Chinese Journal of Electronics
vol. 33, no. 3, pp. 683–693, May 2024
https://doi.org/10.23919/cje.2022.00.383

RESEARCH ARTICLE

New Related-Tweakey Boomerang Attacks and Distinguishers on Deoxys-BC

Jiamei LIU, Lin TAN, and Hong XU

PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China

Corresponding author: Lin TAN, Email: tanlin100@163.com
Manuscript Received November 9, 2022; Accepted March 22, 2023

Abstract — Deoxys-BC is the primitive tweakable block cipher of the Deoxys family of authenticated encryption schemes. Based on existing related-tweakey boomerang distinguishers, this paper improves the boomerang attacks on 11-round Deoxys-BC-256 and 13-round Deoxys-BC-384 by the optimized key guessing and the precomputation technique. It transfers a part of subtweakey guess in the key-recovery phase to the precomputation resulting in a significant reduction of the overall time complexity. For 11-round Deoxys-BC-256, we give a related-tweakey boomerang attack with time/data/memory complexities of $2^{218.6}/2^{125.7}/2^{125.7}$, and give another attack with the less time complexity of $2^{215.8}$ and memory complexity of 2^{120} when the adversary has access to the full codebook. For 13-round Deoxys-BC-384, we give a related-tweakey boomerang attack with time/data/memory complexities of $2^{k-96}+2^{157.5}/2^{120.4}/2^{113}$. For the key size $k=256$, it reduces the time complexity by a factor of 2^{31} compared with the previous 13-round boomerang attack. In addition, we present two new related-tweakey boomerang distinguishers on 11-round Deoxys-BC-384 with the same probability as the best previous distinguisher.
Keywords — Block cipher, Tweakable block cipher, Boomerang attack, Related-tweakey.
Citation — Jiamei LIU, Lin TAN, and Hong XU, "New Related-Tweakey Boomerang Attacks and Distinguishers on Deoxys-BC," *Chinese Journal of Electronics*, vol. 33, no. 3, pp. 683–693, 2024. doi: 10.23919/cje.2022.00.383.

I. Introduction

Authenticated encryption (AE) is an encryption approach that addresses confidentiality and authenticity at the same time. During recent years, AE have attracted increasing attention of the cryptography associations, such as CAESAR Competition [1] and NIST Lightweight Cryptography AEAD (authenticated encryption with associated data) Project [2]. Tweakable block cipher was proposed by Liskov *et al.* in [3]. Besides the inputs of plaintext and key, it takes an additional input called tweak. In [4], a new TWEAKEY framework was proposed to design tweakable block ciphers, which uses a unified view of the key and tweak denoted as tweakey. The tweakable block cipher Deoxys-BC is designed following the TWEAKEY framework and uses the AES round function. Deoxys-BC is the primitive of the AE scheme Deoxys [5], in which Deoxys-II was selected as the primary choice in the final portfolio of the CAESAR Competition for the "Defense in depth" category.

Boomerang attack [6] is an extension of the differential attack. It allows the adversary to concatenate two short differential paths to get a longer distinguisher. The boomerang attack can be converted to the amplified boomerang attack [7] and rectangle attack [8]. The related-key boomerang and rectangle attacks were proposed in [9], which are powerful for cryptanalysis of many block ciphers such as KASUMI [10], [11], AES [12], SKINNY [13], [14], GIFT [15] and Deoxys-BC [16]–[21]. In [16], Cid *et al.* gave the first third-party analysis of Deoxys-BC. They proposed a method to search the related-tweakey (RK) boomerang distinguishers, and attacked 10-round Deoxys-BC-256 and 13-round Deoxys-BC-384. In [17], Sasaki reduced the complexities of the boomerang attacks by a structural technique. In [18], Cid *et al.* proposed a tool named Boomerang Connectivity Table (BCT) to evaluate the boomerang probability of S-box, and improved the probability of the boomerang distinguisher on 10-round Deoxys-BC-384. In [19], a new tool named Boomerang Difference Table (BDT) was proposed, which was used to increase the probability of the 9-round boomerang distinguisher on Deoxys-BC-256. In [20], Zhao *et al.* improved the related-tweakey boomerang and rectangle attacks on round-reduced Deoxys-BC, which were improved

Associate Editor: Prof. Jianfeng MA, Guizhou University.

by themselves in [21]. In [13], Dong *et al.* improved the key guessing strategies in the rectangle attacks on the linear key-schedule ciphers and improved the related-tweakey rectangle attack on 14-round Deoxys-BC-384. Later, Song *et al.* [22] proposed a unified and generic framework for optimizing rectangle attack, and improved related-key boomerang and rectangle attacks on 11-round Deoxys-BC-256. Besides, these are some security evaluations of Deoxys-BC against the impossible differential attacks [23], [24] and meet-in-the-middle (MITM) attacks [25]–[27].

In this paper, we improve the related-tweakey boomerang attacks on 11-round Deoxys-BC-256 and 13-round Deoxys-BC-384 by the optimized key guessing and the precomputation technique. It transfers a part of subtweakey guess in the key-recovery phase to the precomputation resulting in a significant reduction of the overall time complexity. In addition, we present two new related-tweakey boomerang distinguishers on 11-round Deoxys-BC-384 with the same probability as the best previous distinguisher in [21]. The summary of main cryptanalysis results of Deoxys-BC is listed in Table 1.

Table 1 Summary of main cryptanalysis results of Deoxys-BC (MITM denotes meet-in-the-middle; RK denotes related-tweakey)

Version	Rounds	Approach	Time	Data	Memory	Key size	Ref.
256	9	MITM	$2^{113.6}$	2^{108}	2^{102}	$k > 113$	[25]
	10	Impossible differential	$2^{173.1}$	2^{135}	2^{64}	$k > 173$	[24]
	10	RK boomerang	2^{170}	2^{98}	2^{98}	$k > 170$	[17]
	10	RK boomerang	$2^{109.1}$	$2^{98.4}$	2^{88}	$k = 128$	[20]
	11	RK rectangle	$2^{249.9}$	$2^{122.1}$	$2^{128.2}$	$k > 252$	[20]
	11	RK rectangle	$2^{222.49}$	$2^{126.78}$	2^{128}	$k > 222$	[22]
	11	RK boomerang	$2^{222.5*}$	$2^{126.2*}$	2^{128}	$k > 222$	[22]
	11	RK boomerang	$2^{218.6}$	$2^{125.7}$	$2^{125.7}$	$k > 218$	Sect. III.2
	11	RK boomerang	$2^{215.8}$	2^{130}	2^{120}	$k > 215$	Sect. III.3
384	11	MITM	2^{251}	2^{113}	2^{226}	$k > 256$	[26]
	12	RK boomerang	2^{148}	2^{100}	2^{100}	$k = 256$	[17]
	12	RK boomerang	2^{98}	2^{98}	2^{64}	$k = 128$	[20]
	13	RK rectangle	2^{270}	2^{127}	2^{144}	$k > 270$	[16]
	13	RK rectangle	$2^{186.7}$	$2^{125.2}$	2^{136}	$k = 256$	[21]
	13	RK boomerang	$2^{191.3}$	2^{125}	2^{136}	$k = 256$	[20]
	13	RK boomerang	$2^{157.5} + 2^{k-96}$	$2^{120.4}$	2^{113}	$k > 157$	Sect. IV
	14	RK rectangle	2^{260}	$2^{125.2}$	2^{140}	$k > 260$	[13]

Note: *The time and data complexities are corrected from $2^{218.65}$ and $2^{122.4}$, respectively. In [22], the calculation of the number of ciphertext pairs is wrong when the number of structures $y < 1$. In this case, the parameter $r_f = 128$. From $y \cdot 2^{128}$ ciphertexts, there are $y^2 \cdot 2^{256}$ pairs obtained, which is less than $y \cdot 2^{256}$ given in [22] for $y < 1$. For one expected right quartet, the parameters are corrected by $y = 2^{-3.8}$ and $D = 2^{124.2}$, which are used for the complexity computation in [22].

