Multidimensional Differential-Linear Cryptanalysis of ARIA Block Cipher

Wentan Yi, Jiongjiong Ren, and Shaozhen Chen

ARIA is a 128-bit block cipher that has been selected as a Korean encryption standard. Similar to AES, it is robust against differential cryptanalysis and linear cryptanalysis. In this study, we analyze the security of ARIA against differential-linear cryptanalysis. We present five rounds of differential-linear distinguishers for ARIA, which can distinguish five rounds of ARIA from random permutations using only 284.8 chosen plaintexts. Moreover, we develop differential-linear attacks based on six rounds of ARIA-128 and seven rounds of ARIA-256. This is the first multidimensional differential-linear cryptanalysis of ARIA and it has lower data complexity than all previous results. This is a preliminary study and further research may obtain better results in the future.

Keywords: ARIA, Block cipher, Cryptanalysis, Linear hull, Multidimensional differential-linear attack.

I. Introduction

ARIA [1] is a block cipher designed by the Korean cryptographers Kwon and others in ICISC 2003. The upgraded version 1.0 of ARIA [2] was selected as a Korean standard block cipher by the Ministry of Commerce, Industry, and Energy [3] in 2004. ARIA has also been adopted by several standard protocols such as IETF (RFC 5794 [4]), SSL/TLS (RFC 6209 [5]) and PKCS #11 [6]. In Korea, ARIA has been used widely, especially in government-to-public services. Thus, studies of the security of ARIA are important in various areas of cryptanalysis and it is necessary to constantly reevaluate its security using various cryptanalytic techniques.

The design of ARIA is provably resistant against differential and linear attacks, but many other cryptanalysis methods have been developed to attack ARIA, such as integral attacks [7], [8], boomerang attacks [9], meet-in-the-middle attacks [10]–[12], impossible differential attacks [13]–[15], zero-correlation linear attacks [16], and biclique attacks [17]. Li and others [7] presented integral attacks based on six-round ARIA-128 and seven-round ARIA-256. Fleischmann and others [9] reported boomerang attacks based on six rounds of ARIA-128 and seven rounds of ARIA-256 using all the plaintexts. Wu and others [13] presented a six-round impossible differential attack against ARIA, which was improved with lower attack complexities by Li and others [14]. Du and Chen [15] demonstrated an impossible differential attack on seven-round ARIA-256 with one extended round. Yi and others [16] reported some four-round zero-correlation linear approximations of ARIA and presented zero-correlation linear attacks on six rounds of ARIA-128 and seven rounds of ARIA-256. Chen and Xu [17] presented biclique attacks on full-round ARIA-256 with about $2^{255.2}$ encryptions. Tang and others [10] employed a meet-in-the-middle attack to break seven rounds of ARIA-192 and eight rounds of ARIA-256, which

Manuscript received Aug. 7, 2016; revised Oct. 11, 2016; accepted Nov. 29, 2016.

Wentan Yi (corresponding author, nlwt8988@gmail.com), Jiongjiong Ren (jiongjiong_fun@163.com), and Shaozhen Chen (chenshaozhen@vip.sina.com) are with the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China.

https://doi.org/10.4218/etrij.17.0116.0544

Table 1. Comparison of attacks on ARIA.

Attack type	Rounds	Date	Time	Memory	Reference
Integral	6	$2^{127.2}$ CPs	$2^{124.4}$ Enc	$2^{124.4}$ Byte	[7]
Integral	7	$2^{100.6}$ CPs	$2^{225.8}$ Enc	N/A	[7]
Impossible differential	6	2^{125} CPs	2^{238} Enc	2^{121} Byte	[15]
Impossible differential	7	2^{125} CPs	2^{238} Enc	2^{125} Byte	[15]
Zero correlation linear	6	$2^{123.6}$ KPs	2^{121} Enc	$2^{90.3}$ Byte	[16]
Zero correlation linear	7	$2^{124.6}$ KPs	$2^{203.5}$ Enc	2^{152} Byte	[16]
Meet-in-the-middle	7	2^{120} KPs	$2^{185.3}$ Enc	2^{187} Byte	[10]
Meet-in-the-middle	7	2^{113} KPs	$2^{135.1}$ Enc	2^{130} Byte	[12]
Boomerang	6	2^{128} KPs	2^{108} Enc	2^{56} Byte	[9]
Boomerang	7	2^{128} KPs	2^{236} Enc	2^{184} Byte	[9]
Differential-linear	6	$2^{84.4}$ CPs	$2^{112.8}$ Enc	2^{96} Byte	Section 4.1
Differential-linear	7	$2^{84.6}$ CPs	$2^{215.3}$ Enc	2^{224} Byte	Section 4.2

were improved by Akshima and others [11] and Bai and others [12], respectively.

However, the security of ARIA against differential-linear attack is still unclear. Differential-linear attack, which was introduced by Langford and Hellman [18], is a combination of differential and linear attacks, where the basic idea is to split the cipher under consideration into two parts. A strong truncated differential exists for the first part of the cipher and a strongly biased linear approximation for the second part. Subsequently, these types of attacks were discussed and generalized by Biham and others [19], Langford [20], Liu and others [21], Lu [22], and Wagner [23]. A more rigorous analysis was provided recently by Blondeau and others [24] in FSE 2014, where a multidimensional generalization was introduced, which was defined for multiple input differences and multidimensional linear output masks.

