Finding Impossible Differentials for Rijndael-like and 3D-like Structures

Ting Cui, Chen-hui Jin
Information Science and Technology Institute
Zhengzhou, 450004 - China
[e-mail: cuiting_1209@yahoo.com.cn]
*Corresponding author: Ting Cui

Received October 14, 2012; revised February 13, 2013; revised March 7, 2013;
accepted March 19, 2013; published March 29, 2013

Abstract

Impossible Differential Cryptanalysis (IDC) uses impossible differentials to discard wrong subkeys for the first or the last several rounds of block ciphers. Thus, the security of a block cipher against IDC can be evaluated by impossible differentials. This paper studies impossible differentials for Rijndael-like and 3D-like ciphers, we introduce methods to find 4-round impossible differentials of Rijndael-like ciphers and 6-round impossible differentials of 3D-like ciphers. Using our methods, various new impossible differentials of Rijndael and 3D could be searched out.

Keywords: Block cipher, impossible differential, Rijndael structure, 3D structure.
1. Introduction

Impossible differential cryptanalysis (IDC) was first proposed by Knudsen [14] and Biham [1] to attack DEAL and Skipjack. It is known as one of the most powerful attacks on block ciphers. This cryptanalysis has attracted wide attention and many good results are achieved [1,2,3,7,9,10,11,13,17].

Compared with traditional differential cryptanalysis, IDC considers the differential characteristics with probability 0, when a pair of plaintexts satisfies the input difference of the characteristics, the difference of ciphertexts decrypted by the right subkey never satisfy the output difference of characteristics. By this way we can discard wrong subkeys and recover the right subkey. Impossible differential attack is composed of two steps: finding the longest characteristics and recovering the subkeys. Retrieving the characteristics often use the idea of “miss-in-the-middle”, namely to find two differential characteristics with probability 1 from encryption and decryption, and connect them together when there are some inconsistencies in the middle. As is suggested by [4], the key step of IDC is to retrieve the longest impossible differentials. In [4,5], two methods were provided to find impossible differentials of various block ciphers, but both of them have their limitations and some important inconsistencies are ignored [6].

This paper focuses on finding new impossible differentials for two block ciphers: the Rijndael-like block ciphers and the 3D-like ciphers. The cipher Rijndael [7] was submitted to the AES (Advanced Encryption Standard) and was later selected as the AES. Since its selection, Rijndael has received a great deal of attentions, both in block cipher design and cryptanalysis. In [9], 4-round impossible differential of AES128 is detected for the first time, and this ID distinguisher was used in most later IDC results (e.g. in [2] and [17]). And in [10], some new impossible differentials of AES are searched out. In CANS 2008, the new iterated block cipher 3D [8] was designed inspired by AES. The novel design of 3D cipher also attracts some research interests: in 2010, Tang et al proposed a 6-round impossible differential of 3D cipher and attack 9-round 3D cipher [10], then later in ISPEC 2011, Jorge launched a 10-round impossible differential attack by using new 6-round distinguisher of 3D cipher [15], and Takuma et al presented 11- and 13-round attacks on 3D with the truncated differential cryptanalysis in [16], now is approved to be the best attack on 3D.

Although impossible differential cryptanalysis does not give the best attack on these two ciphers [18,16], impossible differential properies still need to be sufficiently considered. Up to now, the longest impossible differential for AES-128 is still 4-round [9,10], while the longest impossible differential for 3D cipher is 6-round [11,15]. In this paper, we will present new methods to find impossible differentials of these two structures. By applying our results, various new impossible differentials of these two block ciphers can be searched out.

Our paper is organized as follows. In Section 2, we introduce some basic notions. In Section 3 and 4, we find various impossible differentials of these two structures. In Section 5, we draw conclusions.

2. Preliminaries

We will introduce some basic notations and definitions through this paper.

\[ \oplus \] the bitwise XOR;

\[ + \] the addition over real number space;
the compound operation of two functions;
\#\{\bullet\} the number of elements in a set;
\Delta x \quad \text{the XOR difference of } \ x \text{ and } x';
\omega(X) \quad \text{the number of nonzero components of vector } X.