The organization of this paper is as follows. In Section II, we recall the specification of Deoxys-BC and the boomerang attacks. In Section III, two related-tweakey boomerang attacks on 11-round Deoxys-BC-256 are given. In Section IV, the improved related-tweakey boomerang attack on 13-round Deoxys-BC-384 is given. In Section V, we present two new related-tweakey boomerang distinguishers on 11-round Deoxys-BC-384, and conclude this paper in Section VI.

II. Preliminaries

1. Description of Deoxys-BC

Deoxys-BC is an AES-based tweakable block cipher. According to the TWEAKEY framework [4], the tweakey $KT = K \parallel T$ is used to provide a unified view of the key K and the tweak T for Deoxys-BC. Deoxys-BC-n has 128-bit block and n-bit tweakey, $n = 256, 384$. The key size and tweak size can vary as long as the key size $k \geq 128$. The number round r is 14 for Deoxys-BC-256 and 16 for Deoxys-BC-384. The state of Deoxys-BC is viewed as a 4×4 matrix of bytes where the index is as

$$\begin{pmatrix} 0 & 4 & 8 & 12 \\ 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \end{pmatrix}$$

Deoxys-BC uses the AES round function [28], consisting of the following four operations.

- AddRoundTweakey (AK): XOR an 128-bit round subtweakey to the internal state.
- SubBytes (SB): Apply the 8-bit S-box to each of the 16 bytes of the internal state separately.
- ShiftRows (SR): Rotate the i-th row left by i posi-

tions, $i = 0, 1, 2, 3$.

- MixColumns (MC): Multiply the internal state by the 4×4 MDS matrix over the finite field GF(2^8).

After the last round, an additional AK operation is performed to produce the ciphertext. The subtweakeys are generated from the tweakey KT by a special key schedule algorithm. For more details on Deoxys-BC, readers can refer to [5].

Notations STK_i: the i-th round subtweakey;

IK_i: the equivalent subtweakey of STK_i, that is $\mathrm{IK}_i = \mathrm{SR}^{-1} \circ \mathrm{MC}^{-1}(\mathrm{STK}_i)$;

X_i: the state before SB operation in the i-th round;

Y_i: the state after SB operation in the i-th round;

Z_i: the state after adding the equivalent subtweakey IK_{i+1} in the i-th round;

W_i: the state after SR operation in the i-th round;

$X[j]$: the j-th byte of the state $X, 0 \le j \le 15$.

Then internal states propagation in the i-th round can be represented as follows:

$$X_i \xrightarrow{\mathrm{SB}} Y_i \xrightarrow[\mathrm{IK}_{i+1}]{AK} Z_i \xrightarrow{\mathrm{SR}} W_i \xrightarrow{\mathrm{MC}} X_{i+1}$$

2. Boomerang attacks

Boomerang attack proposed by Wagner [6] is an extension of differential attack in the adaptive chosen plaintext and ciphertext setting. The adversary decompose the function E into two parts $E = E_1 \circ E_0$. There exits a differential $\alpha \to \beta$ with probability p for E_0 and a differential $\gamma \to \delta$ with probability q for E_1. Then the two differentials can be combined into a boomerang distinguisher on E. The probability of the boomerang distinguisher can be estimated by

$$\Pr[E^{-1}(E(x) \oplus \delta) \oplus E^{-1}(E(x \oplus \alpha) \oplus \delta) = \alpha] = p^2 q^2$$

As it was pointed out in [7] and [8], when α and δ are fixed, β and γ can be any possible values as long as $\beta \ne \gamma$. Then the probability of the boomerang distinguisher can be increased to $\hat{p}^2 \hat{q}^2$, where

$$\hat{p} = \sqrt{\sum_i \Pr^2(\alpha \to \beta_i)}, \quad \hat{q} = \sqrt{\sum_j \Pr^2(\gamma_j \to \delta)}$$

The related-key boomerang attack was proposed by Biham *et al.* [9], as Figure 1. Assume one has a related-key differential $\alpha \to \beta$ over E_0 under a key difference ΔK with a probability p and another related-key differential $\gamma \to \delta$ over E_1 under a key difference ∇K with a probability q. Let K_1, K_2, K_3 and K_4 be four related keys, where $K_2 = K_1 \oplus \Delta K$, $K_3 = K_1 \oplus \nabla K$, $K_4 = K_1 \oplus \Delta K \oplus \nabla K$. The related-key boomerang distinguisher is used as follows:

1) Randomly choose a plaintext pair (P_1, P_2) statisfied $P_1 \oplus P_2 = \alpha$, and query the encryption oracle under the keys K_1, K_2 to get the corresponding ciphertext pair (C_1, C_2).

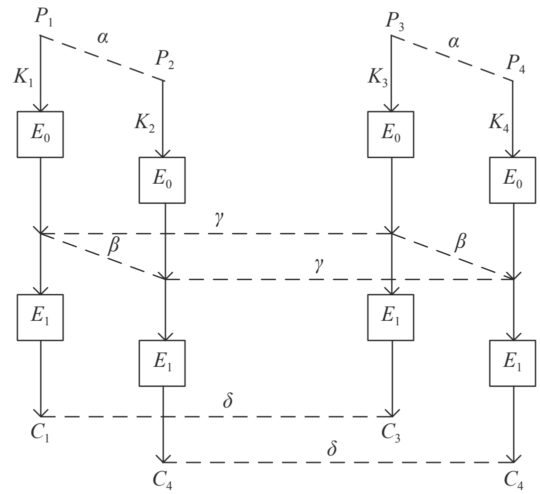

Figure 1 Related-key boomerang distinguisher.

2) Compute (C_3, C_4) by $C_3 = C_1 \oplus \delta$ and $C_4 = C_2 \oplus \delta$, and query the decryption oracle under the keys K_3, K_4 to obtain the corresponding palintext pair (P_3, P_4).

3) Check whether $P_3 \oplus P_4 = \alpha$ or not. If yes, a right quartet (P_1, P_2, P_3, P_4) is obtained, otherwise return to step 1).

A boomerang distinguisher can be converted to a distinguisher in the chosen plaintext or ciphertext setting, the amplified boomerang [7] and rectangle [8], with the probability of $2^{-n}\hat{p}^2\hat{q}^2$, where n is the block size of a cipher.

Success probability The success probability of boomerang attack with an h-bit advantage is evaluated as [20] and [29] by

$$P_s = \Phi\left(\frac{\sqrt{sS_N} - \Phi^{-1}(1 - 2^{-h})}{\sqrt{S_N + 1}}\right)$$

where $S_N = \hat{p}^2\hat{q}^2/2^{-n}$ is the signal-to-noise ratio and s is the expected number of right quartets.