This paper focuses on the multidimensional differential-linear attack on ARIA. Several five-round differential-linear distinguishers are constructed for ARIA, and the security of six rounds of ARIA-128 and seven rounds of ARIA-256 are evaluated by multidimensional differential-linear cryptanalysis. Our main contributions are summarized as follows.

Construction of several differential-linear distinguishers for -round ARIA. In EUROCRYPTO 2016, Sun and others [25] proved that the longest rounds was four for the impossible differentials and zero correlation linear hulls of ARIA without considering the S-box details. In CRYPTO 2016, Sun and others [26] constructed several types of five-round zero-correlation linear hulls for AES provided that the difference of two subkey bytes is known. However, this method cannot be employed to construct longer distinguishers for ARIA due to the specific usage of the neighboring confusion layer and involutional diffusion layer. This paper describes several differential-linear distinguishers for five-round ARIA with multiple input differences and multidimensional linear output masks, which can distinguish five rounds of ARIA from random permutations using about $2^{84.8}$ chosen plaintexts.

Launching attacks on ARIA with multidimensional differential-linear cryptanalysis. Five-round differential-linear distinguishers are given, thus we could mount a key-recovery attack against round-reduced ARIA using a multidimensional differential-linear attack. The attack on six-round ARIA requires $2^{83.1}$ chosen plaintexts and $2^{101.4}$ encryptions. Moreover, we propose an attack on seven-round ARIA with a data complexity of $2^{83.1}$ chosen plaintexts and time complexity of $2^{215.3}$ encryptions. These are the first applications of the multidimensional differential-linear attack technique. Table 1 summarizes several previous types of attack and our results based on ARIA.

The remainder of this paper is organized as follows. In Section II, we provide a brief description of ARIA and a formalized description of differential-linear cryptanalysis. In Section III, we construct several five-round differential-linear distinguishers for ARIA. Using these distinguishers, Section IV presents the attacks on six-round ARIA-128 and seven-round ARIA-256. In Section V, we give our conclusions.

II. Preliminaries

First, we give some notations and definitions that are used throughout this study, as well as a brief description of ARIA. We then provide a formalized description of differential-linear cryptanalysis.

1. Notations and Definitions

$|A|$ denotes the number of elements in set A. Given a subspace U of $\mathbb{F}_2^n$, let us denote $U^{\perp}$ as the orthogonal subspace of U with respect to the inner product of $\mathbb{F}_2^n$. We use the notation *sp*(a) to denote the vector subspace $\{0, a\} \in \mathbb{F}_2^n$ spanned by a. The plaintexts and ciphertexts are denoted by p c. A 128-bit internal state A is represented as a 4 × 4 byte matrix. The symbol $A[i]$ is used to express a byte of A, where i is the ordering of bytes i = 0, … , 15 and the first column includes A[0, 1, 2, 3], the second column includes A[4, 5, 6, 7], and so on. The number of rounds is denoted by N_r. The symbols X_i, Y_i, and Z_i denote the intermediate values before the substitution layer (SL), diffusion layer (DL), and AddRoundKey (AK) operations in the i-th round, respectively. The subkey of the i-th round is denoted by k_i and the whitening key is denoted by k_0. The symbol u_i is used to represent the equivalent key with $u_i = DL(k_i)$.

Given a vectorial Boolean function F on $\mathbb{F}_2^n$, the differential is given by $(\delta \to \Delta)$ with an input difference Δ and an output difference δ, and its probability is defined as

$$Pr_F(\delta \to \Delta) = 2^{-n}\,|A_{(\delta,\Delta)}|,$$

where $A_{(\delta,\Delta)} = \{x \in \mathbb{F}_2^n \mid f(x) \oplus f(x \oplus \delta) = \Delta\}$.

The linear approximation is given by $(\alpha \to \beta)$ with an input mask α and an output mask β, where its bias is defined as

$$\epsilon_F(\alpha,\beta) = 2^{-n}\,|\{x \in \mathbb{F}_2^n \mid \beta \cdot F(x) \oplus \alpha \cdot x = 0\}| - \frac{1}{2},$$

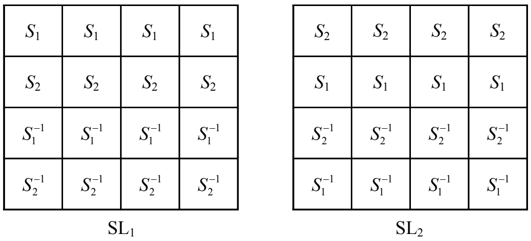
and the correlation of the linear approximation is given by

$$Cor_F(\alpha,\beta) = |2\epsilon_F(\alpha,\beta) - 1|.$$

2. Brief Description of ARIA

ARIA is a block cipher of 128-bit, which uses variable key sizes; that is, N_r depends on the key sizes. ARIA iterates 12 rounds for 128-bit key size, 14 rounds for 192-bit key size, and 16 rounds for 256-bit key size. The round function comprises the following three basic operations.

