SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2019, Vol. 62 032102:1–032102:12
https://doi.org/10.1007/s11432-017-9382-2

Related-tweakey impossible differential attack on reduced-round Deoxys-BC-256

Rui ZONG[1], Xiaoyang DONG[2*] & Xiaoyun WANG[1,2*]

[1]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
[2]*Institute for Advanced Study, Tsinghua University, Beijing* 100084*, China*

Received 27 December 2017/Revised 25 January 2018/Accepted 28 February 2018/Published online 31 January 2019

Abstract Deoxys-BC is the internal tweakable block cipher of Deoxys, a third-round authenticated encryption candidate at the CAESAR competition. In this study, by adequately studying the tweakey schedule, we seek a six-round related-tweakey impossible distinguisher of Deoxys-BC-256, which is transformed from a 3.5-round single-key impossible distinguisher of AES, by application of the mixed integer linear programming (MILP) method. We present a detailed description of this interesting transformation method and the MILP-modeling process. Based on this distinguisher, we mount a key-recovery attack on 10 (out of 14) rounds of Deoxys-BC-256. Compared to previous results that are valid only when the key size > 204 and the tweak size < 52, our method can attack 10-round Deoxys-BC-256 as long as the key size $\geqslant 174$ and the tweak size $\leqslant 82$. For the popular setting in which the key size is 192 bits, we can attack one round more than previous studies. Note that this paper only gives a more accurate security evaluation and does not threaten the security of full-round Deoxys-BC-256.

Keywords related-tweakey impossible differential attack, tweakable block cipher, Deoxys-BC-256, tweakey schedule, MILP

Citation Zong R, Dong X Y, Wang X Y. Related-tweakey impossible differential attack on reduced-round Deoxys-BC-256. Sci China Inf Sci, 2019, 62(3): 032102, https://doi.org/10.1007/s11432-017-9382-2

1 Introduction

To satisfy the growing demand for authenticated encryption, the CAESAR competition[1)] was launched in 2013 by the international cryptologic research community. The competition has three rounds. In March 2014, the first-round competition received 57 submissions; in July 2015, 30 candidates were chosen during the second round of the competition; and in August 2016, 15 candidate ciphers were selected during the third round. The final winner was announced at a later date from amongst the third-round competition candidates.

Deoxys [1] is one of the 15 authenticated encryption candidates of the CAESAR third-round competition. The design of Deoxys is based on a tweakable block cipher Deoxys-BC, using the well-studied AES [2] round function as a building block.

The concept of a tweakable block cipher (TBC) was first proposed by Liskov et al. [3] in 2002. In addition to the secret key and a plaintext, a tweakable block cipher employs a third input: the tweak, which can be public, to yield a ciphertext. Its design is mainly motivated to solve the problem that for a traditional block cipher, when encrypted by the same key even in different cases, the plaintext will be

* Corresponding author (email: xiaoyangdong@mail.tsinghua.edu.cn, xiaoyunwang@mail.tsinghua.edu.cn)
1) http://competitions.cr.yp.to/caesar-submissions.html.

Table 1 Cryptanalysis results for Deoxys-BC-256. Our attack can be mounted on Deoxys-BC-256 with a wider key size range. Because the cipher adopts the TWEAKEY framework (such as the tweak-updating mode, i.e., the tweak can be changed but the key stays the same), our attack is more efficient as the data complexity can be beyond full-codebook. A beyond-full-codebook attack on SKINNY was published in [9]; we give a more specified description about beyond-full-codebook attacks in Subsection 2.2.

Primitive	Number of rounds	Tweak size	Key size	Time	Data	Attack type	Ref.
Deoxys-BC-256	8/14	128	128	$\leqslant 2^{128}$	–	MitM	[1]
	$\leqslant 8/14$	128	128	$\leqslant 2^{128}$	–	Differential	[1]
	9/14	128	128	2^{128}	2^{117}	Rectangle	[8]
	10/14	< 52	> 204	2^{204}	$2^{127.58}$	Rectangle	[8]
	10/14	$\leqslant 82$	$\geqslant 174$	$2^{173.1}$	2^{135}	Impossible differential	This paper

transformed into a fixed ciphertext. There have been many TBCs, including Skinny [4], PRINCE [5], and QARMA [6].

In contrast to many tweakable block constructions that take a known permutation or a block cipher as a black box and use the tweak as an independent input, Deoxys-BC adopts the TWEAKEY framework [7], which provides a unified view of the key and the tweak, denoted by tweakey. This means that when given the public round permutation (for instance, the AES round function), the tweakable block cipher can be a primitive with arbitrary tweak and key sizes. For ciphers that adopt this framework, a dedicated tweakey schedule will use the $(k+t)$-bit tweakey, composed of a k-bit key (k can be almost any value) and a t-bit tweak, to produce n-bit round subtweakeys. For Deoxys-BC, there are two versions: Deoxys-BC-256 with a 256-bit tweakey and Deoxys-BC-384 with a 384-bit tweakey. The subtweakey size is 128 bits for both versions. In Deoxys, the size of the key and the tweak can vary within the tweakey length as long as the key size is longer than or equal to the block size, i.e., 128 bits.

Related work. At FSE 2018, Ref. [8] using related-tweakey rectangle attacks to analyze both Deoxys-BC-256 and Deoxys-BC-384 was presented. Compared to the security evaluation given by the designer, the work in [8] improved the number of analyzed rounds by two for Dexoys-BC-256 and five for Deoxys-BC-384. These attacks greatly improved the related-tweakey differential bounds provided by the designers.

Our contribution. In this study, we analyze Deoxys-BC-256 against impossible differential attacks and give a more accurate security evaluation of 10-round (out of 14-round) Deoxys-BC-256. First, we describe a method that can derive longer related-key impossible distinguishers from single-key impossible distinguishers. Second, using this method, after an adequate study of the tweakey schedule, we build an MILP model of six-round Deoxys-BC-256 and find a six-round related-tweakey impossible distinguisher. Finally, based on this distinguisher, we mount an attack including 10-round Deoxys-BC-256. The attack needs a time complexity of $2^{173.1}$ 10-round encryptions and a data complexity of 2^{135} plaintexts. Compared to previous results, the attack applies to a wider range of key sizes and can attack one more round on Deoxys-BC-256 with a key size of 192 bits, thus providing a more accurate security evaluation. All analysis results are shown in Table 1.