III. Boomerange Attacks on 11-Round Deoxys-BC-256

In [20], Zhao *et al.* gave a 9-round boomerang distinguisher on Deoxys-BC-256 with the probability $2^{-120.4}$, where α = (00 b0 00 00 00 c0 00 00 7b 00 af 0000 00 00 c2), δ = (00 00 00 00 f2 0d ff f2 8f 7b 8a 05 00 0084 00). They attacked 11-round Deoxys-BC-256 by using the first 8-round path of the 9-round distinguisher. In this section, we use the 9-round distinguisher to present an 11-round related-tweakey attack on Deoxys-BC-256 as Figure 2, with the time complexity of $2^{218.6}$. The details of the differential characteristic of the boomerang distinguisher can refer to [20]. In addition, when the adversary has access to full codebook, we present another 11-round boomerang attack on Deoxys-BC-256 with less time complexity. Since MC and SR do not impact the cryptanalysis, for simplicity, we denote $SR^{-1} \circ MC^{-1}(C)$ by the

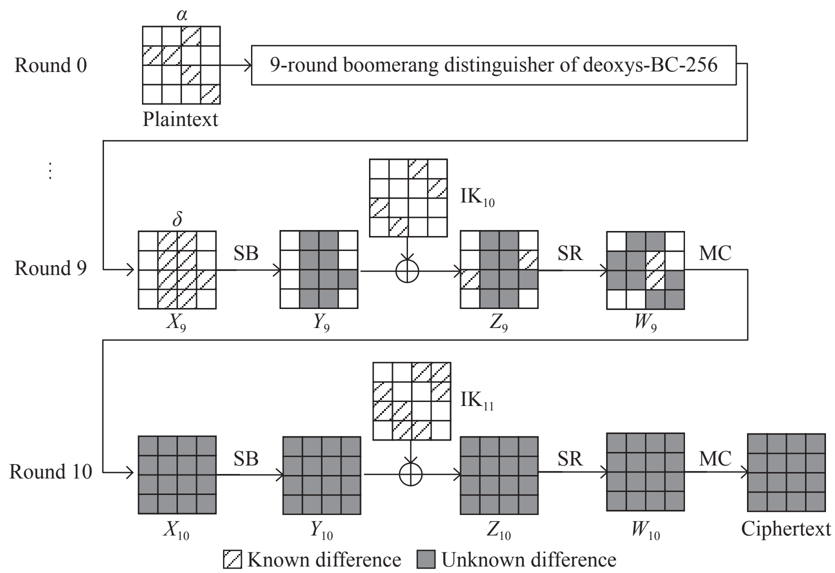

Figure 2 Related-tweakey boomerang attack on 11-round Deoxys-BC-256.

ciphertext C in the last round.

1. Precomputation

We precompute two tables. The first precomputed table T_1 of size 2^{112} is constructed as follows.

1) For each of 2^{48} values of $\mathrm{IK}_{11}[8,9,10,11]$ and $\mathrm{IK}_{10}[7,8]$,

2) For each of 2^{32} values of $X_9[7,8]$ and $W_9[9,10]$, compute the values of the third column of Z_{10} under the related keys K_1, K_2, denoted by z_1, z_2. Then compute the corresponding z_3, z_4 under K_3, K_4 after XORing the known differences $\Delta X_9[7,8]=(\mathrm{f2},\ \mathrm{8f}), \Delta W_9[9,10]=(\mathrm{7f},\mathrm{ef})$. Then store (z_1,z_3) and (z_2,z_4) in the sets L_1 and L_2, respectively.

3) For each (z_1,z_3) in L_1 and each (z_2,z_4) in L_2, store the value of $\mathrm{IK}_{11}[8,9,10,11]$ and $\mathrm{IK}_{10}[7,8]$ in the table T_1 indexed by (z_1,z_2,z_3,z_4).

To prepare the table T_1, it needs memory complexity of $2^{48+64}=2^{112}$ and time complexity of 2^{112} memory accesses. For any (z_1,z_2,z_3,z_4), there are $2^{112-128}=2^{-16}$ key candidates on average suggested by T_1.

The second precomputed table T_2 of size 2^{120} is constructed similarly.

1) For each of 2^{56} values of $\mathrm{IK}_{11}[4,5,6,7]$ and $\mathrm{IK}_{10}[4,9,14]$,

2) For each of 2^{32} values of $X_9[4,9,14]$ and $W_9[7]$, compute the values of the second column of Z_{10} under the related keys K_1, K_2, denoted by z_1, z_2. Then compute the corresponding z_3, z_4 under K_3, K_4 after XORing the known differences $\Delta X_9[4,9,14]=(\mathrm{f2},\mathrm{7b},84)$, $\Delta W_9[7]=0$. Then, store (z_1,z_3) and (z_2,z_4) in the sets L_1 and L_2 respectively.

3) For each (z_1,z_3) in L_1 and each (z_2,z_4) in L_2, store the value of $\mathrm{IK}_{11}[4,5,6,7]$ and $\mathrm{IK}_{10}[4,9,14]$ in the table T_2 indexed by (z_1,z_2,z_3,z_4).

To prepare the table T_2, it needs memory complexity of $2^{56+64}=2^{120}$ and time complexity of 2^{120} memory accesses. For any (z_1,z_2,z_3,z_4), there are $2^{120-128}=2^{-8}$ key candidates on average suggested by T_2.

2. Attack on 11-round Deoxys-BC-256

After preparing the two precomputed tables T_1 and T_2, we give the detail of the key recovery attack on 11-round Deoxys-BC-256.

Data collection Choose 2^t plaintext pairs (P_1,P_2) satisfying $P_1\oplus P_2=\alpha$, denoted by the set S. Query the corresponding ciphertexts under the four related keys K_1, K_2, K_3 and K_4, and construct the following two sets of size 2^t.

$$
\begin{aligned}
S_1=\{&(P_1,C_1,P_2,C_2)\mid(P_1,P_2)\in S,\\
&C_1=E_{K_1}(P_1),C_2=E_{K_2}(P_2)\}
\end{aligned}
$$

$$
\begin{aligned}
S_2=\{&(P_3,C_3,P_4,C_4)\mid(P_3,P_4)\in S,\\
&C_3=E_{K_3}(P_3),C_4=E_{K_4}(P_4)\}
\end{aligned}
$$

Key recovery Guess 12-byte $\mathrm{IK}_{11}[0,1,2,3,12,13,14,15]$ and $\mathrm{IK}_{10}[5,6,10,11]$, then carry out the following process.

1) Initialize a list of 2^{104} counters, each of with corresponding to a 13-byte $\mathrm{IK}_{11}[4,5,6,7,8,9,10,11]$ and $\mathrm{IK}_{10}[4,7,8,9,14]$.

2) For each $(P_1,C_1,P_2,C_2)\in S_1$, partially decrypt (C_1,C_2) to obtain the values of $W_9[0,3,12,13]$ and $X_9[5,6,10,11]$, denoted by (w_1,x_1,w_2,x_2). Then store (P_1,C_1,P_2,C_2) into a hash table H indexed by (w_1,x_1,w_2,x_2).

3) For each $(P_3,C_3,P_4,C_4)\in S_2$, partially decrypt (C_3,C_4) to obtain the corresponding (w_3,x_3,w_4,x_4). Since $\Delta W_9[0,3,12,13]=0$ and $\Delta X_9[5,6,10,11]=(\mathrm{0d},\mathrm{ff},\mathrm{8a},05)$, we construct the quartets (C_1,C_2,C_3,C_4) by looking up the hash table H with the index $(w_3,x_3\oplus(\mathrm{0d},\mathrm{ff},\mathrm{8a},05)$, $w_4,x_4\oplus(\mathrm{0d},\mathrm{ff},\mathrm{8a},05))$. There are about 2^{2t-128} quartets.

