_{\mu,3}$, $X^{s-1}_{\mu,12}$ and $X^{s-1}_{\mu,15}$ according to the corresponding S-boxes. Then get the value of $Y^{s-2}_{\mu,0} \oplus Y^{s-2}_{\mu,3} \oplus Y^{s-2}_{\mu,12} \oplus Y^{s-2}_{\mu,15}$ and denote the value as v^{s-2}. Go to (III).

(III). For any of the 2^{24} possible values of θ_2 satisfying $Y^{s-2}_{\mu,0} \oplus Y^{s-2}_{\mu,3} \oplus Y^{s-2}_{\mu,12} \oplus Y^{s-2}_{\mu,15} = v^{s-2}$, obtain $X^{s-2}_{\mu,0}$, $X^{s-2}_{\mu,3}$, $X^{s-2}_{\mu,12}$ and $X^{s-2}_{\mu,15}$ according to the corresponding S-boxes. Then calculate the parity of

$$0\text{x}4D \bullet (X^{s-2}_{\mu,0} \oplus X^{s-2}_{\mu,3} \oplus X^{s-2}_{\mu,12} \oplus X^{s-2}_{\mu,15}).$$

If the parity is 0, increase the relevant counter T'_ξ by the value of T_l, and decrease by the value of T_l otherwise.

Step 3. For the ξ such that the value of $|T'_\xi|$ is maximal, take the value of the corresponding $K^{s-1}_g \| K^s_g$ as the correct key information.

Actually, we need to guess about 80 bits in the above attack. Thus following the Theorem 2 proposed in [17], the number of plaintext-ciphertext pairs required in the attack can be estimated as $2^{5.5} \times \frac{1}{(2^{-50.15})^2} = 2^{105.8}$ in order to achieve a high success probability of 88% approximately (i.e., $N = 2^{105.8}$). The time complexity of the attack is dominated mainly by the calculations of $Y^s_{\mu,0}$, $Y^s_{\mu,3}$, $Y^s_{\mu,12}$ and $Y^s_{\mu,15}$ in the step 1 and the decryptions of the S-boxes in the step 2(III). Consequently, the time complexity of the attack is around $2^{105.8} \times \frac{4}{16\times 7} + 2^{16} \times 2^{32} \times 2^{24} \times 2^{24} \times \frac{4}{16\times 7} \approx 2^{100.99}$ 7-round ARIA encryptions. Regarding the memory complexity of the attack, it is primarily owing to keeping the counters $\{T'_\xi\}_{0\le\xi\le 2^{80}-1}$ (the size of each counter is set to 106 bits) in the step 2. Accordingly, the memory complexity of the attack is about $2^{80} \times 106/8 \approx 2^{83.73}$ bytes.

For the cases of $s = 9$ and $s = 11$, the procedures of the attacks on the first 9 rounds and the first 11 rounds of ARIA are the same as that in the case of $s = 7$ except the step 2 and step 3 which are described as below.

Case 1: $s = 9$.

Step 2. Let K^{s-3}_g, K^{s-2}_g, K^{s-1}_g, K^s_g denote $K^{s-3}_0 \oplus K^{s-3}_3 \oplus K^{s-3}_{12} \oplus K^{s-3}_{15}$, $K^{s-2}_0 \oplus K^{s-2}_3 \oplus K^{s-2}_{12} \oplus K^{s-2}_{15}$, $K^{s-1}_0 \oplus K^{s-1}_3 \oplus K^{s-1}_{12} \oplus K^{s-1}_{15}$ and $K^s_0 \oplus K^s_3 \oplus K^s_{12} \oplus K^s_{15}$ respectively. Let θ_1, θ_2, θ_3, θ_4, ξ denote $Y^{s-1}_{\mu,0}\|Y^{s-1}_{\mu,3}\|Y^{s-1}_{\mu,12}\|Y^{s-1}_{\mu,15}$, $Y^{s-2}_{\mu,0}\|Y^{s-2}_{\mu,3}\|Y^{s-2}_{\mu,12}\|Y^{s-2}_{\mu,15}$, $Y^{s-3}_{\mu,0}\|Y^{s-3}_{\mu,3}\|Y^{s-3}_{\mu,12}\|Y^{s-3}_{\mu,15}$, $Y^{s-4}_{\mu,0}\|Y^{s-4}_{\mu,3}\|Y^{s-4}_{\mu,12}\|Y^{s-4}_{\mu,15}$ and $K^{s-3}_g\|K^{s-2}_g\|K^{s-1}_g\|K^s_g\|\theta_1\|\theta_2\|\theta_3\|\theta_4$ respectively. Initialize 2^{160} counters $\{T'_\xi\}_{0\le\xi\le 2^{160}-1}$ (the size of each counter could be set to $\lceil \log_2^N \rceil$ bits), where T'_ξ corresponds to ξ. For each possible value of $K^{s-3}_g\|K^{s-2}_g\|K^{s-1}_g\|K^s_g$, do the following:

(I). For each possible vaule of l, calculate $X^s_{\mu,0}$, $X^s_{\mu,3}$, $X^s_{\mu,12}$ and $X^s_{\mu,15}$ according to the corresponding S-boxes. Then compute the value of $Y^{s-1}_{\mu,0} \oplus Y^{s-1}_{\mu,3} \oplus Y^{s-1}_{\mu,12} \oplus Y^{s-1}_{\mu,15}$ and denote the value as v^{s-1}. Go to (II).

(II). For any of the 2^{24} possible values of θ_1 satisfying $Y^{s-1}_{\mu,0} \oplus Y^{s-1}_{\mu,3} \oplus Y^{s-1}_{\mu,12} \oplus Y^{s-1}_{\mu,15} = v^{s-1}$, derive $X^{s-1}_{\mu,0}$, $X^{s-1}_{\mu,3}$, $X^{s-1}_{\mu,12}$ and $X^{s-1}_{\mu,15}$ according to the corresponding S-boxes. Then get the value of $Y^{s-2}_{\mu,0} \oplus Y^{s-2}_{\mu,3} \oplus Y^{s-2}_{\mu,12} \oplus Y^{s-2}_{\mu,15}$ and denote the value as v^{s-2}. Go to (III).

(III). For any of the 2^{24} possible values of θ_2 satisfying $Y^{s-2}_{\mu,0} \oplus Y^{s-2}_{\mu,3} \oplus Y^{s-2}_{\mu,12} \oplus Y^{s-2}_{\mu,15} = v^{s-2}$, obtain $X^{s-2}_{\mu,0}$, $X^{s-2}_{\mu,3}$, $X^{s-2}_{\mu,12}$ and $X^{s-2}_{\mu,15}$ according to the corresponding S-boxes. Then compute the value of $Y^{s-3}_{\mu,0} \oplus Y^{s-3}_{\mu,3} \oplus Y^{s-3}_{\mu,12} \oplus Y^{s-3}_{\mu,15}$ and denote the value as v^{s-3}. Go to (IV).

(IV). For any of the 2^{24} possible values of θ_3 satisfying $Y^{s-3}_{\mu,0} \oplus Y^{s-3}_{\mu,3} \oplus Y^{s-3}_{\mu,12} \oplus Y^{s-3}_{\mu,15} = v^{s-3}$, derive $X^{s-3}_{\mu,0}$, $X^{s-3}_{\mu,3}$, $X^{s-3}_{\mu,12}$ and $X^{s-3}_{\mu,15}$ according to the

corresponding S-boxes. Then get the value of $Y_{\mu,0}^{s-4} \oplus Y_{\mu,3}^{s-4} \oplus Y_{\mu,12}^{s-4} \oplus Y_{\mu,15}^{s-4}$ and denote the value as v^{s-4}. Go to (V).