2 Preliminaries

First, we give a detailed description of Deoxys-BC-256; second, we present a validation of the beyond-full-codebook impossible attack on Deoxys-BC-256. Next, we discuss some useful propositions and the notations used in this paper.

2.1 Description of Deoxys-BC-256

In this subsection, we recall the details of the Deoxys-BC-256 block cipher. We assume that the reader is familiar with the AES block cipher [2]. Figure 1 shows the structure of Deoxys-BC-256.

Deoxys-BC is the internal ad-hoc tweakable block cipher of the Deoxys authenticated encryption scheme, conforming to the TWEAKEY framework [7]. Except for the two standard inputs of a block ci-

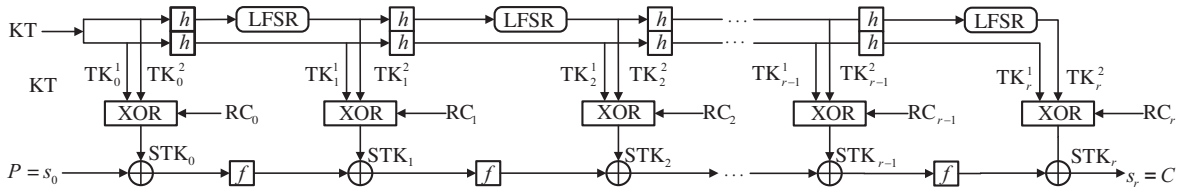

Figure 1 Structure of Deoxys-BC-256.

pher, i.e., a plaintext P and a key K, this cipher adopts a third input called a tweak T, i.e., $E_K(T, P) = C$. According to the TWEAKEY framework, we can use a single input, called the tweakey, to provide a unified view of the tweak and the key. The length of the tweakey is the cumulative size of the key and the tweak. For Deoxys-BC-256, the tweakey size is 256 bits; for Deoxys-BC-384, the tweakey size is 384 bits. In this paper, we focus on Deoxys-BC-256. For more information, we refer to [1].

Deoxys-BC is an AES-like design, i.e., it is an iterative substitution-permutation network (SPN) that transforms the plaintext through a certain number of round functions (that depend on the tweakey) to a ciphertext. As the Deoxys-BC cipher uses the AES round function, we can represent the internal state as a 4×4 matrix of bytes. The corresponding index is

$$\text{Internal state} = (0, 1, 2, 3, \ldots, 14, 15) = \begin{pmatrix} 0 & 4 & 8 & 12 \\ 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \end{pmatrix}.$$

Deoxys-BC-256 round function. The round function, similar to AES, has four operations applied to the internal state, as follows:

- **AddRoundTweakey (AK)** - XOR the 128-bit round subtweakey (defined further) to the internal state.
- **SubBytes (SB)** - Apply the 8-bit Sbox $\boldsymbol{S}$ of AES [2] to each of the 16 bytes of the internal state[2)].
- **ShiftRows (SR)** - Rotate the 4-byte i-th row left by $\rho[i]$ positions, where $\rho = (0, 1, 2, 3)$.
- **MixColumns (MC)** - Multiply the internal state by the 4×4 constant MDS matrix $\boldsymbol{M}$ defined below whose coefficients lie in $\mathbb{K}$[3)]. The matrix $\boldsymbol{M}$ and the inverse matrix $\overline{\boldsymbol{M}}$ are shown as follows:

$$\boldsymbol{M} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}, \quad \overline{\boldsymbol{M}} = \begin{pmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{pmatrix}.$$

After the last round, a final AK operation is performed to produce the ciphertext.

Definition of the subtweakey. The structure of the tweakey schedule distinguishes Deoxys-BC from the classical construction of an AES-like block cipher.

We use KT to denote the concatenation of the key K and the tweak T, i.e., $\text{KT} = K||T$. Then, the tweakey state is divided into 128-bit words. For Deoxys-BC-256, the size of KT is 256 bits, with the first (most significant) 128 bits of KT denoted by KT^2 and the second by KT^1.

A subtweakey of the i-th round is defined as

$$\text{STK}_i = \text{TK}_i^1 \oplus \text{TK}_i^2 \oplus \text{RC}_i. \tag{1}$$

The 128-bit words TK_i^2 and TK_i^1 are outputs produced by a special tweakey schedule algorithm, initialized with $\text{TK}_0^1 = \text{KT}^1$ and $\text{TK}_0^2 = \text{KT}^2$. The tweakey schedule algorithm is defined as

$$\text{TK}_{i+1}^1 = h(\text{TK}_i^1), \quad \text{TK}_{i+1}^2 = h(\text{LFSR}(\text{TK}_i^2)). \tag{2}$$

2) The specified detail of the Sbox is not presented as it does not influence the analysis process in this paper.

3) $\mathbb{K}$ denotes the base field as $GF(2^8)$ defined by the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. This is the base field used in AES.

Table 2 h-permutation

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$h(i)$	1	6	11	12	5	10	15	0	9	14	3	4	13	2	7	8

The h operation, shown in Table 2, is a simple byte permutation.

The LFSR function is simply the application of a linear feedback shifting register to each of the 16 bytes of a tweakey 128-bit word, i.e.,

$$\mathrm{LFSR}(x_7||x_6||x_5||x_4||x_3||x_2||x_1||x_0) = (x_6||x_5||x_4||x_3||x_2||x_1||x_0||x_7 \oplus x_5).$$

Finally, RC_i are the round constants of the tweakey schedule, and are defined as

$$\mathrm{RC}_i = \begin{pmatrix} 1 & \mathrm{RCON}[i] & 0 & 0 \\ 2 & \mathrm{RCON}[i] & 0 & 0 \\ 4 & \mathrm{RCON}[i] & 0 & 0 \\ 8 & \mathrm{RCON}[i] & 0 & 0 \end{pmatrix},$$

where $\mathrm{RCON}[i]$ denotes the i-th key schedule constants of the AES.

Deoxys. Deoxys is an authenticated encryption design based on Deoxys-BC. It has two modes: Deoxys-I, a nonce-based authenticated encryption scheme to be used in a nonce-respecting setting; and Deoxys-II, a nonce-based authenticated encryption scheme that can provide security even in a nonce-misuse setting.