SL: Based on four 8 × 8-bit S-boxes S_1, S_2 and their inverses S_1^{-1}, S_2^{-1}, ARIA has two types of SL: SL$_1$ and SL$_2$ (see Fig. 1). SL$_1$ is used in the odd rounds and SL$_2$ is used in the even rounds.



S_1	S_1	S_1	S_1
S_2	S_2	S_2	S_2
S_1^{-1}	S_1^{-1}	S_1^{-1}	S_1^{-1}
S_2^{-1}	S_2^{-1}	S_2^{-1}	S_2^{-1}

SL$_1$

S_2	S_2	S_2	S_2
S_1	S_1	S_1	S_1
S_2^{-1}	S_2^{-1}	S_2^{-1}	S_2^{-1}
S_1^{-1}	S_1^{-1}	S_1^{-1}	S_1^{-1}

SL$_2$

Fig. 1. Two substitution layers in ARIA.

DL: The linear DL is a 16 × 16 involution binary matrix with branch number 8.

$$\begin{pmatrix}
0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&0\\
0&0&1&0&0&1&0&1&1&1&0&0&1&0&0&1\\
0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1\\
1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0\\
1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1\\
0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1\\
1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0\\
0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0\\
1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1\\
1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0\\
0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&1\\
0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0\\
0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0\\
1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0\\
1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0\\
0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1
\end{pmatrix}$$

AK: This is an operation for XORing the state and the 128-bit round subkey.

An additional whitening AK operation is performed before the first round and a DL operation is omitted in the last round. Our attacks do not utilize the key relations, so we omit the details of ARIA's key schedule. For further details of ARIA, please refer to [1].

3. Differential-Linear Cryptanalysis

In this section, we describe differential-linear cryptanalysis. For a n-bit block cipher $E_r = E_{r_2} \circ E_{r_1}$ with $r = r_1 + r_2$ rounds, we apply an r_2-round linear approximation $(\alpha \to \beta)$ to E_{r_2} with a bias ϵ, and we apply an r_1-round differential $(\delta \to \Delta)$ to E_{r_1} with probability p, ($0 < p \le 1$) where $\delta \cdot \Delta = 0$. Then, we have

$$\begin{aligned}\beta \cdot \left(E_r(x) \oplus E_r(x \oplus \delta)\right) &= \alpha \cdot \left(E_{r_1}(x \oplus \delta) \oplus E_{r_1}(x)\right)\\ &\oplus \alpha \cdot E_{r_1}(x \oplus \delta) \oplus \beta \cdot E_r(x \oplus \delta)\\ &\oplus \alpha \cdot E_{r_1}(x) \oplus \beta \cdot E_r(x).\end{aligned}$$

If we assume that the round functions involved behave independently and that the two inputs $E_{r_1}(x)$ and $E_{r_1}(x \oplus \delta)$ of E_{r_2} behave as independent inputs with respect to the linear approximation, then when $\alpha \cdot (E_{r_1}(x \oplus \delta) \oplus E_{r_1}(x)) = 0$, the probability is

$$Pr\left(\beta \cdot \left(E_r(x) \oplus E_r(x \oplus \delta)\right)\right) = \frac{1}{2} + 2\epsilon^2.$$

For the other cases, we assume that the approximation is a random distribution and the probability is 1/2. Thus, we have the following.

$$\begin{aligned}Pr\left(\beta\cdot\left(E_r(x)\oplus E_r(x\oplus\delta)\right)=0\right)\\ &= p\times(1/2+2\epsilon^2)+(1-p)/2\\ &=1/2+2p\epsilon^2.\end{aligned}$$

If the bias is sufficiently large, the distinguisher can be used as the basis of a differential-linear attack to distinguish E_r from a random function. In general, the attack has a data complexity of $o(p^{-2}\epsilon^{-4})$.

In FES 2014, Celine and others [17] introduced a generalization of differential-linear cryptanalysis defined for multiple input differences and multidimensional linear output masks, which only relies on the independence of the two parts of the cipher. Denote the bias of a multidimensional differential-linear approximation as

$$\epsilon(U,W)=Pr(U^{\perp}/\{0\}\rightarrow W^{\perp})-1/|W|.$$

Theorem 1. Assume that the parts E_{r_1} and E_{r_2} of the block cipher $E_r=E_{r_2}\circ E_{r_1}$ are independent. Then,

$$\epsilon(U,W)=\frac{2}{|W|}\sum_{v\in\mathbb{F}_2^n/\{0\}}\epsilon(U,v)C(v,W), \tag{1}$$

where $\epsilon(U,v)=Pr\left(U^{\perp}/\{0\}\xrightarrow{E_{r_1}}sp(v)^{\perp}\right)-1/2,$ and $C(v,W)=\sum_{w\in W/\{0\}}Cor^2(v\cdot y\oplus w\cdot E_{r_2}(y))$ is the capacity of the multidimensional linear approximation with nonzero input mask *v* and all nonzero output masks *w* in the space *W*.