4) For each of 2^{2t-128} quartets, lookup the precomputed table T_1 to find the candidates of $\mathrm{IK}_{11}[8,9,10,11]$

and $\mathrm{IK}_{10}[7,8]$. Since T_1 provides a filter of 2^{-16}, there are about 2^{2t-144} quartets remaining. Then lookup T_2 to find the candidates of $\mathrm{IK}_{11}[4,5,6,7]$ and $\mathrm{IK}_{10}[4,9,14]$. If an 104-bit key candidate involved is suggested, then increase the corresponding counter by 1. Since T_2 provides a filter of 2^{-8}, there are about 2^{2t-152} suggestions.

5) Select the higher 2^{104-h} count values to be the candidate subkeys. Then exhaustively search the remaining $k-200$ unknown key bits and verify them.

For the collected data, there are 2^{2t} quartets satisfying the input difference α in two sides of the 9-round boomerang distinguisher. We regard the difference in X_9 as random after decrypting ciphertext quartets. Then the probability $\Delta X_9 = \delta$ in one side of the boomerang distinguisher is 2^{-127}. The probability of the 9-round boomerang distinguisher is $2^{-120.4}$, so there are $2^{2t-247.4}$ expected right quartets. The expected value of the counter is $2^{2t-247.4}$ for the right key, while it is 2^{2t-256} for the wrong keys. The complexity in data collection is $4\cdot 2^t$. The time and memory complexities both are 2^{120} in precomputation. In key recovery phase, for each guess of 12 bytes, the time complexity of step 2) and step 3) is 2^{t+2} one-round decryptions and 2^t table lookups. In step 4), the time complexity is about 2^{2t-128} table lookups. Regarding one table lookup as one-round encryption [30], the overall time complexity is about $4\cdot 2^t + 2^{120} + 2^{96}\cdot (5\cdot 2^t + 2^{2t-128})/11 + 2^{k-h}$ encryptions. Take $t = 123.7$ for the expected $s = 2^{2t-247.4} = 1$ right quartet, and take $h = 40$ for the success probability $P_s = 68.8\%$. The overall time complexity is $2^{218.6}$, the data and memory complexities both are $2^{125.7}$.

3. Attack on 11-round Deoxys-BC-256 with full codebook

In this subsection, we will give another 11-round boomerang attack on Deoxys-BC-256 with less time complexity than the attack in Section III.2, at the cost of full codebook under four related keys. We construct the structures in the internal state W_9 such that $\Delta W_9[0,3,12,13] = 0$ for the ciphertext pairs (C_1, C_3). Then there are 4 bytes of ΔX_9 matching the difference δ in the end of the boomerang distinguisher, that is $\Delta X_9[0,1,12,15] = 0$. So, the probability of (C_1, C_3) satisfying $\Delta X_9 = \delta$ is increased to 2^{-96}. The detailed attack process is given as follows.

Key recovery Construct y structures at the first and last columns of W_9. Each structure consists of 2^{32} elements taking all the possible values on $W_9[1,2,14,15]$ while $W_9[0,3,12,13]$ fixed to constants.

1) Guess 8-byte $\mathrm{IK}_{11}[0,1,2,3,12,13,14,15]$. For each element in each structure, compute the first and last columns of the ciphertexts C_1, C_3 under the keys K_1, K_3. Traverse all the 2^{64} possible values of the second and third columns of C_1, and query their plaintexts P_1 under the key K_1. Compute all $P_2 = P_1 \oplus \alpha$ and query their ciphertexts C_2 under the key K_2. Do the same operations for C_3. Then we obtain the following two sets of size 2^{96} for each structure.

$$\begin{aligned} S_1 = \{(P_1, C_1, P_2, C_2) \mid\ & P_1 = E_{K_1}^{-1}(C_1), \\ & P_2 = P_1 \oplus \alpha, C_2 = E_{K_2}(P_2)\} \end{aligned}$$

$$\begin{aligned} S_2 = \{(P_3, C_3, P_4, C_4) \mid\ & P_3 = E_{K_3}^{-1}(C_3), \\ & P_4 = P_3 \oplus \alpha, C_4 = E_{K_4}(P_3)\} \end{aligned}$$

2) Guess 4-byte subtweakey $\mathrm{IK}_{10}[5,6,10,11]$. Initialize a list of 2^{104} counters corresponding to 13-byte $\mathrm{IK}_{11}[4,5,6,7,8,9,10,11]$ and $\mathrm{IK}_{10}[4,7,8,9,14]$.

3) For each $(P_1, C_1, P_2, C_2) \in S_1$, partially decrypt (C_1, C_2) to obtain the values of $W_9[0,3,12,13]$ and $X_9[5,6,10,11]$, denoted by (w_1, x_1, w_2, x_2). Store (P_1, C_1, P_2, C_2) into a hash table H indexed by (x_1, w_2, x_2).

4) For each $(P_3, C_3, P_4, C_4) \in S_2$, partially decrypt (C_3, C_4) to obtain the corresponding (w_3, x_3, w_4, x_4). Then we construct the quartets (C_1, C_2, C_3, C_4) by looking up the hash table H with the index $(x_3 \oplus (\mathrm{0d}, \mathrm{ff}, \mathrm{8a}, 05), w_4, x_4 \oplus (\mathrm{0d}, \mathrm{ff}, \mathrm{8a}, 05))$. There are about $2^{96+96-96} = 2^{96}$ quartets obtained for each structure.

5) For all the $y2^{96}$ quartets, execute the step 4) and step 5) of the key recovery in Section III.2.

Since the probability of $\Delta X_9 = \delta$ is 2^{-96} and the 9-round boomerang distinguisher is $2^{-120.4}$, there are $y2^{96\times 2-96-120.4} = y2^{-24.4}$ expected right quartets. The expected value of the counter for the right key is $y2^{-24.4}$, while it is $y2^{-32}$ for the wrong keys. The time complexity of step 1) is about $4\cdot y2^{96}$. The time complexity in step 3) and step 4) both are $2^{96}\cdot 2\cdot y2^{96}$ one-round decryptions and $2^{96}\cdot y2^{96}$ table lookups. In step 5), the time complexity is about $2^{96}y2^{96}$ table lookups. Therefore, the overall time complexity is about $4\cdot y2^{96} + 7\cdot 2^{96}y2^{96}/11 + 2^{k-h}$. Take $y = 2^{24.4}$ for one right quartet and $h = 46$ for the success probability $P_s = 67.4\%$. The overall time complexity is $2^{215.8}$ encryptions. Due to the full codebook under four related-tweakeys, the data complexity is $4\times 2^{128} = 2^{130}$. The memory complexity in the precomputation phase is $2^{112} + 2^{120}$, and in the key recovery phase, the memory complexity is 3×2^{96}. So, the overall memory complexity is about 2^{120}.

IV. Boomerang Attack on 13-Round Deoxys-BC-384

In this section, we improve the 13-round related-tweakey boomerang attack on Deoxys-BC-384 using the precomputation technique. As shown in Figure 3, we use the 11-round boomerang distinguisher in [21] with the probability $2^{-118.4}$, where $\alpha = (00\ 00\ 00\ 00\ 00\ 00\ 85\ 00\ 00\ 9\mathrm{a}\ 00\ 0050\ 32\ 00\ \mathrm{e}9)$ and $\delta = (00\ 00\ 00\ 00\ 00\ \mathrm{a}4\ 83\ \mathrm{a}4\ \mathrm{da}\ 00\ 00\ \mathrm{f}200\ 00\ 00\ 00)$. The details of the differentials of the boomerang distinguisher refer to [21]. Denote $\mathrm{SR}^{-1}\circ \mathrm{MC}^{-1}(C)$ by the ciphertext C in the last round for simplicity.