With the recommended parameters, when instantiated with the Deoxys-BC-256 block cipher, the two modes lead to a 128-bit key version (denoted by Deoxys-I-128-128 and Deoxys-II-128-128). For more information about Deoxys, we refer to the Deoxys document [1].

2.2 Beyond full-codebook

Recall that a tweakable block cipher takes as its input a key (of fixed length n) and a tweak (of fixed length t). The TWEAKEY framework [7] offers further flexibility in setting the limit of data resources for an attack. For ciphers adopting the TWEAKEY framework, such as Deoxys-BC-256, one can add a tweak of almost any length and/or extend the key space of the block cipher to (almost) any size as long as the key space and the tweak space are suitable for the tweakey schedule. This provides attackers with a potentially optimal strategy to attack the ciphers: select the key size as large as possible, which results in a higher security claim, as long as the size of the tweak is large enough to supply the required data. Thus, in this scenario, an attack can be valid even if the data complexity is beyond full-codebook, and an attack is more difficult when the key size is smaller (the size range is wider).

In fact, beyond-full-codebook attacks have been shown to be realistic and powerful. In [10], the authors analyze the NIST standard for Format-Preserving Encryption with beyond-full-codebook attacks and exploit the fact that the cipher is a Feistel-based tweakable block cipher. In [9], several beyond-full-codebook attacks on different versions of SKINNY are presented.

In [8], the authors discuss beyond-full-codebook attacks for tweakable block ciphers. They also examine beyond-codebook rectangle attacks on Deoxys-BC. However, the beyond-full-codebook rectangle attack is complex and may be impossible as the sufficiently large plaintext/tweak space also provides too many wrong pairs that probabilistically satisfy the same input and output differences without following the characteristic. However, when considering the impossible differential attack, this problem does not exist because the differential propagates with probability 1 or 0.

2.3 Some propositions

Proposition 1 (Differential property of Sbox, [11])**.** Given the nonzero input and output differences of an Sbox, there exists only one pair of actual values on average to satisfy these two differences.

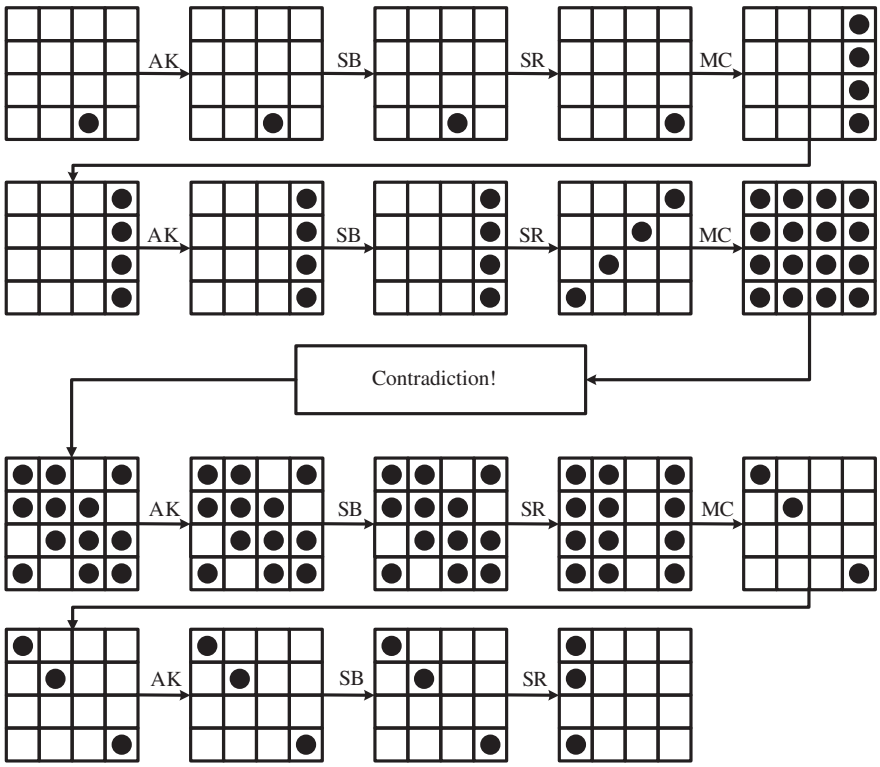

Figure 2 A 3.5-round single-key impossible distinguisher of AES.

Proposition 2 (The 3.5-round single-key impossible distinguisher of AES [12])**.** Consider 3.5-round AES encryption which omits the last MC operation. If a pair of plaintexts differ by only one byte, then the ciphertexts cannot be equal in any of the following combinations of bytes: (0,5,10,15), (3,4,9,14), (2,7,8,13), or (1,6,11,12).

Proof. If the plaintexts differ only in one byte, they will be active in all four bytes of one column after the first MC operation. Then, after the second MC, the difference will be active in all bytes. On the other hand, if the ciphertexts are equal in one of the four prohibited combinations of bytes, after the third MC, the data will be equal in one column. Thus, before the third MC, the data in this column is also equal. Therefore, after the second MC, there are at least 4 bytes in which the data are equal. This is a contradiction because all bytes of the data differ after the MC in the forward direction. Therefore, this is impossible.

One possible case is illustrated in Figure 2.

Proposition 3 (Subtweakey difference cancellation)**.** As noticed by the designers [1], using the simple LFSR given in Subsection 2.1, a single subtweakey difference cancellation can occur every 15 rounds for Deoxys-BC-256. Suppose that a single cell of TK^1 and TK^2 are active. Let $a1$ and $a2$ be differences of the active cells, respectively. Then, the subtweakey difference of the first round is $a2 \bigoplus a1$ at this cell, and in the i-th round, the subtweakey difference is $a2 \bigoplus \mathrm{LFSR}^i(a1)$, ignoring the position permutation h. Because $a1$ and $a2$ are both nonzero differences, $a2 \bigoplus \mathrm{LFSR}^i(a1) = 0$ can occur once every 15 rounds.

2.4 Notation

- X_i represents the internal state after AK in round i.
- Y_i represents the internal state after SB in round i.
- Z_i represents the internal state after SR in round i.
- W_i represents the internal state after MC in round i.
- ΔS represents the difference value of S and S'.
- (S, S') represents a pair of internal states where $S \bigoplus S' = \Delta S$.