Using the linear attack framework [27]–[29], the data complexity of the multidimensional differential-linear distinguisher with input differences in $U^{\perp}$ and output masks in *W* is proportional to

$$\frac{2}{|U^{\perp}|}\frac{|W|^{-1}}{\epsilon^2(U,W)}=\frac{|W|}{2|U^{\perp}|}\frac{1}{\left(\sum_v\epsilon(U,v)C(v,W)\right)^2}. \tag{2}$$

Estimating (1) requires the estimation of $2^n|U|$ shorter differentials and $2^n|W|$ linear approximations, which is clearly infeasible in real cases. To solve this, Blondeau and others [24] suggested decomposing it into two sums with respect to a set $V\in\mathbb{F}_2^n$, that is,

$$\epsilon(U,W)=\frac{2}{|W|}\left(\sum_{v\in V/\{0\}}+\sum_{v\notin V}\epsilon(U,v)C(v,W)\right).$$

Under the following assumption, the bias of differential-linear approximation can be approximated by only considering a subspace *V* of $\mathbb{F}_2^n$.

Assumption 1. (Assumption 2 in [17]). Given a set *V*, we assume that

$$\left|\frac{2}{|W|}\sum_{v\in V/\{0\}}\epsilon(U,v)C(v,W)\,|\leq|\,\epsilon(U,W)\right|. \tag{3}$$

III. Several Distinguishers for Five Rounds of ARIA

In this section, we construct several differential-linear approximations over five rounds of ARIA, with two rounds of differentials and three rounds of linear hulls.

Constructing the Differential Characteristics. The two-round differential states that given a pair of (p,p') with nonzero differences in byte 7 and byte 13, the corresponding output differentials of byte 0 and byte 10 are equal after two rounds of ARIA, that is,

$$\Delta Z_2[0]=\Delta Z_2[10],$$

as shown in the upper part of Fig. 2. This can be deduced directly based on the properties of the DL layer.

Constructing the Linear Characteristics. The SL in the odd round is different from that in the even round, so we consider that the linear trails starts from the odd round. Let the input linear mask for the third round be $\overline{a}=(a,0,0,0;0,0,0,0;\ 0,0,a,0;0,0,0,0)$, the output masks of SL for the third round be $\overline{b}=(b,0,0,0;0,0,0,0;\ 0,0,b,0;0,0,0,0)$, the output masks of SL for the 4-th round be $\overline{c}=(0,0,c,0;\ c,c,0,0;0,c,0,0;0,0,c,c)$, and the output masks of SL for the 5-th round be $\overline{d}=(d,0,0,0;0,0,0,0;\ 0,0,d,0;0,0,0,0)$, where $a,b,c,d\in\mathbb{F}_2^8/\{0\}$. The square correlation of the linear hull $(\overline{a},\overline{d})$ can be computed by

$$\begin{aligned}C_{E_3}(\overline{a},\overline{d})&=\sum_{b,c\in\mathbb{F}_2^8/\{0\}}Cor_{\mathrm{SL1}}^2(\overline{a},\overline{b})Cor_{\mathrm{SL2}}^2(\overline{b},\overline{c})\\ &\qquad\times Cor_{\mathrm{SL1}}^2(\overline{c},\overline{d})\\ &=\sum_{b,c\in\mathbb{F}_2^8/\{0\}}Cor_{S_1}^2(a,b)Cor_{S_1}^2(b,a)Cor_{S_2}^4(b,c)\\ &\qquad\times Cor_{S_2}^2(c,b)Cor_{S_1}^4(c,b)Cor_{S_2}^2(b,c)\\ &\qquad\times Cor_{S_1}^2(c,d)Cor_{S_1}^2(d,c).\end{aligned}$$

Using the computer algorithm, for any $(\overline{a},\overline{d})$, we have

$$C_{E_3}(\overline{a},\overline{d})\approx 2^{-61.7},\ \sum_{d\in\mathbb{F}_2^n/\{0\}}C_{E_3}(\overline{a},\overline{d})\approx 2^{-53.7},$$

and

$$\sum_{a,d\in\mathbb{F}_2^n/\{0\}}C_{E_3}(\overline{a},\overline{d})=2^{-45.9}.$$

Let $U^{\perp}=\{(0,\ 0,\ 0,\ 0;\ 0,\ 0,\ 0,\ *;0,\ 0,\ 0,\ 0;\ 0,\ *,\ 0,\ 0)\}$ $W=\{(d,\ 0,\ 0,\ 0;\ 0,\ 0,\ 0,\ 0;\ 0,\ 0,\ d,\ 0;\ 0,\ 0,\ 0,\ 0)\}$, and $V=\{(a,\ 0,\ 0,\ 0;\ 0,\ 0,\ 0,\ 0;\ 0,\ 0,\ a,\ 0;\ 0,\ 0,\ 0,\ 0)\}$, where $d,a\in\mathbb{F}_2^n/\{0\}$ and $*$ denotes a nonzero byte, then we have

$$\sum_{v\in V/\{0\}}\epsilon(U,v)C(v,W)=2^{-46.9}.$$

By (1) and Assumption 1, to distinguish five rounds of ARIA from random permutations, the required data complexity is about

$$\frac{|2^8|-1}{2(2^{16}-1)}2^{93.8} \approx 2^{84.8}.$$

IV. Differential-Linear Attacks on Round-reduced ARIA

Consider the plaintexts p and p', which differ only at byte 7 and byte 13, and c and c' are the corresponding ciphertexts after five rounds of ARIA, respectively. We obtain 2^8-1 linear approximations:

$$\overline{d}_i \cdot c \oplus \overline{d}_i \cdot c' = 0, \quad \text{where} \quad d_i \in \mathbb{F}_2^n / \{0\}.$$