Precomputation Similar to the precomputation in Section III.1, we precompute two tables T_3 and T_4. The table T_3 of size 2^{112} is constructed as follows.

1) For each of 2^{48} values of $\mathrm{IK}_{13}[8,9,10,11]$ and

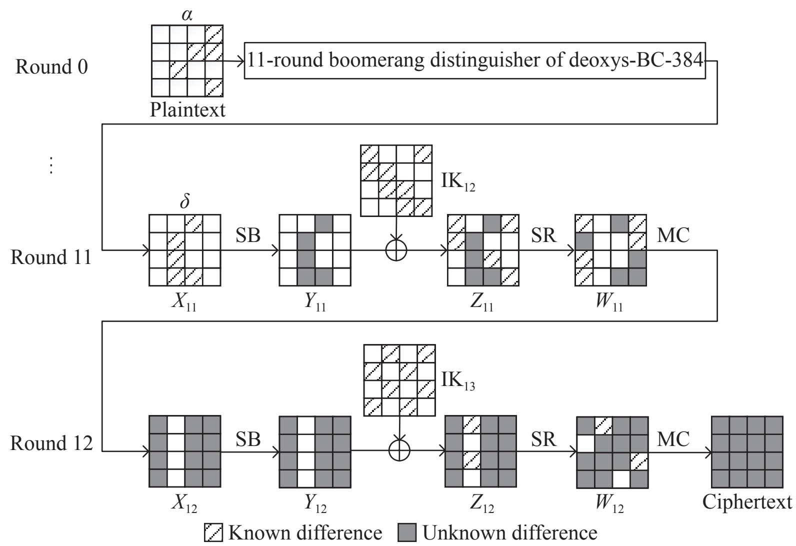

Figure 3 Related-tweakey boomerang attack on 13-round Deoxys-BC-384.

$\mathrm{IK}_{12}[7,8]$,

2) For each of 2^{32} values of $X_{11}[7,8]$ and $W_{11}[9,10]$, compute the values of the third column of Z_{12} under the related keys K_1, K_2, denoted by z_1, z_2. Then compute the corresponding z_3, z_4 under K_3, K_4 after XORing the known differences $\Delta X_{11}[7,8] = (\mathrm{a4}, \mathrm{da})$, $\Delta W_{11}[9,10] = 0$. Then store (z_1, z_3) and (z_2, z_4) in the sets L_1 and L_2, respectively.

3) For each (z_1, z_3) in L_1 and each (z_2, z_4) in L_2, store the value of $\mathrm{IK}_{13}[8,9,10,11]$ and $\mathrm{IK}_{12}[7,8]$ in the table T_3 indexed by (z_1, z_2, z_3, z_4).

The second precomputed table T_4 of size 2^{112} is constructed similarly.

1) For each of 2^{48} values of $\mathrm{IK}_{13}[12,13,14,15]$ and $\mathrm{IK}_{12}[6,11]$.

2) For each of 2^{32} values of $X_{11}[6,11]$ and $W_{11}[12,13]$, compute the values of the last column of Z_{12} under the related keys K_1, K_2, denoted by z_1, z_2. Then compute the corresponding z_3, z_4 under K_3, K_4 after XORing the known differences $\Delta X_{11}[6,11] = (83, \mathrm{f2})$, $\Delta W_{11}[12,13] = (81, \mathrm{cf})$. Then store (z_1, z_3) and (z_2, z_4) in the sets L_1 and L_2, respectively.

3) For each (z_1, z_3) in L_1 and each (z_2, z_4) in L_2, store the value of $\mathrm{IK}_{13}[12,13,14,15]$ and $\mathrm{IK}_{12}[6,11]$ in the table T_4 indexed by (z_1, z_2, z_3, z_4).

To prepare the table T_3 and T_4, it needs memory complexity of 2^{113} and time complexity of 2^{113} memory access totally. For any (z_1, z_2, z_3, z_4), T_3 and T_4 both suggest 2^{-16} key candidates on average.

Data collection Construct y structures of ciphertexts, each traversing all possible values on 12-byte $Z_{12}[0,1,2,3,8,9,10,11,12,13,14,15]$ with the other 4 bytes fixed to appropriate constants. For each structure S, choose another ciphertext structure S' such that the difference of the 4-byte constants between S and S' is equal to $(\mathrm{bc}, 00, 82, 00)$.

Then construct the following two sets of the size 2^{96} for each structure.

$$\begin{aligned} S_1 = \{ & (P_1, C_1, P_2, C_2) \mid P_1 = E_{K_1}^{-1}(C_1), \\ & P_2 = P_1 \oplus \alpha, C_2 = E_{K_2}(P_2), C_1 \in S\} \\ S_2 = \{ & (P_3, C_3, P_4, C_4) \mid P_3 = E_{K_3}^{-1}(C_3), \\ & P_4 = P_3 \oplus \alpha, C_4 = E_{K_4}(P_3), C_3 \in S'\} \end{aligned}$$

Key recovery Guess 5-byte $IK_{13}[0,1,2,3]$ and $IK_{12}[5]$, then carry out the following process.

1) Initialize a list of 2^{96} counters corresponding to 12-byte $\mathrm{IK}_{12}[6,7,8,11]$ and $\mathrm{IK}_{13}[8,9,10,11,12,13,14,15]$.

2) For each $(P_1, C_1, P_2, C_2) \in S_1$, partially decrypt (C_1, C_2) to obtain the values of $W_{11}[0,2,3]$ and $X_{11}[5]$, denoted by (w_1, x_1, w_2, x_2). Store (P_1, C_1, P_2, C_2) into a hash table H indexed by 96-bit $(w_1, x_1, w_2, x_2, C_2[4,5,6,7])$.

3) For each $(P_3, C_3, P_4, C_4) \in S_2$, partially decrypt (C_3, C_4) to obtain the corresponding (w_3, x_3, w_4, x_4). Since $\Delta X_{11}[5] = \mathrm{a4}$, $\Delta W_{11}[0,2,3] = (\mathrm{ae}, \mathrm{1e}, \mathrm{3d})$ and $\Delta Z_{12}[0,2,3] = (\mathrm{bc}, 00, 82, 00)$, we construct the quartets (C_1, C_2, C_3, C_4) by looking up H with the index $(w_3 \oplus (\mathrm{ae}, \mathrm{1e}, \mathrm{3d}), x_3 \oplus \mathrm{a4}, w_4 \oplus (\mathrm{ae}, \mathrm{1e}, \mathrm{3d}), x_4 \oplus \mathrm{a4}, C_4[4,5,6,7] \oplus (\mathrm{bc}, 00, 82, 00))$. There are about $2^{96+96-96} = 2^{96}$ quartets obtained for each structure.

4) For all the $y2^{96}$ quartets, lookup the precomputed table T_3 to find the candidates of $\mathrm{IK}_{13}[8,9,10,11]$ and $\mathrm{IK}_{12}[7,8]$. Since T_3 provides a filter of 2^{-16}, there are about $y2^{80}$ quartets remaining. Then lookup T_4 to find the candidates of $\mathrm{IK}_{13}[12,13,14,15]$ and $\mathrm{IK}_{12}[6,11]$. If a 96-bit key candidate involved is suggested, then increase the corresponding counter by 1. Since T_3 provides a filter of 2^{-16}, there are about $y2^{64}$ suggestions.

5) Select the higher 2^{96-h} counter values to be the candidate subkeys. Then exhaustively search the remaining $k - 136$ unknown key bits and verify them.