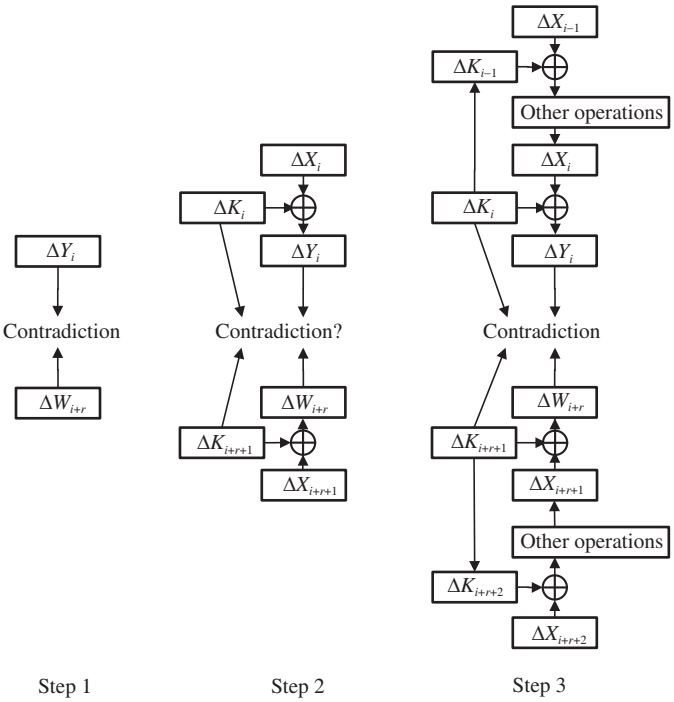

Figure 3 Search for longer related-key differential.

- $X[j]$ represents the j-th byte of X.
- $\overline{F}$ represents the inverse function of F.

3 Attack on Deoxys-BC-256

3.1 Longer related-key impossible distinguisher

In this subsection, we explain the process of extending a single-key impossible differential to a longer related-key impossible differential (see Figure 3).

First, suppose we already obtained an r-round single-key impossible differential of a cipher:

$$\Delta Y_i = \Delta\text{in} \nrightarrow \Delta\text{out} = \Delta W_{i+r}.$$

Then, we think about the related-key scenario. When we set $\Delta X_i = 0$ and $\Delta K_i = \Delta$in, after the AK operation, the internal state difference ΔY_i is also Δin as $\Delta Y_i = \Delta X_i \bigoplus \Delta K_i$. Similarly, when we set $\Delta X_{i+r+1} = 0$ and $\Delta K_{i+r+1} = \Delta$out, then $\Delta W_{i+r} = \Delta X_{i+r+1} \bigoplus \Delta K_{i+r+1} = \Delta$out. Now, we get the input and output difference of the original single-key distinguisher and check whether $\Delta K_i \to \Delta K_{i+r+1}$ is possible. Notice that not only ΔY_i and ΔW_{i+r} but also the key difference from ΔK_i to ΔK_{i+r+1} will influence the position of active nibbles from ΔY_i and ΔW_{i+r}. We need to check whether the contradiction still holds. If it does, we go to the next step; otherwise, we choose another single-key impossible differential and check in the same way.

If contradictions still exist, we can add one round both on the top and on the bottom of the distinguisher. According to the key schedule, we deduce ΔK_{i-1} and ΔK_{i+r+2} from ΔK_i and ΔK_{i+r+1}, respectively. After that, we set $\Delta X_{i-1} = \Delta K_{i-1}$ and $\Delta X_{i+r+2} = \Delta K_{i+r+2}$. This will ensure $\Delta X_i = 0$ and $\Delta X_{i+r+1} = 0$. Thus, we get the input and output difference of the distinguisher in the previous step.

Now, we extend the original differential by two more rounds. If possible, we can continue to extend more rounds in the same way.

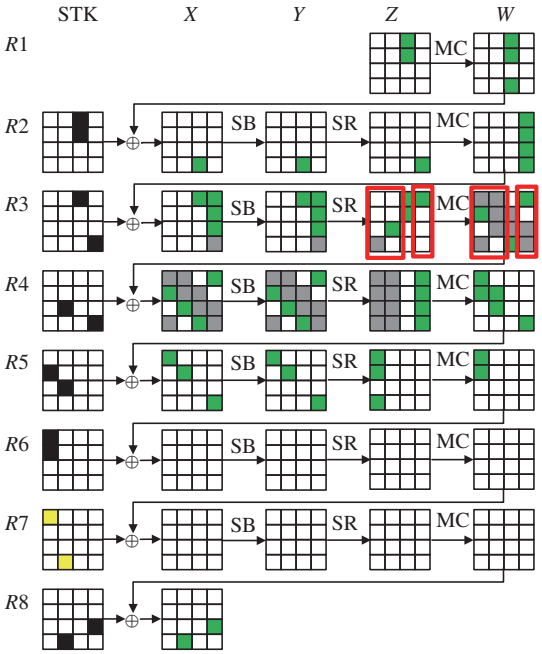

Figure 4 (Color online) Related-key impossible distinguisher of Deoxys-BC-256. Green nibbles indicate active bytes of cipher internal states, white nibbles indicate inactive bytes of internal states, gray nibbles indicate uncertain bytes, black nibbles indicate active bytes of the subtweakeys, and yellow nibbles indicate inactive bytes because of Proposition 3. Red boxes indicate contradictions of this distinguisher.

3.2 Search for related-tweakey impossible distinguisher with MILP method

MILP problems are mathematical optimization problems in which only some variables are constrained to be integers. The goal is to find the optimal value that minimizes/maximizes the objective function satisfying all of the inequality constraints. This was introduced in [13, 14] and improved in [15–18].

In [19, 20], two different automatic tools for searching impossible differentials with the MILP method are presented. However, the tool in [19] is not suitable for the related-key setting. In [20], the authors regard searching for the single-key impossible differential and the related-key impossible differential as two completely independent processes. By contrast, our method looks for related-key impossible differentials and tries to derive the relation between the single-key impossible differentials and the related-key impossible differentials.

By using the method described in Subsection 3.1 and the property of the tweakey schedule in Proposition 3, we extend two more rounds in the bottom of the single-key distinguisher in Figure 2 and seek out a six-round related-key distinguisher shown in Figure 4.