(V). For any of the 2^{24} possible values of θ_4 satisfying $Y_{\mu,0}^{s-4} \oplus Y_{\mu,3}^{s-4} \oplus Y_{\mu,12}^{s-4} \oplus Y_{\mu,15}^{s-4} = v^{s-4}$, obtain $X_{\mu,0}^{s-4}$, $X_{\mu,3}^{s-4}$, $X_{\mu,12}^{s-4}$ and $X_{\mu,15}^{s-4}$ according to the corresponding S-boxes. Then calculate the parity of

$$0\text{x}4D \bullet (X_{\mu,0}^{s-4} \oplus X_{\mu,3}^{s-4} \oplus X_{\mu,12}^{s-4} \oplus X_{\mu,15}^{s-4}).$$

If the parity is 0, increase the relevant counter T'_ξ by the value of T_l, and decrease by the value of T_l otherwise.
Step 3. For the ξ such that the value of $|T'_\xi|$ is maximal, take the value of the corresponding $K_g^{s-3}\|K_g^{s-2}\|K_g^{s-1}\|K_g^s$ as the correct key information.

Case 2: $s = 11$.

Step 2. Let K_g^{s-5}, K_g^{s-4}, K_g^{s-3}, K_g^{s-2}, K_g^{s-1}, K_g^s denote $K_0^{s-5} \oplus K_3^{s-5} \oplus K_{12}^{s-5} \oplus K_{15}^{s-5}$, $K_0^{s-4} \oplus K_3^{s-4} \oplus K_{12}^{s-4} \oplus K_{15}^{s-4}$, $K_0^{s-3} \oplus K_3^{s-3} \oplus K_{12}^{s-3} \oplus K_{15}^{s-3}$, $K_0^{s-2} \oplus K_3^{s-2} \oplus K_{12}^{s-2} \oplus K_{15}^{s-2}$, $K_0^{s-1} \oplus K_3^{s-1} \oplus K_{12}^{s-1} \oplus K_{15}^{s-1}$ and $K_0^s \oplus K_3^s \oplus K_{12}^s \oplus K_{15}^s$ respectively. Let θ_1, θ_2, θ_3, θ_4, θ_5, θ_6, ξ denote $Y_{\mu,0}^{s-1}\|Y_{\mu,3}^{s-1}\|Y_{\mu,12}^{s-1}\|Y_{\mu,15}^{s-1}$, $Y_{\mu,0}^{s-2}\|Y_{\mu,3}^{s-2}\|Y_{\mu,12}^{s-2}\|Y_{\mu,15}^{s-2}$, $Y_{\mu,0}^{s-3}\|Y_{\mu,3}^{s-3}\|Y_{\mu,12}^{s-3}\|Y_{\mu,15}^{s-3}$, $Y_{\mu,0}^{s-4}\|Y_{\mu,3}^{s-4}\|Y_{\mu,12}^{s-4}\|Y_{\mu,15}^{s-4}$, $Y_{\mu,0}^{s-5}\|Y_{\mu,3}^{s-5}\|Y_{\mu,12}^{s-5}\|Y_{\mu,15}^{s-5}$, $Y_{\mu,0}^{s-6}\|Y_{\mu,3}^{s-6}\|Y_{\mu,12}^{s-6}\|Y_{\mu,15}^{s-6}$ and $K_g^{s-5}\|K_g^{s-4}\|K_g^{s-3}\|K_g^{s-2}\|K_g^{s-1}\|K_g^s\|\theta_1\|\theta_2\|\theta_3\|\theta_4\|\theta_5\|\theta_6$ respectively. Initialize 2^{240} counters $\{T'_\xi\}_{0 \le \xi \le 2^{240}-1}$ (the size of each counter could be set to $\lceil \log_2^N \rceil$ bits), where T'_ξ corresponds to ξ. For each possible value of $K_g^{s-5}\|K_g^{s-4}\|K_g^{s-3}\|K_g^{s-2}\|K_g^{s-1}\|K_g^s$, do the following:
(I). For each possible vaule of l, calculate $X_{\mu,0}^s$, $X_{\mu,3}^s$, $X_{\mu,12}^s$ and $X_{\mu,15}^s$ according to the corresponding S-boxes. Then compute the value of $Y_{\mu,0}^{s-1} \oplus Y_{\mu,3}^{s-1} \oplus Y_{\mu,12}^{s-1} \oplus Y_{\mu,15}^{s-1}$ and denote the value as v^{s-1}. Go to (II).