For the collected data, since the pairs (C_1, C_3) satisfy the difference $\Delta X_{11}[3,4,9,14] = 0$ after partial decryption, the probability of $\Delta X_{11} = \delta$ is 2^{-96}. The probability of the 11-round boomerang distinguisher is $2^{-118.4}$, so there are $y2^{96\times 2-96-118.4} = y2^{-22.4}$ expected right quartets. The expected value of the counter for the right key is $y2^{-22.4}$, while it is $y2^{-32}$ for the wrong keys. The data and time complexities of data collection both are $4 \cdot y2^{96}$. In precomputation phase, the time and memory complexities both are 2^{113}. In key recovery phase, the time complexity in step 2) and step 3) both are $2^{40} \cdot 2 \cdot y2^{96}$ one-round decryptions and $2^{40} \cdot y2^{96}$ table lookups. The time complexity in step 4) is about $2^{40} \cdot y2^{96}$ table lookups. Thus, the overall time complexity is $4 \cdot y2^{96} + 2^{113} + 2^{40} \cdot 7 \cdot y2^{96}/13 + 2^{k-h}$. Take $y = 2^{22.4}$ for one right quartet and $h = 96$ for the success probability $P_s = 54.2\%$. The overall time complexity is $2^{157.5} + 2^{k-96}$, the data complexity is $2^{120.4}$ and the memory complexity is 2^{113} bounded by the precomputation. For $k = 256$, the time complexity is $2^{160.3}$, reducing by a factor of 2^{31} compared with the previous attack in [20].

V. New Boomerang Distinguishers on 11-Round Deoxys-BC-384

In [21], Zhao *et al.* gave the best known boomerang distinguisher on 11-round Deoxys-BC-384 with the probability $2^{-118.4}$. The tools of BDT and BDT′ [19] are used to compute the accurate probability in the middle two-round boomerang switch. They found two differential characteristics in the middle two-round boomerang switch with the probabilities 2^{-13} and 2^{-14}, respectively. Then the boomerang probability of the middle two-round is $2^{-13} + 2^{-14} = 2^{-12.4}$. Whether there are the other boomerang differential characteristics with the same or higher probability? Based on the same truncated differential as [21], we search all the differentials of the two-round boomerang switch. As mentioned in [21], there are only one differential path having the probability 2^{-41} for the upper part. Keeping the same differential trail for the upper part as [21], we find two new boomerang differentials with the same probability $2^{-12.4}$, which both consist of two differential characteristics of probabilities 2^{-13} and 2^{-14}. Then deducing the appropriate lower differential trails from the obtained middle two-round boomerang differentials, we give two new related-tweakey boomerang distinguishers on 11-round Deoxys-BC-384 with the same probability $2^{-118.4}$. The distinguisher I is listed in Table A-1 in Appendix A, and its another differential in the middle two-round boomerang switch is presented in Table A-2. The distinguisher II is listed in Table A-3 and its another differential in the middle two-round boomerang switch is presented in Table A-4. The difference $\Delta\mathrm{STK}_0$ is equal to $(00, 85, 00, 00, 9a, 00, 00, 00, 32, 00, e9, 50, 00, 00, 00, 00)$ in the first round of the two distinguishers. The initial difference of the distinguishers is the same as $\Delta\mathrm{STK}_0$, we omit the AK operation in the first round in the tables.

VI. Conclusions

In this paper, utilizing the precomputation technique, we improve the related-tweakey boomerang attacks on round-reduced Deoxys-BC based on the existing boomerang distinguishers. We give a better related-tweakey boomerang attack on 11-round Deoxys-BC-256 with time/data/memory complexities of $2^{218.6}/2^{125.7}/2^{125.7}$, and give another 11-round attack with the less time and memory complexities when the adversary has access to the full codebook. We also improve the related-tweakey boomerang attack on 13-round Deoxys-BC-384. For the key size $k = 256$, it reduces the time complexity by a factor of 2^{31} compared with the previous 13-round boomerang attack. In addition, we present two new related-tweakey boomerang distinguishers on 11-round Deoxys-BC-384 with the same probability as the best previous distinguisher. The precomputation technique used in this paper transfers a part of subtweakey guess in the key-recovery phase to the precomputation phase, resulting in a significant reduction of the overall attack complexity. The precomputation technique could be applied to improve the key recovery attack on other block ciphers.

Acknowledgements

This work was supported by the National Cryptography Development Fund of China (Grant Nos. MMJJ 20170103 and MMJJ20180204).

Appendix A. New Boomerang Distinguishers on 11-Round Deoxys-BC-384

Table A-1 Distinguisher I of 11-round Deoxys-BC-384 (The probabilities marked with † are only counted once)

$\Delta\mathrm{TK}_0^1$: 00 00 00 00 00 00 8b 00 00 c4 00 00 a6 7a 00 c5																	
$\Delta\mathrm{TK}_0^2$: 00 00 00 00 00 00 ad 00 00 c4 00 00 d8 73 00 21																	
$\Delta\mathrm{TK}_0^3$: 00 00 00 00 00 00 a3 00 00 9a 00 00 2e 3b 00 0d																	
$\nabla\mathrm{TK}_0^1$: 00 00 00 00 00 00 00 f6 00 00 0e 00 00 00 00 00																	
$\nabla\mathrm{TK}_0^2$: 00 00 00 00 00 00 00 ef 00 00 cd 00 00 00 00 00																	
$\nabla\mathrm{TK}_0^3$: 00 00 00 00 00 00 00 34 00 00 24 00 00 00 00 00																	
R	ΔX				ΔY				$\Delta\mathrm{IK}$				ΔZ				pr
1	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Table A-1 (Continued)

2	00	00	00	00	00	00	00	00	e0	00	26	38	e0	00	26	38	1
	00	00	00	00	00	00	00	00	d1	ad	00	9f	d1	ad	00	9f	
	00	00	00	00	00	00	00	00	f7	c1	ed	00	f7	c1	ed	00	
	00	00	00	00	00	00	00	00	00	01	d9	8d	00	01	d9	8d	
3	57	00	00	00	6b	00	00	00	49	be	00	00	22	be	00	00	2^{-28}
	00	00	00	00	00	00	00	00	00	e0	e1	00	00	e0	e1	00	
	00	00	4f	00	00	00	2a	00	00	00	69	4f	00	00	43	4f	
	7a	00	00	f1	a6	00	00	15	7a	00	00	29	b6	00	00	3c	
4	00	a6	00	00	00	2b	00	00	00	2b	00	00	00	00	00	00	2^{-13}
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	bd	00	00	00	19	00	00	00	19	00	00	00	00	00	00	00	
5	00	00	00	00	00	00	00	00	cd	03	d0	d4	cd	03	d0	d4	1
	00	00	00	00	00	00	00	00	bf	26	8f	77	bf	26	8f	77	
	00	00	00	00	00	00	00	00	c1	04	78	5f	c1	04	78	5f	
	00	00	00	00	00	00	00	00	e7	e3	06	09	e7	e3	06	09	
6	9a	34	00	00	8e		00	00	bd	8b	9b	00	33		9b	00	2^{-7}†
	00	00	85	00	00	00		00	00	46	c7	d6	00	46		d6	
	00	00	00	b9	00	00	00		b4	00	4d	ad	b4	00	4d		
	00	00	00	00	00	00	00	00	f2	e3	00	e6	f2	e3	00	e6	
7	07		1b	00				00				b7				b7	1
	8e		08	00				00				52				52	
	8e		00	00			00	00			5b	00			5b	00	
	89		09	00				00				fb				fb	
6		00			00	00			2a	00			2a	00			1
			00			59	00			66	00			3f	00		
				00			76	00			55	00			23	00	
	00				00			9a	00			ab	00			31	
7	07	00	00	00	09	00	00	00	09	00	00	00	00	00	00	00	2^{-7}†
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00		00	00	00	06	00	00	00	06	00	00	00	00	00	
	00	00	00		00	00	00	03	00	00	00	03	00	00	00	00	
8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
10	00	00	00	00	00	00	00	00	00	82	81	00	00	82	81	00	1
	00	00	00	00	00	00	00	00	00	00	c3	ca	00	00	c3	ca	
	00	00	00	00	00	00	00	00	af	00	00	af	af	00	00	af	
	00	00	00	00	00	00	00	00	f5	f3	00	00	f5	f3	00	00	
11	00	1b	00	00	00	cc	00	00	00	00	b1	00	00	cc	b1	00	2^{-12}
	00	00	17	00	00	00	93	00	00	00	00	34	00	00	93	34	
	00	00	00	00	00	00	00	00	27	00	00	00	27	00	00	00	
	00	00	00	00	00	00	00	00	00	b0	00	00	00	b0	00	00	