Then, by using the multidimensional linear cryptanalysis technique proposed in [30], a key recovery attack based on the differential-multidimensional linear distinguisher can be mounted on ARIA using a standard technique such as guessing k bits of the last round subkeys.

In brief, the framework of the χ^2 method is as follows. Let V_n denote the space of n-dimensional binary vectors. A function $g: V_n \rightarrow V_m$ with $g=(g_0, g_1, \dots, g_{m-1})$, where g_i is a linear approximation is called the vectorial linear approximation of dimension m.

Let p be the probability distribution of m-dimensional linear approximations. The capacity of $p=(p_0, \dots, p_{2^m-1})$ is defined by

$$C_p = \sum_{i=0}^{2^m-1} \frac{(p_i-u_i)^2}{u_i}, \qquad (4)$$

where $u=(u_0, \dots, u_{2^m-1})$ is a uniform distribution. It is well known that C_p is equal to the sum of the square of the correlations of all 2^m-1 linear approximations.

For $k \in (0,1,\dots,2^k-1)$, we obtain empirical probability distributions $Q_k=(q_{k,0},\dots,q_{k,2^m-1})$ by measuring the frequency of m-dimensional vectors, which are the Boolean values of m linear independent approximations. Then, the candidate keys are sorted according to their χ^2-statistics defined as

$$D(k) = 2^m \sum_{i=0}^{m} (q_{k,i}-2^{-m})^2, \qquad M=2^m-1,$$

which represent the l_2-distance of the Q_k from the uniform distribution.

If the right key is ranked in position d from the top among 2^d key candidates, we say that the attack has an advantage of (l − $\log_2 d$) [31]. The advantage of the χ^2-method using statistic (4) is derived in Theorem 1 [30] by

$$d = \frac{\left(NC_p - 4\Phi^{-2}(2P_s-1)\right)^2}{4M},$$

where P_s is the probability of success, N is the amount of data, C_p is the capacity, $M=2^m-1$ is the number of linear approximations, and

$$\Phi(x) = \int_{-\infty}^{x} \frac{1}{2\sqrt{\pi}} e^{t^2/2} \mathrm{d}t.$$

1. Six-Round Attack

Based on the five rounds of differential-linear approximations, which start from the first round and end at the fifth round, we present some key-recovery attacks on six-round ARIA-128. One round is appended after the differential-linear approximates, as shown in Fig. 3. The partial decryptions using the partial sum technique proceed as follows.

1. Define a structure of 2^{16} plaintexts, where $p[7, 13]$ take all the possible 2^{16} values and the remaining 14 bytes are fixed to some constants. Therefore, we can generate $2^{16} \times (2^{16}-1)/2 \approx 2^{31}$ plaintext pairs using a structure and each of them satisfies the plaintext difference. Request the

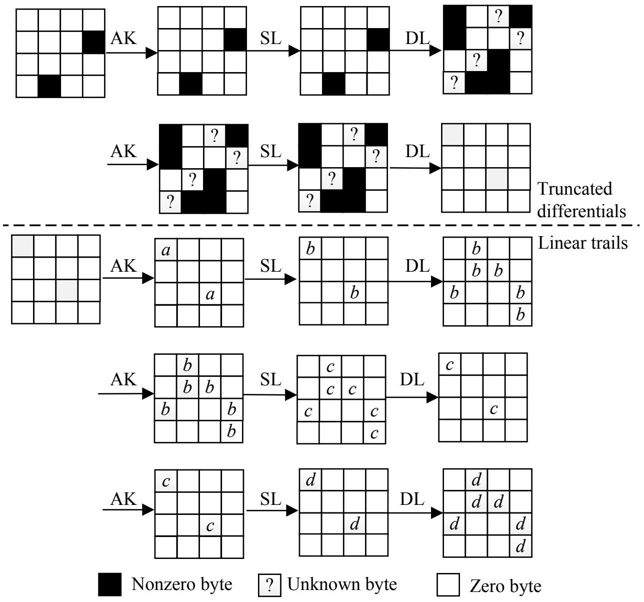


Fig. 2. Differential-linear approximations for five-round ARIA.