Next, we describe the modeling process.

Constraints for the tweakey schedule.

When considered only at the byte level, the subtweakey schedule of two successive rounds is just a byte permutation. We use $\mathrm{stk}_i[j]$ ($\mathrm{stk}_{i+1}[j']$) to denote the activeness of the corresponding relevant bytes in STK_i (STK_{i+1}). The constraint is

$$\mathrm{stk}_i[j] - \mathrm{stk}_{i+1}[j'] = 0, \quad j' = h(j).$$

When considered at the bit level, the subtweakey differences should satisfy several conditions.

(1) As shown in $R1$ of Figure 4, the MC operation is a 2-to-3 transformation from Z_1 to W_1, and $\Delta W_1[8, 9] = \Delta\mathrm{STK}_2[8, 9]$. To satisfy these two conditions, $3 \times \Delta\mathrm{STK}_2[8]$ should be equal to $\Delta\mathrm{STK}_2[9]$. As these operations are all in a finite field $\mathbb{K}$ (the irreducible polynomial is $x^8 + x^4 + x^3 + x + 1$), we can use eight variables to denote the 8-bit variable $\Delta\mathrm{STK}_i[j]$.

For example, $(a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ denotes

$$\Delta\mathrm{STK}_2[8] = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0,$$

and then

$$\begin{aligned}
&3 \times \Delta\mathrm{STK}_2[8] \\
&= (x+1) \cdot (a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0) \\
&= (a_6 \oplus a_7)x^7 + (a_5 \oplus a_6)x^6 + (a_4 \oplus a_5)x^5 + (a_3 \oplus a_4 \oplus a_7)x^4 \\
&\quad + (a_2 \oplus a_3 \oplus a_7)x^3 + (a_1 \oplus a_2)x^2 + (a_0 \oplus a_1 \oplus a_7)x + (a_0 \oplus a_7). \qquad (3)
\end{aligned}$$

$(b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0)$ denotes

$$\Delta\mathrm{STK}_2[9] = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0.$$

Then,

$$3 \times \Delta\mathrm{STK}_2[8] = \Delta\mathrm{STK}_2[9]$$

can be represented by

$$\begin{aligned}
&a_6 \oplus a_7 = b_7, \quad a_5 \oplus a_6 = b_6, \\
&a_4 \oplus a_5 = b_5, \quad a_3 \oplus a_4 \oplus a_7 = b_4, \\
&a_2 \oplus a_3 \oplus a_7 = b_3, \quad a_1 \oplus a_2 = b_2, \qquad (4) \\
&a_0 \oplus a_1 \oplus a_7 = b_1, \quad a_0 \oplus a_7 = b_0.
\end{aligned}$$

These equations can be described by MILP constraints. For example, $a_6 \oplus a_7 = b_7$ can be restrained by

$$a_6 + a_7 + b_7 - 2d_{\oplus} = 0, \qquad (5)$$

where $d_{\oplus}$ is a dummy bit variable.

$a_3 \oplus a_4 \oplus a_7 = b_4$ can be restrained by

$$\begin{aligned}
&-a_3 + a_4 + a_7 + b_4 \geqslant 0, \quad a_3 - a_4 + a_7 + b_4 \geqslant 0, \\
&a_3 + a_4 - a_7 + b_4 \geqslant 0, \quad a_3 + a_4 + a_7 - b_4 \geqslant 0, \\
&a_3 - a_4 - a_7 - b_4 \geqslant -2, \quad -a_3 + a_4 - a_7 - b_4 \geqslant -2, \qquad (6) \\
&-a_3 - a_4 + a_7 - b_4 \geqslant -2, \quad -a_3 - a_4 - a_7 + b_4 \geqslant -2.
\end{aligned}$$

The other equations in (3) can be described as MILP constraints in a similar way to (4) and (5).

(2) The difference of W_5 is equivalent to the difference of STK_6; and in the backward direction, W_4 has at most three active columns. Thus, after an MC operation, the corresponding column of Z_5 has at most 3 active bytes. What's more, after $\overline{\mathrm{SR}}$ and $\overline{\mathrm{SB}}$ operations in $R5$, the positions of active bytes in STK_5 and X_5 occupy at most three columns. For example, $\Delta Z_5[2] = 0$ is equivalent to $13 \times \Delta W_5[0] = 9 \times \Delta W_5[1]$. The modeling process is similar to that in Step 1.

(3) According to Proposition 3, we can set the 2 bytes in $R7$ inactive, so the corresponding two values should be zero. This means $\Delta\mathrm{TK}_7^1[1] = \Delta\mathrm{TK}_7^2[1]$ and $\Delta\mathrm{TK}_7^1[6] = \Delta\mathrm{TK}_7^2[6]$. The bit-level modeling process is simple and similar to that in Step 1.

Constraints for AK. We use $(w_{i-1}[j], \mathrm{stk}_i[j], x_i[j])$ to denote the activeness of the corresponding relevant bytes in $(W_{i-1}, \mathrm{STK}_i, X_i)$. Then, for $(w_{i-1}[j], \mathrm{stk}_i[j], x_i[j])$, the possible values are $(0,0,0)$, $(0,1,1)$, $(1,0,1)$, $(1,1,0)$, and $(1,1,1)$. We can use the following inequalities to include all five solutions:

$$\begin{aligned}
&w_{i-1}[j] + \mathrm{stk}_i[j] - x_i[j] \geqslant 0, \\
&w_{i-1}[j] - \mathrm{stk}_i[j] + x_i[j] \geqslant 0, \\
&-w_{i-1}[j] + \mathrm{stk}_i[j] + x_i[j] \geqslant 0.
\end{aligned}$$

Constraints for SB. As the SB operation does not change the activeness of a byte, it is equivalent to $y_i[j] - x_i[j] = 0$.

Constraints for SR. This operation is a byte permutation and does not change the activeness of bytes either. We use $z_i[j'] - y_i[j] = 0$ to denote SR with $j = \mathrm{SR}(j')$.