**Definition 1** [12]. Let \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) and \( \alpha, \beta \in \{0,1\}^n \), the differential probability of \( f \) is defined by

\[
p_f(\alpha \rightarrow \beta) = \frac{1}{2^n} \#\{x \in \{0,1\}^n : f(x) \oplus f(x \oplus \alpha) = \beta\}.
\]

It is widely known that if \( f \) is a bijection with \( p_f(\alpha \rightarrow \beta) > 0 \), then \( \alpha \neq 0 \) iff \( \beta \neq 0 \).

**Definition 2** [7]. (branch number) Let \( f(x) = M \times x \), where \( M = (m_{ij})_{n\times n} \) is a matrix over \( GF(2^m) \), and \( x \) is a \( n \times 1 \) vector over \( GF(2^m) \). Then the branch number of \( f \) is defined by

\[
Br(f) = \min\{w(x) + w(Mx) : x \in GF(2^m)^n \setminus \{0\}\}.
\]

**Definition 3** [12]. (differential active S-box) A differential active S-box is defined as an S-box whose input difference is non-zero.

### 2.1. Brief Description of Rijndael-like Structure

The Rijndael-like structure operates on \( n \times n \)-word state, which is represented as a \( n \times n \) state of words(a \( n \times n \) matrix), and the state for a \( 2^n \) data-block, \( (x_0,0, \cdots, x_{n-1,0}, x_0,1, \cdots, x_{n-1,n-1}) \), is denoted by the word matrix \( X = (x_{i,j})_{n\times n} \). Each round of Rijndael-like structure is composed of four operations:

\[
Round_{\text{Rijndael}}(X) = \text{ARK} \circ \text{MC} \circ \text{SR} \circ \text{SB}(X),
\]

where

- **SubBytes (SB):** applying the bijective S-box \( S \) on each word, i.e.
  \[
  \text{SB} : (x_{i,j})_{n\times n} \rightarrow (y_{i,j})_{n\times n}, y_{i,j} = s(x_{i,j});
  \]

- **ShiftRows (SR):** cyclically shifting each row, i.e.
  \[
  \text{SR} : (x_{i,j})_{n\times n} \rightarrow (r_{i,j})_{n\times n}, r_{i,j} = x_{(i+\text{mod}_n)}(j);\]

- **MixColumns (MC):** multiplication of each column by a constant \( n \times n \) matrix, i.e.
  \[
  \text{MC} : (x_{i,j})_{n\times n} \rightarrow M_{n\times n}(x_{i,j})_{n\times n};
  \]

- **AddRoundKey (ARK):** XORing the state and a \( n^2 \)-word subkey, i.e.
  \[
  \text{ARK}(X) = X \oplus K_i;
  \]

where \( K_i \) is the round key.

Like all other works on Rijndael cipher, we assume the last MC operation is omitted.

### 2.2 Brief Description of 3D-like Structure

The 3D-like structure also has an SPN structure, message block is represented as a 3-dimensional cube(\( n \times n \times n \) state of words, see Fig. 1), and in this paper, we represented the cube as a matrix...
For any fixed $0 \leq k \leq n - 1$, the matrix $(x_{i,j})_{kn}$ is said to be the $k$-th vertical slice of the cube (see Fig. 1).

**Fig. 1.** State cube of 3D-like structure

The $i$-th round of 3D-like structure is composed of four operations:

$$
\tau_i(X) = \pi \circ \theta_{mod2^i} \circ \gamma \circ \kappa_i(X),
$$

where

- $\kappa_i$: XORing the state and a $n^3$-word $i$-th round subkey, i.e.
  $$\kappa_i(X) = X \oplus K_i,$$
  where $K_i$ is the $i$-th round subkey;

- $\gamma$: applying the bijective S-box $s$ on each word, i.e.
  $$\gamma(X) = (s(x_{0,0,0}), \ldots, s(x_{n-1,n-1,n-1}));$$

- $\theta_1, \theta_2$: cyclically shifting operations, where $\theta_1$ operates within each vertical slice and $\theta_2$ operates between different vertical slices, i.e.
  $$\theta_1: (x_{k,i,j})_{kn} \rightarrow (y_{k,i,j})_{kn}, y_{k,i,j} = x_{k,i,(j+t_i) \mod n}, \text{ where } \{t_i : 0 \leq i \leq n - 1\} = Z_n;$$
  and
  $$\theta_2: (x_{k,i,j})_{kn} \rightarrow (z_{k,i,j})_{kn}, z_{k,i,j} = x_{(k+c_i) \mod n,i,j}, \text{ where } \{c_i : 0 \leq i \leq n - 1\} = Z_n;$$

For brevity, we call $\theta_1$ SWS (Shift within Slice) and $\theta_2$ SBS (Shift between Slices) for short;

- $\pi$: multiplication of each column of the state cube by a constant $n \times n$ matrix, i.e.
  $$\pi(X) = M_{non} \times X.$$  

Likewise, we omit the last $\pi$ operation.