(II). For any of the 2^{24} possible values of θ_1 satisfying $Y_{\mu,0}^{s-1} \oplus Y_{\mu,3}^{s-1} \oplus Y_{\mu,12}^{s-1} \oplus Y_{\mu,15}^{s-1} = v^{s-1}$, derive $X_{\mu,0}^{s-1}$, $X_{\mu,3}^{s-1}$, $X_{\mu,12}^{s-1}$ and $X_{\mu,15}^{s-1}$ according to the corresponding S-boxes. Then get the value of $Y_{\mu,0}^{s-2} \oplus Y_{\mu,3}^{s-2} \oplus Y_{\mu,12}^{s-2} \oplus Y_{\mu,15}^{s-2}$ and denote the value as v^{s-2}. Go to (III).

(III). For any of the 2^{24} possible values of θ_2 satisfying $Y_{\mu,0}^{s-2} \oplus Y_{\mu,3}^{s-2} \oplus Y_{\mu,12}^{s-2} \oplus Y_{\mu,15}^{s-2} = v^{s-2}$, obtain $X_{\mu,0}^{s-2}$, $X_{\mu,3}^{s-2}$, $X_{\mu,12}^{s-2}$ and $X_{\mu,15}^{s-2}$ according to the corresponding S-boxes. Then compute the value of $Y_{\mu,0}^{s-3} \oplus Y_{\mu,3}^{s-3} \oplus Y_{\mu,12}^{s-3} \oplus Y_{\mu,15}^{s-3}$ and denote the value as v^{s-3}. Go to (IV).

(IV). For any of the 2^{24} possible values of θ_3 satisfying $Y_{\mu,0}^{s-3} \oplus Y_{\mu,3}^{s-3} \oplus Y_{\mu,12}^{s-3} \oplus Y_{\mu,15}^{s-3} = v^{s-3}$, derive $X_{\mu,0}^{s-3}$, $X_{\mu,3}^{s-3}$, $X_{\mu,12}^{s-3}$ and $X_{\mu,15}^{s-3}$ according to the corresponding S-boxes. Then get the value of $Y_{\mu,0}^{s-4} \oplus Y_{\mu,3}^{s-4} \oplus Y_{\mu,12}^{s-4} \oplus Y_{\mu,15}^{s-4}$ and denote the value as v^{s-4}. Go to (V).

Table 1. Summary of Attacks on Reduced-round ARIA

Type of Attack	Key Size	Rounds	Data	Time	Memory
ID [9]	all	5	$2^{71.3}$ CP	$2^{71.6}$ Enc	2^{76} B *
MIMA [15]	all	5	2^{25} CP	$2^{65.4}$ Enc	$2^{126.5}$ B *
BA [13]	all	5	2^{109} ACPC	2^{110} Enc	2^{61} B *
IA [11]	all	5	$2^{27.5}$ CP	$2^{76.7}$ Enc	$2^{31.5}$ B *
ID [8]	all	6	2^{121} CP	2^{112} Enc	2^{125} B *
ID [9]	all	6	$2^{120.5}$ CP	$2^{104.5}$ Enc	2^{125} B *
ID [9]	all	6	2^{113} CP	$2^{121.6}$ Enc	2^{117} B *
IA [11]	192/256	6	$2^{124.4}$ CP	$2^{172.4}$ Enc	$2^{128.4}$ B *
MIMA [15]	all	6	2^{56} CP	$2^{121.5}$ Enc	$2^{126.5}$ B *
BA [13]	all	6	2^{128} KP	2^{108} Enc	2^{60} B *
IA [12]	all	6	$2^{99.2}$ CP	$2^{71.4}$ Enc	–
MIMA [15]	192/256	7	2^{120} CP	$2^{185.3}$ Enc	2^{191} B *
BA [13]	256	7	2^{128} KP	2^{236} Enc	2^{188} B *
ID [10]	256	7	2^{125} CP	2^{238} Enc	–
IA [12]	256	7	$2^{100.6}$ CP	$2^{225.8}$ Enc	–
LC (This paper)	all	7	$2^{105.8}$ KP	$2^{100.99}$ Enc	$2^{83.73}$ B
MIMA [15]	256	8	2^{56} CP	$2^{251.6}$ Enc	2^{256} B *
LC (This paper)	192/256	9	$2^{108.3}$ KP	$2^{154.83}$ Enc	$2^{163.77}$ B
LC (This paper)	256	11	$2^{110.3}$ KP	$2^{218.54}$ Enc	$2^{243.8}$ B