Table A-2 Another 2-round boomerang switch of distinguisher I (The probabilities marked with † are counted once)

R	ΔX				ΔY				ΔIK				ΔZ				pr
6	9a	34	00	00	17		00	00	bd	8b	9b	00	aa		9b	00	2^{-7}†
	00	00	85	00	00	00		00	00	46	c7	d6	00	46		d6	
	00	00	00	b9	00	00	00		b4	00	4d	ad	b4	00	4d		
	00	00	00	00	00	00	00	00	f2	e3	00	e6	f2	e3	00	e6	
7	2e		1b	00				00				b7				b7	1
	17		08	00				00				52				52	
	47		00	00			00	00			5b	00			5b	00	
	39		09	00				00				fb				fb	
6		00			17	00			2a	00			3d	00			1
			00			c8	00			66	00			ae	00		
				00			80	00			55	00			d5	00	
	00				00			b5	00			ab	00			1e	
7	58	00	00	00	09	00	00	00	09	00	00	00	00	00	00	00	2^{-6}†
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00		00	00	00	06	00	00	00	06	00	00	00	00	00	
	00	00	00		00	00	00	03	00	00	00	03	00	00	00	00	

Table A-3 Distinguisher II of 11-round Deoxys-BC-384 (The probabilities marked with † are only counted once)

ΔTK_0^1 : 00 00 00 00 00 00 8b 00 00 c4 00 00 a6 7a 00 c5

ΔTK_0^2 : 00 00 00 00 00 00 ad 00 00 c4 00 00 d8 73 00 21

ΔTK_0^3 : 00 00 00 00 00 00 a3 00 00 9a 00 00 2e 3b 00 0d

∇TK_0^1 : 00 00 00 00 00 00 00 f6 00 00 0e 00 00 00 00 00

∇TK_0^2 : 00 00 00 00 00 00 00 ef 00 00 cd 00 00 00 00 00

∇TK_0^3 : 00 00 00 00 00 00 00 34 00 00 24 00 00 00 00 00

R	ΔX				ΔY				ΔIK				ΔZ				pr
1	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
2	00	00	00	00	00	00	00	00	e0	00	26	38	e0	00	26	38	1
	00	00	00	00	00	00	00	00	d1	ad	00	9f	d1	ad	00	9f	
	00	00	00	00	00	00	00	00	f7	c1	ed	00	f7	c1	ed	00	
	00	00	00	00	00	00	00	00	00	01	d9	8d	00	01	d9	8d	
3	57	00	00	00	6b	00	00	00	49	be	00	00	22	be	00	00	2^{-28}
	00	00	00	00	00	00	00	00	00	e0	e1	00	00	e0	e1	00	
	00	00	4f	00	00	00	2a	00	00	00	69	4f	00	00	43	4f	
	7a	00	00	f1	a6	00	00	15	7a	00	00	29	b6	00	00	3c	
4	00	a6	00	00	00	2b	00	00	00	2b	00	00	00	00	00	00	2^{-13}
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	bd	00	00	00	19	00	00	00	19	00	00	00	00	00	00	00	
5	00	00	00	00	00	00	00	00	cd	03	d0	d4	cd	03	d0	d4	1
	00	00	00	00	00	00	00	00	bf	26	8f	77	bf	26	8f	77	
	00	00	00	00	00	00	00	00	c1	04	78	5f	c1	04	78	5f	
	00	00	00	00	00	00	00	00	e7	e3	06	09	e7	e3	06	09	

Table A-3 (Continued)

6	9a	34	00	00	db		00	00	bd	8b	9b	00	66		9b	00	2^{-6}†
	00	00	85	00	00	00		00	00	46	c7	d6	00	46		d6	
	00	00	00	b9	00	00	00		b4	00	4d	ad	b4	00	4d		
	00	00	00	00	00	00	00	00	f2	e3	00	e6	f2	e3	00	e6	
7	ad		1b	00				00				b7				b7	1
	db		08	00				00				52				52	
	8b		00	00			00	00			5b	00			5b	00	
	76		09	00				00				fb				fb	
6		00			00	00			dc	00			dc	00			1
			00			79	00			cb	00			b2	00		
				00			13	00			23	00			30	00	
	00				00			35	00			c6	00			f3	
7	ad	00	00	00	2c	00	00	00	2c	00	00	00	00	00	00	00	2^{-7}†
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00		00	00	00	a7	00	00	00	a7	00	00	00	00	00	
	00	00	00		00	00	00	de	00	00	00	de	00	00	00	00	
8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
9	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	1
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
10	00	00	00	00	00	00	00	00	00	ae	70	00	00	ae	70	00	1
	00	00	00	00	00	00	00	00	00	00	f9	d5	00	00	f9	d5	
	00	00	00	00	00	00	00	00	32	00	00	32	32	00	00	32	
	00	00	00	00	00	00	00	00	11	b6	00	00	11	b6	00	00	
11	00	74	00	00	00	f1	00	00	00	00	cf	00	00	f1	cf	00	2^{-12}
	00	00	21	00	00	00	9e	00	00	00	00	bb	00	00	9e	bb	
	00	00	00	00	00	00	00	00	8c	00	00	00	8c	00	00	00	
	00	00	00	00	00	00	00	00	00	2d	00	00	00	2d	00	00	

Table A-4 Another 2-round boomerang switch of distinguisher II (The probabilities marked with † are counted once)

R	ΔX				ΔY				ΔIK				ΔZ				pr
6	9a	34	00	00	a7		00	00	bd	8b	9b	00	1a		9b	00	2^{-7}†
	00	00	85	00	00	00		00	00	46	c7	d6	00	46		d6	
	00	00	00	b9	00	00	00		b4	00	4d	ad	b4	00	4d		
	00	00	00	00	00	00	00	00	f2	e3	00	e6	f2	e3	00	e6	
7	55		1b	00				00				b7				b7	1
	a7		08	00				00				52				52	
	f7		00	00			00	00			5b	00			5b	00	
	f2		09	00				00				fb				fb	
6		00			a7	00			dc	00			7b	00			1
			00			00	00			cb	00			cb	00		
				00			a7	00			23	00			84	00	
	00				00			a7	00			c6	00			61	

Table A-4 (Continued)

R	ΔX				ΔY				ΔIK				ΔZ				pr
7	55	00	00	00	2c	00	00	00	2c	00	00	00	00	00	00	00	2^{-7}†
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00		00	00	00	a7	00	00	00	a7	00	00	00	00	00	
	00	00	00		00	00	00	de	00	00	00	de	00	00	00	00	

References

[1] "CAESAR: Competition for authenticated encryption: Security, applicability, and robustness, 2014," Available at: http://competitions.cr.yp.to/caesar.html, 2019-02-20.