Constraints for MC. Modeling the MC operation is essentially expressing the transformation property of the MDS matrix with branch number 5. For all input and output differences, except the case where all of them are zero, the number of active bytes is at least 5. Then, the number of solutions is $2^8 - C_8^1 - C_8^2 - C_8^3 - C_8^4 = 94$. We use $(z_i[0], z_i[1], z_i[2], z_i[3], w_i[0], w_i[1], w_i[2], w_i[3])$ to denote the activeness of the eight input and output differences. The solutions can be denoted by the following inequalities:

$$\begin{aligned}
-4 \times z_i[0] + z_i[1] + z_i[2] + z_i[3] + w_i[0] + w_i[1] + w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] - 4 \times z_i[1] + z_i[2] + z_i[3] + w_i[0] + w_i[1] + w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] + z_i[1] - 4 \times z_i[2] + z_i[3] + w_i[0] + w_i[1] + w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] + z_i[1] + z_i[2] - 4 \times z_i[3] + w_i[0] + w_i[1] + w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] + z_i[1] + z_i[2] + z_i[3] - 4 \times w_i[0] + w_i[1] + w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] + z_i[1] + z_i[2] + z_i[3] + w_i[0] - 4 \times w_i[1] + w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] + z_i[1] + z_i[2] + z_i[3] + w_i[0] + w_i[1] - 4 \times w_i[2] + w_i[3] &\geqslant 0,\\
z_i[0] + z_i[1] + z_i[2] + z_i[3] + w_i[0] + w_i[1] + w_i[2] - 4 \times w_i[3] &\geqslant 0.
\end{aligned}$$

In order to satisfy the second constraint of the tweakey schedule, we need to add one more inequality for the MC in $R5$:

$$z_i[0] + z_i[1] + z_i[2] + z_i[3] + w_i[0] + w_i[1] + w_i[2] + w_i[3] \leqslant 5.$$

We add all the above constraints into the final model, and set the position of active bytes of the input and the output as fixed. If the returned result we get is 'infeasible', then the fixed differential is impossible. Finally, we get the impossible differential shown in Figure 4.

In the forward direction from Z_1 to Z_3, the number of active bytes of the first and last two columns of Z_3 is 1; in the backward direction from X_8 to W_3, the corresponding number in W_3 is 3. This is inconsistent with the transform property of an MDS matrix with branch number 5 as $1 + 3 = 4 < 5$.

As the MILP modeling process of the subtweakey difference values is at the bit level and the constraints are strict, we provide actual values of the differential characteristics conforming to the distinguisher in Table 3.

3.3 Attack process

We add two rounds both on the top and the bottom of the distinguisher in Subsection 3.2, and successfully mount a 10-round key recovery attack on Deoxys-BC-256, as shown in Figure 5.

In order to better attack the bottom two rounds, we bring forward the AK operation before the SR operation of the previous round, and use ruK_i to denote $\overline{\mathrm{SR}}(\overline{\mathrm{MC}}(\mathrm{STK}_i))$. To distinguish the original order, we use $X \xrightarrow{\mathrm{SB}} Y \xrightarrow{\mathrm{ruK}} \mathrm{ruX} \xrightarrow{\mathrm{SR}} \mathrm{ruZ} \xrightarrow{\mathrm{MC}} \mathrm{ruW}$ to denote the internal state in $R9$ and $R10$. Notice that like the difference value of STK, all differences of ruK are fixed and known.

The attack process is as follows:

(1) Construct 2^n structures in which each structure is made up of 2^{64} plaintexts. In each structure, we set $\Delta P[15] = \Delta\mathrm{STK}_0[15]$ and $\Delta P[1, 2, 6, 7, 8, 11, 12, 13]$ for the 8 active bytes. Then, each structure will provide 2^{128} pairs.

(2) Choose $(\mathrm{KT}, \mathrm{KT}')$ in that the tweakey difference satisfies the subtweakey difference trail in Figure 5. Encrypt the plaintexts under two tweakeys, and only choose the pairs that satisfy $\overline{\mathrm{MC}}(\Delta C)[1, 2, 4, 5, 14, 15] = 0$ and $\overline{\mathrm{MC}}(\Delta C)[11] = \Delta\mathrm{ruK}_{10}[7]$. In total, we get 2^{72+n} pairs.

(3) For each of the remaining pairs, perform the following steps:

(3.1) Guess the value of $\Delta W_0[8, 13]$. Because $\Delta W_0[15] = \Delta\mathrm{STK}_1[15]$ and $\Delta\mathrm{STK}_1[15]$ is known, we can deduce the value of $\Delta Z_0[8, 9, 10, 11, 12, 13, 14, 15]$ by an $\overline{\mathrm{MC}}$ operation. The value of $\Delta Y_0[1, 2, 6, 7, 8, 11, 12,$

Table 3 Actual values of impossible differential conforming the distinguisher

Round	Index	ΔTK^1	ΔTK^2	ΔSTK	ΔX	ΔZ	ΔW
1	8	–	–	–	–	0x3d	0x3d
	9	–	–	–	–	0x3d	0x47
	10	–	–	–	–	0x00	0x00
	11	–	–	–	–	0x00	0x7a
2	8	0x66	0x5b	0x3d	–	–	–
	9	0x36	0x71	0x47	–	–	–
	11	–	–	–	0x7a	–	–
3	9	0x66	0xb6	0xd0	–	–	–
	14	0x36	0xe3	0xd5	–	–	–
4	14	0x66	0x6c	0x0a	–	–	–
	7	0x36	0xc6	0xf0	–	–	–
5	7	0x66	0xd9	0xbf	–	–	–
	0	0x36	0x8d	0xbb	–	0x3e	0xd5
	1	–	–	–	–	0xba	0x2d
	2	–	–	–	–	0x00	–
	3	–	–	–	–	0x7c	–
6	0	0x66	0xb3	0xd5	–	–	–
	1	0x36	0x1b	0x2d	–	–	–
7	1	0x66	0x66	0x00	–	–	–
	6	0x36	0x36	0x00	–	–	–
8	6	0x66	0xcd	0xab	0xab	–	–
	15	0x36	0x6d	0x5b	0x5b	–	–