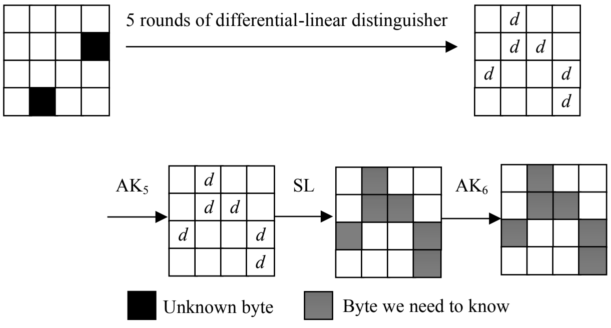


Fig. 3. Differential-linear attack on six-round ARIA-128.

encryption of N structures to find $N2^{31}$ message pairs.

2. Allocate 8-bit counters $V_1[x_1]$ for 2^{96} possible values of $x_1 = c[2,4,5,9,14,15] \,||\, c'[2,4,5,9,14,15]$ and initialize them as zero. For the corresponding ciphertext pairs after six rounds of encryption, extract the value of x_1 and increase the corresponding counter $V_1[x_1]$. The required time complexity of this is $N \times 2^{15}$ memory accesses in order to process the chosen plaintext-ciphertext pairs. If we assume that processing each memory access is equivalent to one round of encryption, then the time complexity of this step is about $N \times 2^{15}$ one-round encryptions.
3. Allocate a counter $V_2[x_2]$ for 2^{88} possible values of $x_2 = c[4,5,9,14,15] \,||\, c'[4,5,9,14,15] \,||\, I^1$ and initialize them as zero. Guess $k_6[2]$ and partially decrypt x_1 to obtained the value of x_2; that is, compute
$$I^1 = S_1^{-1}\left(c[2] \oplus k_6[2]\right) \oplus S_1^{-1}\left(c'[2] \oplus k_6[2]\right),$$
and then update the corresponding counter by $V_2[x_2]$ + = $V_1[x_1]$. The computation requires about $2^{96} \times 2^{8}$ one-round encryptions.
4. Allocate a counter $V_3[x_3]$ for 2^{72} possible values of $x_3 = c[5,9,14,15] \,||\, c'[5,9,14,15] \,||\, I^2$ and initialize them as zero. Guess $k_6[4]$ and partially decrypt x_2 to obtain the value of x_3; that is, compute
$$I^2 = I^1 \oplus S_1\left(c[4] \oplus k_6[4]\right) \oplus S_1\left(c'[4] \oplus k_6[4]\right),$$
and then update the corresponding counter by $V_3[x_3]$ + = $V_2[x_2]$. The computation requires about $2^{88} \times 2^{16}$ one-round encryptions.
5. Allocate a counter $V_4[x_4]$ for 2^{56} possible values of $x_4 = c[9,14,15] \,||\, c'[9,14,15] \,||\, I^3$ and initialize them as zero. Guess $k_6[5]$ and partially decrypt x_3 to obtain the value of x_4; that is, compute
$$I^3 = I^2 \oplus S_2(c[5] \oplus k_6[5]) \oplus S_2(c'[5] \oplus k_6[5]),$$
and then update the corresponding counter by $V_4[x_4]$ + = $V_3[x_3]$. The computation requires about $2^{72} \times 2^{24}$ one-round encryptions.
6. Allocate a counter $V_5[x_5]$ for 2^{40} possible values of $x_5 = c[14,15] \,||\, c'[14,15] \,||\, I^4$ and initialize them as zero. Guess $k_6[9]$ and partially decrypt x_4 to obtain the value of x_5; that is, compute
$$I^4 = I^3 \oplus S_2\left(c[9] \oplus k_6[9]\right) \oplus S_2\left(c'[9] \oplus k_6[9]\right),$$
and then update the corresponding counter by $V_5[x_5]$ + = $V_4[x_4]$. The computation requires about $2^{56} \times 2^{32}$ one-round encryptions.
7. Allocate a counter $V_6[x_6]$ for 2^{24} possible values of $x_6 = c[15] \,||\, c'[15] \,|\, I^5$ and initialize them as zero. Guess $k_6[14]$ and partially decrypt x_5 to obtain the value of x_6; that is, compute
$$I^5 = I^4 \oplus S_1^{-1}\left(c[14] \oplus k_6[14]\right) \oplus S_1^{-1}\left(c'[14] \oplus k_6[14]\right),$$
and then update the corresponding counter by $V_6[x_6]$ + = $V_5[x_5]$. The computation requires about $2^{40} \times 2^{40}$ one-round encryptions.
8. Allocate a counter $V_7[x_7]$ for 2^8 possible values of $x_7 = I^6$ and initialize them as zero. Guess $k_6[15]$ and partially decrypt x_6 to obtain the value of x_7; that is, compute
$$I^6 = I^5 \oplus S_2^{-1}\left(c[15] \oplus k_6[15]\right) \oplus S_2^{-1}\left(c'[15] \oplus k_6[15]\right),$$
and then update the corresponding counter by $V_7[x_7]$ + = $V_6[x_6]$. The computation requires about $2^{24} \times 2^{48}$ one-round encryptions.
9. Allocate a counter vector $V_8[z]$. For 2^8 values of x_7, evaluate eight basis linear masks on x_7 and add the evaluations to the vector z, before adding the corresponding $V_8[z]$:$V_8[z]$ + = $V_7[x_7]$. Compute
$$T = 2^8 \sum_{z=0}^{2^8-1} \left(\frac{V_8[z]}{2^{15}N} - \frac{1}{2^8} \right)^2 .$$
10. Allocate a counter vector $V_9[k]$, repeat Step 2 through Step 8 for all of the guessed keys, compute T_k, and store it in $V_9[k]$. Sort the candidate keys according to the value of $V_9[k]$ and search for the right key from the top of the sorted keys.