ID: Impossible Differential, MIMA: Meet-in-the-Middle Attack,
BA: Boomerang Attack, IA: Integral Attack, LC: Linear Cryptanalysis,
CP: Chosen plaintexts, KP: Known plaintexts,
ACPC: Adaptive chosen plaintexts and ciphertexts,
Enc: Encryptions, B: Bytes,
-: Not given in the related paper, *: Estimated in [13].

(V). For any of the 2^{24} possible values of θ_4 satisfying $Y^{s-4}_{\mu,0} \oplus Y^{s-4}_{\mu,3} \oplus Y^{s-4}_{\mu,12} \oplus Y^{s-4}_{\mu,15} = v^{s-4}$, obtain $X^{s-4}_{\mu,0}$, $X^{s-4}_{\mu,3}$, $X^{s-4}_{\mu,12}$ and $X^{s-4}_{\mu,15}$ according to the corresponding S-boxes. Then compute the value of $Y^{s-5}_{\mu,0} \oplus Y^{s-5}_{\mu,3} \oplus Y^{s-5}_{\mu,12} \oplus Y^{s-5}_{\mu,15}$ and denote the value as v^{s-5}. Go to (VI).

(VI). For any of the 2^{24} possible values of θ_5 satisfying $Y^{s-5}_{\mu,0} \oplus Y^{s-5}_{\mu,3} \oplus Y^{s-5}_{\mu,12} \oplus Y^{s-5}_{\mu,15} = v^{s-5}$, derive $X^{s-5}_{\mu,0}$, $X^{s-5}_{\mu,3}$, $X^{s-5}_{\mu,12}$ and $X^{s-5}_{\mu,15}$ according to the corresponding S-boxes. Then get the value of $Y^{s-6}_{\mu,0} \oplus Y^{s-6}_{\mu,3} \oplus Y^{s-6}_{\mu,12} \oplus Y^{s-6}_{\mu,15}$ and denote the value as v^{s-6}. Go to (VII).

(VII). For any of the 2^{24} possible values of θ_6 satisfying $Y^{s-6}_{\mu,0} \oplus Y^{s-6}_{\mu,3} \oplus Y^{s-6}_{\mu,12} \oplus Y^{s-6}_{\mu,15} = v^{s-6}$, obtain $X^{s-6}_{\mu,0}$, $X^{s-6}_{\mu,3}$, $X^{s-6}_{\mu,12}$ and $X^{s-6}_{\mu,15}$ according to the corresponding S-boxes. Then calculate the parity of

$$0\text{x}4D \bullet (X^{s-6}_{\mu,0} \oplus X^{s-6}_{\mu,3} \oplus X^{s-6}_{\mu,12} \oplus X^{s-6}_{\mu,15}).$$

If the parity is 0, increase the relevant counter T'_ξ by the value of T_l, and decrease by the value of T_l otherwise.

Step 3. For the ξ such that the value of $|T'_\xi|$ is maximal, take the value of the corresponding $K_g^{s-5}\|K_g^{s-4}\|K_g^{s-3}\|K_g^{s-2}\|K_g^{s-1}\|K_g^s$ as the correct key information.

Since we need to guess about 160 bits and 240 bits in case 1 and case 2 respectively, according to the Theorem 2 proposed in [17], the number of plaintext-ciphertext pairs required in these cases can be estimated as $2^8 \times \frac{1}{(2^{-50.15})^2} = 2^{108.3}$ and $2^{10} \times \frac{1}{(2^{-50.15})^2} = 2^{110.3}$ respectively in order to achieve a high success probability of 88% approximately (i.e., $N = 2^{108.3}$ in case 1 and $N = 2^{110.3}$ in case 2). The time complexities and memory complexities in these cases can be measured similarly to those in the case of $s = 7$. Thus the time complexities in these cases are around $2^{32} \times 2^{32} \times 2^{24} \times 2^{24} \times 2^{24} \times 2^{24} \times \frac{4}{16\times 9} \approx 2^{154.83}$ 9-round ARIA encryptions and $2^{48} \times 2^{32} \times 2^{24} \times 2^{24} \times 2^{24} \times 2^{24} \times 2^{24} \times 2^{24} \times \frac{4}{16\times 11} \approx 2^{218.54}$ 11-round ARIA encryptions respectively, and the memory complexities in these cases are about $2^{160} \times 109/8 \approx 2^{163.77}$ bytes and $2^{240} \times 111/8 \approx 2^{243.8}$ bytes respectively.