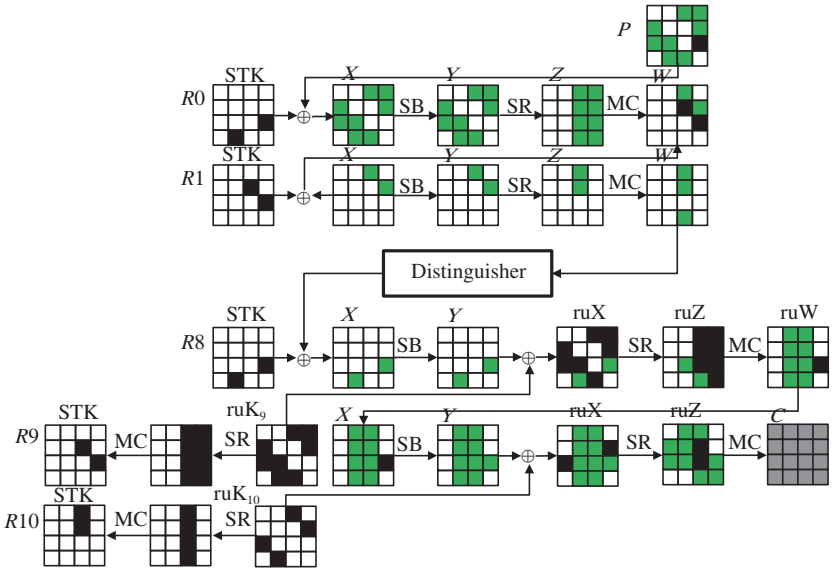

Figure 5 (Color online) Attack process on 10-round Deoxys-BC-256. Black boxes in internal state mean these byte differences are brought from subtweakey differences or are equivalent to difference of some subtweakey bytes.

13] is also known as $Y_0[1,2,6,7,8,11,12,13] = \overline{\mathrm{SR}}(Z_0[8,9,10,11,12,13,14,15])$. Moreover, we can deduce the value of $\Delta X_0[1,2,6,7,8,11,12,13]$ according to the plaintext pair and $\Delta\mathrm{STK}_0$. Using Proposition 1, we get the value of $X_0[1,2,6,7,8,11,12,13]$. Then, we can get 8 bytes of information of the tweakey as $\mathrm{STK}_0[1,2,6,7,8,11,12,13] = P[1,2,6,7,8,11,12,13] \oplus X_0[1,2,6,7,8,11,12,13]$.

(3.2) In step (3.1), we also get the value of $Y_0[1,2,6,7,8,11,12,13]$. After SR and MC operations, we can get the value of $W_0[8,13]$. In addition, as $\Delta X_1[8] = \Delta W_0[8] \oplus \Delta\mathrm{STK}_1[8]$ and $\Delta X_1[13] = \Delta W_0[13]$, $\Delta X_1[8,13]$ is also known. As shown in Table 3, $\Delta Z_1[8,9]$ is also known. We can also know the value

of $\Delta Y_1[8,13]$ as $\Delta Y_1[8,13] = \Delta Z_1[8,9]$. Using Proposition 1, we can deduce the value of $X_1[8,13]$. By combining it with the known value of $W_0[8,13]$, we can get the value of $\mathrm{STK}_1[8,13]$.

(3.3) Guess the value of $\Delta Y_8[6,15]$. As $\Delta\mathrm{ruX}_8[15] = \Delta Y_8[15]$, $\Delta\mathrm{ruX}_8[1,2,7,8,11,12,13] = \Delta\mathrm{ruK}_9[1,2,7,8,11,12,13]$, and $\Delta\mathrm{ruX}_8[6] = \Delta Y_8[6] \oplus \Delta\mathrm{ruK}_9[6]$, we can know the value of all active bytes of ruX_8 (the value of ΔruK is fixed and known). After SR and MC operations, we can get the value of $\Delta X_9[0,1,2,3,8,12,13,14,15]$.

In the backward direction, we can get the difference value of ruX_9 from the ciphertext pairs. As $\Delta\mathrm{ruK}_{10}$ is known, we can get the value $\Delta Y_9[0,1,2,3,8,12,13,14,15]$ from $\Delta\mathrm{ruX}_9[0,1,2,3,7,8,12,13,14,15] \oplus \Delta\mathrm{ruK}_{10}[2,7,8,13]$.

Using Proposition 1, we can deduce the value of $Y_9[0,1,2,3,8,12,13,14,15]$. From the ciphertext value, we can deduce the value of $\mathrm{ruX}_9[0,1,2,3,8,12,13,14,15]$ after $\overline{\mathrm{SR}}$ and $\overline{\mathrm{MC}}$ operations. Thus, we can get 9 bytes of information of the tweakey: $\mathrm{ruK}_{10}[0,1,2,3,8,12,13,14,15] = Y_9[0,1,2,3,8,12,13,14,15] \oplus \mathrm{ruX}_9[0,1,2,3,8,12,13,14,15]$.

(3.4) In step (3.3), we also get the value of $X_9[0,1,2,3,8,12,13,14,15]$ using Proposition 1. As $\mathrm{ruW}_8 = X_9$, the value of the corresponding bytes of ruW_8 is also known. After an $\overline{\mathrm{MC}}$ operation, we can deduce the value $\mathrm{ruZ}_8[3,14]$. Thus, the value of $\mathrm{ruX}_8[15,6]$ is known as $\mathrm{ruX}_8[15,6] = \mathrm{ruZ}_8[3,14]$.

As $\Delta X_8[15,6] = \Delta\mathrm{STK}_8[15,6]$ is known, by combining it with the guessed value of $\Delta Y_8[15,6]$, we can deduce the value of $Y_8[15,6]$ using Proposition 1.

Thus, we get another 2 bytes of information of the tweakey: $\mathrm{ruK}_9[15,6] = Y_8[15,6] \oplus \mathrm{ruX}_8[15,6]$.

(4) We exhaustively search the left key bits and recover the entire tweakey.

Complexity computation.

In total, we can deduce $8+2+9+2 = 21$ bytes, or 168 bits of information of the tweakey. As we guess 2^{32} values of $(\Delta W_0[8,13], \Delta Y_8[15,6])$, each pair can eliminate 2^{32} values of the 168-bit guessed tweakey information. To satisfy $2^{168} \times (1 - 2^{32}/2^{168})^{2^{72+n}} \ll 1$, we choose $n = 71$.