Let d = 32 be the advantage of the attack and P_s = 0.75 be the probability of success. The capacity of the five-round differential-linear characteristic is $2^{-45.9}$. The number of pairs required is about $2^{99.4}$. The data complexity required for the attack is about $2^{84.4}$ chosen plaintexts.

In total, 48-bit key values are guessed during the encryption phase and only 2^{16} key candidates survive after incorrect key filtration. The complexity of Step 2 is about $2^{112.8}$ six-round encryptions. The total complexity of Step 3 through Step 8 is no more than $2^{101.4}$ six-round encryptions. The total data complexity is about $2^{83.1}$ chosen plaintexts, the time complexity is about $2^{112.8}$ six-round encryptions, and the memory requirement is about 2^{96} bytes for counters.

2. Seven-Round Attack

We can append two rounds after the five-round differential-linear approximations, as shown in Fig. 4. Similar to the six-round attacks, let d = 48 be the advantage of the attack and P_s = 0.75 is the probability of success. The data complexity

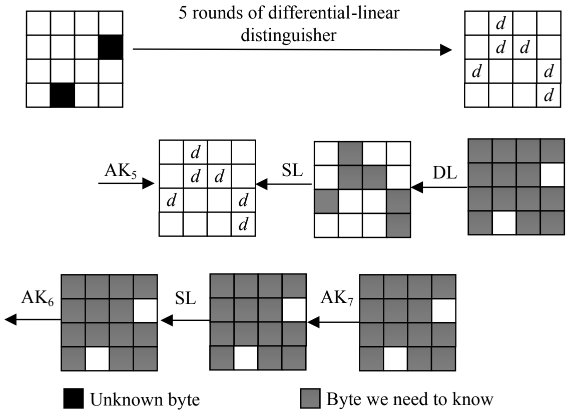


Fig. 4. Differential-linear attack on seven-round ARIA-256.

required for the attack is about $2^{84.6}$ chosen plaintexts. The time complexity is about $2^{215.3}$ seven-round encryptions and the memory requirement is about 2^{224} bytes for counters.

V. Conclusion

In this study, we applied multidimensional differential-linear cryptanalysis to evaluate the security of the block cipher ARIA, which is the first application of the new technique since it was introduced in FES 2014. We presented a six-round attack on ARIA-128 and a seven-round attack on ARIA-256, which have lower data complexity than previous attacks. The key features of our five-round multidimensional differential-linear distinguishers are the special properties of truncated differential and multi-linear hull approximations of the ARIA block cipher. From this viewpoint, multidimensional differential-linear cryptanalysis can be treated as an improved version of linear hull attacks. The attacks described in the present study are preliminary attempts and the first investigation of the strength of ARIA against differential-linear cryptanalysis. We suggest that further research should consider differential-linear cryptanalysis of ARIA.

References

[1] D. Kwon et al., “New Bock Cipher: ARIA,” *Proc. Int. Conf. Inform. Security Cryptology*, Seoul, Rep. of Korea, Nov. 27–28, 2003, pp. 432–445.

[2] National Security Research Institute: Specification of ARIA, version 1.0, January 2005. http://www.nsri.re.kr/ARIA/doc/ARIAspecification-e.pdf

[3] Korean Agency for Technology and Standards (KATS): 128 bit Block Encryption Algorithm ARIA, *KS X 1213:2004*, Dec. 2004.

[4] D. Kwon et al., *A Description of the ARIA Encryption Algorithm. RFC 5794*, Mar. 2010. https://tools.ietf.org/html/rfc5794

[5] W. Kim et al., *Addition of the ARIA Cipher Suites to Transport Layer Security (TLS). RFC 6209*, Apr. 2011. https://tools.ietf.org/html/rfc6209

[6] RSA Laboratories, Additional PKCS \#11 Mechanisms, *PKCS \#11 v2.20 Amendment, Revision 1, 2007.*

[7] P. Li, B. Sun, and C. Li, “Integral Cryptanalysis of ARIA,” *Int. Conf. Inscrypt*, Beijing, China, Dec. 12–15, 2009, pp. 1–14.

[8] Y. Li, W. Wu, and L. Zhang, “Integral Attacks on Reduced-round ARIA Block Cipher,” *Proc. ISPEC*, Seoul, Rep. of Korea, May 12–13, 2010, pp. 19–29.

[9] E. Fleischmann et al., “New Boomerang Attacks on ARIA,” *Int. Conf. Cryptology India*, Hyderabad, India, Dec.12–15, 2010, pp. 163–175.