5 Conclusion

In this paper, we introduce a new idea of deriving a kind of special linear characteristics for byte-oriented SPN block ciphers. Following this idea, we present several special 4-round linear characteristics of ARIA. Then based on such linear characteristics, we mount a key recovery attack on 7-round ARIA with 128/192/256-bit key size, a key recovery attack on 9-round ARIA with 192/256-bit key size as well as a key recovery attack on 11-round ARIA with 256-bit key size. In fact, the designers of ARIA expect that there isn't any effective attack on 8 or more rounds of ARIA with 128/192/256-bit key size by means of linear cryptanalysis. However, our work shows that such attacks do exist. Furthermore, the results of our attacks are better than the previously known cryptanalytic results of ARIA. The complexities of our attacks together with the formerly existing attacks on ARIA are summarized in Table 1.

Acknowledgements. This work has been supported by the National Natural Science Foundation of China (No. 61073150 and No. 61003278), the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, and the Fundamental Research Funds for the Central Universities. Moreover, we are very grateful to the anonymous referees for their comments and editorial suggestions.

References

1. Kwon, D., Kim, J., Park, S., Sung, S.H., et al.: New Block Cipher: ARIA. In: Lim, J.-I., Lee, D.-H. (eds.) ICISC 2003. LNCS, vol. 2971, pp. 432–445. Springer, Heidelberg (2004)

2. National Security Research Institute, Korea. Specification of ARIA. Version 1.0 (2005)
3. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1991)
4. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
5. Knudsen, L.R.: Truncated and Higher Order Differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995)
6. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. Journal of Cryptology 18(4), 291–311 (2005)
7. Knudsen, L.R., Wagner, D.: Integral Cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
8. Wu, W., Zhang, W., Feng, D.: Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia. Journal of Computer Science and Technology 22(3), 449–456 (2007)
9. Li, R., Sun, B., Zhang, P., Li, C.: New Impossible Differentials of ARIA. Cryptology ePrint Archive, Report 2008/227 (2008), `http://eprint.iacr.org/`
10. Du, C., Chen, J.: Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds. In: Heng, S.-H., Wright, R.N., Goi, B.-M. (eds.) CANS 2010. LNCS, vol. 6467, pp. 20–30. Springer, Heidelberg (2010)
11. Li, P., Sun, B., Li, C.: Integral Cryptanalysis of ARIA. In: Bao, F., Yung, M., Lin, D., Jing, J. (eds.) Inscrypt 2009. LNCS, vol. 6151, pp. 1–14. Springer, Heidelberg (2010)
12. Li, Y., Wu, W., Zhang, L.: Integral Attacks on Reduced-Round ARIA Block Cipher. In: Kwak, J., Deng, R.H., Won, Y., Wang, G. (eds.) ISPEC 2010. LNCS, vol. 6047, pp. 19–29. Springer, Heidelberg (2010)
13. Fleischmann, E., Forler, C., Gorski, M., Lucks, S.: New Boomerang Attacks on ARIA. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 163–175. Springer, Heidelberg (2010)
14. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)
15. Tang, X., Sun, B., Li, R., Li, C.: A Meet-in-the-middle Attack on ARIA. Cryptology ePrint Archive, Report 2010/168 (2010), `http://eprint.iacr.org/`
16. Demirci, H., Selçuk, A.A.: A Meet-in-the-Middle Attack on 8-Round AES. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 116–126. Springer, Heidelberg (2008)
17. Selçuk, A.A.: On Probability of Success in Linear and Differential Cryptanalysis. Journal of Cryptology 21(1), 131–147 (2008)