The data complexity is $2^{64+71} = 2^{135}$ plaintexts. The time complexity of step (1) for encrypting the plaintexts is $2 \cdot 2^{64+71} = 2^{136}$. In step (3), the total number of guesses is $2^{72+n+32} = 2^{175}$, which is equivalent to $2^{175} \cdot (8/16 + 2/16 + 2/16 + 9/16) \cdot 1/10 \cdot 2 \approx 2^{173.1}$ 10-round encryptions. Thus, the time complexity is approximately $2^{173.1}$ 10-round encryptions.

Impact on Deoxys authenticated encryption.

We stated that the analysis result has no impact on Deoxys when it uses r-round ($r \geqslant 10$) Deoxys-BC-256 as its primitive with the recommended parameters in [1]: the key size of both Deoxys-I and Deoxys-II based on Deoxys-BC-256 is 128 bits, as the time complexity of our attack is $2^{173.1}$, which is larger than 2^{128}.

However, Deoxys with nine-round Deoxys-BC-256 can be attacked. An attack against nine-round Deoxys-BC-256 can be mounted by removing the last round of the 10-round attack. As the used techniques are similar, we skip the details and only present the main attack results for Deoxys-BC-256. For this nine-round attack, the relevant tweakey nibbles is $8+2+2 = 12$. To recover the 96-bit tweakey information, we need both data complexity and time complexity to be 2^{119}. In fact, after filtering the pairs, the time complexity to recover the key by guessing $(\Delta W_0[8,13], \Delta Y_8[15,6])$ is about 2^{101}, so the time complexity is dominated by encrypting the 2^{119} plaintexts. As the data complexity is less than 2^{124} and the time complexity is less than 2^{128}, this implies Deoxys with nine-round Deoxys-BC-256 can be attacked.

4 Conclusion

In this paper, we introduced a method that can seek out longer related-key impossible differentials from single-key impossible differentials. Using this method, we find a six-round related-key impossible distinguisher of Deoxys-BC-256 by applying the MILP method. Based on this distinguisher, we mount a 10-round attack that can attack the cipher with a wider range of key sizes compared with previous results.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2017YFA0303903), National Natural Science Foundation of China (Grant No. 61672019), National Cryptography Development Fund (Grant No. MMJJ20170121), Zhejiang Province Key R&D Project (Grant No. 2017C01062), Fundamental Research Funds of Shandong University (Grant No. 2016JC029), and China Postdoctoral Science Foundation (Grant No. 2017M620807).

References

1 Jean J, Nikolić I, Peyrin T, et al. Deoxys v1.41. 2016. http://competitions.cr.yp.to/round3/deoxysv141.pdf
2 Daemen J, Rijmen V. The design of rijndael. In: AES - the Advanced Encryption Standard. Berlin: Springer, 2002
3 Liskov M, Rivest R L, Wagner D. Tweakable block ciphers. J Cryptol, 2011, 24: 588–613
4 Beierle C, Jean J, Kölbl S, et al. The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Advances in Cryptology - CRYPTO 2016. Berlin: Springer, 2016. 123–153
5 Borghoff J, Canteaut A, Gneysu T, et al. PRINCE - a low-latency block cipher for pervasive computing applications. In: Advances in Cryptology - ASIACRYPT 2012. Berlin: Springer, 2012. 208–225
6 Avanzi R. The QARMA block cipher family - almost MDS matrices over rings with zero divisors, nearly symmetric Even-Mansour constructions with non-involutory central rounds, and search heuristics for low-latency S-Boxes. IACR Trans Symmetric Cryptol, 2017, 1: 4–44
7 Jean J, Nikolić I, Peyrin T. Tweaks and keys for block ciphers: The TWEAKEY framework. In: Advances in Cryptology - ASIACRYPT 2014. Berlin: Springer, 2014. 274–288
8 Cid C, Huang T, Peyrin T, et al. A security analysis of Deoxys and its internal tweakable block cphers. IACR Trans Symmetric Cryptol, 2017, 3: 73–107
9 Ankele R, Banik S, Chakraborti A, et al. Related-key impossible-differential attack on reduced-round SKINNY. In: Applied Cryptography and Network Security - ACNS 2017. Berlin: Springer, 2017. 208–228
10 Bellare M, Hoang V, Tessaro S. Message-recovery attacks on Feistel-based format preserving encryption. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Seucrity, Vienna, 2016. 444–455
11 Derbez P, Fouque P-A, Jean J. Improved key recovery attacks on reduced-round AES in the single-key setting. In: Advances in Cryptology - EUROCRYPT 2013. Berlin: Springer, 2013. 371–387
12 Biham E, Keller N. Cryptanalysis of reduced variants of Rijndael. In: Prcoeedings of the 3rd AES Candidate Conference, New York, 2000
13 Mouha N, Wang Q J, Gu D W, et al. Differential and linear cryptanalysis using mixed-integer linear programming. In: Proceedings of the 7th International Conference on Information Security and Cryptology, Beijing, 2011. 57–76
14 Wu S B, Wang M S. Security evaluation against differential cryptanalysis for block cipher structures. https://eprint.iacr.org/2011/551
15 Sun S W, Hu L, Wang P, et al. Automatic security evaluation and (related-key) differential characteristic search: Application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Advances in Cryptology - ASIACRYPT 2014. Berlin: Springer, 2014. 158–178
16 Sun S W, Hu L, Song L, et al. Automatic security evaluation of block ciphers with S-bP structures against related-key differential attacks. In: Proceedings of International Conference on Information Security and Cryptology. Berlin: Springer, 2013. 39–51
17 Sun S W, Hu L, Wang M Q, et al. Towards finding the best characteristics of some bit-oriented blcok ciphers and automatic enumeration of (related-key) differential and linear characteristics with predefined properties. https://eprint.iacr.org/2014/747
18 Fu K, Wang M Q, Guo Y H, et al. MILP-based automatic search algorithms for differential and linear trails for Speck. In: Fast Software Encryption - FSE 2016. Berlin: Springer, 2016. 268–288
19 Sasaki Y, Todo Y. New impossible differential search tool from design and cryptanalysis aspects. In: Advances in Cryptology - EUROCRYPT 2017. Berlin: Springer, 2017. 185–215
20 Cui T T, Jia K T, Fu K, et al. New automatic search tool for impossible differentials and zero-correlation linear approximations. http://eprint.iacr.org/2016/689