[10] X. Tang et al., “A Meet-in-the-Middle Attack on Reduced Round ARIA,” *J. Syst. Softw.*, vol. 84, no. 10, Oct. 2011, pp. 1685–1692.

[11] T. Akshima et al., “Improved Meet-in-the-Middle Attacks on 7 and 8-Round ARIA-192 and ARIA-256,” *Int. Conf. Cryptology India*, Bangalore, India, Dec. 6–9, 2015, pp. 198–217.

[12] X. Bai et al., “Improved Meet-in-the-Middle Attacks on Round-reduced ARIA,” *Int. Conf. ISC*, Dallas, TX, USA, Nov. 13–15, 2013, pp. 155–168.

[13] W. Wu, W. Zhang, D. Feng, “Impossible Differential Cryptanalysis of Reduced Round ARIA and Camellia,” *J. Comput. Sci. Technol.*, vol. 22, no. 3, May 2007, pp. 449–456.

[14] R. Li et al., *New Impossible Differential Cryptanalysis of ARIA.* http://eprint.iacr.org/2008/227

[15] C. Du and J. Chen, “Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds,” *Int. Conf. CANS*, Kuala Lumpur, Malaysia, Dec. 12–14, 2010, pp. 20–30.

[16] W. Yi, S. Chen, and K. Wei, “Zero-Correlation Linear Cryptanalysis of Reduced Round ARIA with Partial-sum and FFT,” *Trans. Internet Inform. Syst.*, vol. 9, no. 1, 2015, pp. 280–295.

[17] S. Chen and T. Xu, “Biclique Attack of the Full ARIA-256,” *IET Inform. Security*, vol. 8, no. 5, 2014, pp. 259–264.

[18] S. Langford and M.E. Hellman, “Differential-Linear Cryptanalysis,” *Advances in Cryptology — CRYPTO ’94*, vol. 839, Heidelberg, Berlin; Springer, pp. 17–25.

[19] E. Biham, O. Dunkelman, and N. Keller, “Enhancing Differential-linear Cryptanalysis,” *Advances in Cryptology — ASIACRYPT 2002*, vol. 2501, Heidelberg, Berlin; Springer, pp. 254–266.

[20] S. Langford, “Differential-Linear Cryptanalysis and Threshold Signatures,” Ph.D. Thesis, 1995.

[21] Z. Liu et al., “Differential-Multiple Linear Cryptanalysis,” *Int. Conf. Inscrypt*, Beijing, China, Dec. 12–15, 2009, pp. 35–49.

[22] J. Lu, “A Methodology for Differential-Linear Cryptanalysis and its Applications,” *Proc. Fast Software Encryption*, vol. 7549, Heidelberg, Berlin; Springer, pp. 69–89.

[23] D. Wagner, “Towards a Unifying View of Block Cipher Cryptanalysis,” *Proc. FSE 2004*, vol. 3017, Heidelberg, Berlin;

Springer, pp.16–33.

[24] C. Blondeau, G. Leander, and K. Nyberg, "Differential-Linear Cryptanalysis Revisited," *Int. Workshop FSE*, London, UK, Mar. 3–5, 2014, pp. 411–430.

[25] B. Sun et al., "Provable Security Evaluation of Structures Against Impossible Differential and Zero Correlation Linear Cryptanalysis," *Proc. EUROCRYPT 2016*, vol. 9665, pp. 196–213.

[26] B. Sun et al., "New Insights on the AES-like SPN Ciphers," *Proc. CRYPTO 2016*, vol. 9814, pp. 605–624.

[27] C. Blondeau et al., "Accurate Estimates of the Data Complexity and Success Probability for Various Cryptanalysis," *Annu. Int. Conf. Theory Applicat. Cryptographic Techn.*, Vienna, Austria, May 8–12, 2016, pp. 31–34.

[28] A. Bogdanov et al., "On the Wrong Key Randomization and Key Equivalence Hypothesis in Matsui's Algorithm 2," *Int. Workshop FSE*, Singapore, Mar. 11–13, 2013, pp. 19–38.

[29] A. Selcuk, "On Probability of Success in Linear and Differential Cryptanalysis," *J. Cryptoloy*, vol. 21, no. 1, Jan. 2008, pp. 131–147.

[30] M. Hermelin, J.Y. Cho, and K. Nyberg, "Multidimensional Extension of Matsui's Algorithm 2," *Proc. Fast Softw. Encyption*, vol. 5665, Heidelberg, Berlin: Springer, pp. 209–227.

[31] K. Paterson, "On Linear Hulls, Statistical Saturation Attacks, Present and a Cryptanalysis of Puffin," *Adv. Cryptology – EUROCRYPT*, vol. 6632, Heidelberg, Berlin: Springer, pp. 303–322.

Wentan Yi was born in 1989. He is currently a PhD candidate at the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China. His main research interest is the analysis of block ciphers.

Jiongjiong Ren was born in 1994. He is currently pursuing a PhD degree at the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China. His main research interest is the analysis of block ciphers.

Shaozhen Chen was born in 1965. Currently, she is a professor at the State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou, China. Her research interests are cryptography and information security.