[2] "NIST lightweight cryptography project," Available at: https://csrc.nist.gov/Projects/Lightweight-Cryptography, 2015.

[3] M. D. Liskov, R. L. Rivest, and D. A. Wagner, "Tweakable block ciphers," in *Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, CA, USA, pp.31–46, 2002.

[4] J. Jean, I. Nikolić, and T. Peyrin, "Tweaks and keys for block ciphers: The TWEAKEY framework," in *Proceedings of the 20th International Conference on Advances in Cryptology*, Kaoshiung, China, pp.274–288, 2014.

[5] J. Jean, I. Nikolić, T. Peyrin, *et al.*, "The Deoxys AEAD family," *Journal of Cryptology*, vol. 34, no. 3, article no. articleno.31, 2021.

[6] D. Wagner, "The boomerang attack," in *Proceedings of the 6th International Workshop on Fast Software Encryption*, Rome, Italy, pp.156–170, 1999.

[7] J. Kelsey, T. Kohno, and B. Schneier, "Amplified boomerang attacks against reduced-round MARS and serpent," in *Proceedings of the 7th International Workshop on Fast Software Encryption*, New York, NY, USA, pp.75–93, 2001.

[8] E. Biham, O. Dunkelman, and N. Keller, "The rectangle attack - rectangling the Serpent," in *Proceedings of the International Conference on Advances in Cryptology*, Innsbruck, Austria, pp.340–357, 2001.

[9] E. Biham, O. Dunkelman, and N. Keller, "Related-key boomerang and rectangle attacks," in *Proceedings of the 24th Annual International Conference on Advances in Cryptology*, Aarhus, Denmark, pp.507–525, 2005.

[10] E. Biham, O. Dunkelman, and N. Keller, "A related-key rectangle attack on the full KASUMI," in *Proceedings of the 11th International Conference on Advances in Cryptology*, Chennai, India, pp.443–461, 2005.

[11] O. Dunkelman, N. Keller, and A. Shamir, "A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony," in *Proceedings of the 30th Annual Cryptology Conference on Advances in Cryptology*, Santa Barbara, CA, USA, pp.393–410, 2010.

[12] A. Biryukov and D. Khovratovich, "Related-key cryptanalysis of the full AES-192 and AES-256," in *Proceedings of the 15th International Conference on Advances in Cryptology*, Tokyo, Japan, pp.1–18, 2009.

[13] X. Y. Dong, L. Y. Qin, S. W. Sun, *et al.*, "Key guessing strategies for linear key-schedule algorithms in rectangle attacks," in *Proceedings of the 41st Annual International Conference on Advances in Cryptology*, Trondheim, Norway, pp.3–33, 2022.

[14] G. Z. Liu, M. Ghosh, and L. Song, "Security analysis of SKINNY under related-tweakey settings (long paper)," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 3, pp. 37–72, 2017.

[15] B. X. Zhao, X. Y. Dong, W. Meier, *et al.*, "Generalized related-key rectangle attacks on block ciphers with linear key schedule: Applications to SKINNY and GIFT," *Designs, Codes and Cryptography*, vol. 88, no. 6, pp. 1103–1126, 2020.

[16] C. Cid, T. Huang, T. Peyrin, *et al.*, "A security analysis of Deoxys and its internal tweakable block ciphers," *IACR Transactions on Symmetric Cryptology*, vol. 2017, no. 3, pp. 73–107, 2017.

[17] Y. Sasaki, "Improved related-tweakey boomerang attacks on Deoxys-BC," in *Proceedings of the 10th International Conference on Progress in Cryptology*, Marrakesh, Morocco, pp.87–106, 2018.

[18] C. Cid, T. Huang, T. Peyrin, *et al.*, "Boomerang connectivity table: A new cryptanalysis tool," in *Proceedings of the 37th Annual International Conference on Advances in Cryptology*, Tel Aviv, Israel, pp.683–714, 2018.

[19] H. Y. Wang and T. Peyrin, "Boomerang switch in multiple rounds. Application to AES variants and Deoxys," *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 1, pp. 142–169, 2019.

[20] B. X. Zhao, X. Y. Dong, and K. T. Jia, "New related-tweakey boomerang and rectangle attacks on Deoxys-BC including BDT effect," *IACR Transactions on Symmetric Cryptology*, vol. 2019, no. 3, pp. 121–151, 2019.

[21] B. X. Zhao, X. Y. Dong, K. T. Jia, *et al.*, "Improved related-tweakey rectangle attacks on reduced-round Deoxys-BC-384 and Deoxys-I-256-128," in *Proceedings of the 20th International Conference on Progress in Cryptology*, Hyderabad, India, pp.139–159, 2019.

[22] L. Song, N. N. Zhang, Q. Q. Yang, *et al.*, "Optimizing rectangle attacks: A unified and generic framework for key recovery," in *Proceedings of the 28th International Conference on Advances in Cryptology*, Taipei, China, pp.410–440, 2022.

[23] A. Mehrdad, F. Moazami, and H. Soleimany, "Impossible differential cryptanalysis on Deoxys-BC-256," *The ISC International Journal of Information Security*, vol. 10, no. 2, pp. 93–105, 2018.

[24] R. Zong, X. Y. Dong, and X. Y. Wang, "Related-tweakey impossible differential attack on reduced-round Deoxys-BC-256," *Science China Information Sciences*, vol. 62, no. 3, article no. 32102, 2019.

[25] Y. Liu, B. Shi, D. W. Gu, *et al.*, "Improved meet-in-the-middle attacks on reduced-round Deoxys-BC-256," *The Computer Journal*, vol. 63, no. 12, pp. 1859–1870, 2020.

[26] M. M. Li and S. Z. Chen, "Improved meet-in-the-middle attacks on reduced-round tweakable block cipher Deoxys-BC," *The Computer Journal*, vol. 65, no. 9, pp. 2411–2420, 2022.

[27] R. J. Li and C. H. Jin, "Meet-in-the-middle attacks on round-reduced tweakable block cipher Deoxys-BC," *IET Information Security*, vol. 13, no. 1, pp. 70–75, 2019.

[28] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, Berlin, 2002.

[29] A. A. Selçuk, "On probability of success in linear and differential cryptanalysis," *Journal of Cryptology*, vol. 21, no. 1, pp. 131–147, 2008.

[30] A. Bar-On, O. Dunkelman, N. Keller, *et al.*, "Improved key recovery attacks on reduced-round AES with practical data and memory complexities," in *Proceedings of the 38th Annual International Cryptology Conference on Advances in Cryptology*, Santa Barbara, CA, USA, pp.185–212, 2018.

Jiamei LIU was born in Anhui Province, China, in 1999. She received the B.E. degree in cryptography from PLA Strategic Support Force Information Engineering University in 2020 and is currently pursuing the M.S. degree in cryptography. Her research field is cryptography. (Email: liujiamei182@163.com)

Lin TAN was born in Hubei Province, China, in 1983. He received the Ph.D. degrees in cryptography from Information Engineering University, Zhengzhou, China, in 2012. His research field is cryptography. (Email: tanlin100@163.com)

Hong XU was born in Hubei Province, China, in 1979. She received the Ph.D. degrees in cryptography from Information Engineering University, Zhengzhou, China, in 2007. Her research field is cryptography. (Email: xuhong0504@163.com)