### 3. Retrieving Impossible Differentials for Rijndael-like Cipher

In this section, we will provide some 4-round impossible differentials for Rijndael-like
structure by using the inconsistency of the MixColumn layer in the 2\textsuperscript{nd} round. The transformation we considered is

\[
T(X) = (ARK \circ SR \circ SB_4) \circ (ARK \circ MC \circ SR \circ SB_3) \\
\circ (ARK \circ MC \circ SR \circ SB_3) \circ (ARK \circ MC \circ SR \circ SB_3)(X)
\]

**Definition 4.** (collection set of SR). Let \( SR : (x_{i,j})_{\text{even}} \rightarrow (r_{i,j})_{\text{even}} \) with \( r_{i,j} = x_{i,(j+t_i)\mod n} \),

then the \( j \)-th \((0 \leq j \leq n-1)\) collection set of \( SR \) is defined by

\[
\Omega_j = \{(i, (j+t_i) \mod n) : 0 \leq i \leq n-1\}.
\]

For the input state matrix \( X_{\text{even}} = (x_{i,j}) \), if \( (i, j) \in \Omega_j \), then the \( SR \) operation will move \( x_{i,j} \) to the \( l \)-th column.

**Example 1.** For AES-128, the \( SR \) layer is defined as

\[
\begin{bmatrix}
x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\
x_{1,0} & x_{1,1} & x_{1,2} & x_{1,3} \\
x_{2,0} & x_{2,1} & x_{2,2} & x_{2,3} \\
x_{3,0} & x_{3,1} & x_{3,2} & x_{3,3}
\end{bmatrix} \rightarrow
\begin{bmatrix}
x_{0,0} & x_{0,1} & x_{0,2} & x_{0,3} \\
x_{1,1} & x_{1,2} & x_{1,3} & x_{1,0} \\
x_{2,2} & x_{2,3} & x_{2,0} & x_{2,1} \\
x_{3,3} & x_{3,0} & x_{3,1} & x_{3,2}
\end{bmatrix}_{SR},
\]

where \( t_0 = 0, t_1 = 1, t_2 = 2, t_3 = 3 \), thus

\[
\Omega_0 = \{(0,0),(1,1),(2,2),(3,3)\}, \Omega_1 = \{(0,1),(1,2),(2,3),(3,0)\}, \\
\Omega_2 = \{(0,2),(1,3),(2,0),(3,1)\}, \Omega_3 = \{(0,3),(1,0),(2,1),(3,2)\}.
\]

The properties below are trivial.

**Property 1.** For a given input difference state matrix:

1. \( ARK, SB, ARK^{-1}, SB^{-1} \) change neither the number nor the coordinates of differential active S-boxes;

2. \( SR, SR^{-1} \) do not change the number of differential active S-boxes;

3. \( MC, MC^{-1} \) only influence current column.

**Theorem 1.** Let \( M_{\text{even}} \) be the matrix representation of the MixColumn transformation with branch number \( d+1 \). Let the collection sets of \( SR \) and \( SR^{-1} \) be \( \Omega_0, \ldots, \Omega_{n-1} \) and \( \Phi_0, \ldots, \Phi_{n-1} \), respectively. If \( \Delta x_{p_1,i_1}, \ldots, \Delta x_{p_t,i_t}, \Delta y_{q_1,j_1}, \ldots, \Delta y_{q_t,j_t} \) are nonzero, and for some \( z_1 + z_2 \leq d \) hold

\[
\{(p_1,i_1), \ldots, (p_t,i_t)\} \subseteq \bigcup_{u=1}^{z_1} \Omega_{k_u}, \{(q_1,j_1), \ldots, (q_t,j_t)\} \subseteq \bigcup_{v=1}^{z_2} \Phi_{k_v},
\]

then

\[
(0, \ldots, 0, \Delta x_{p_1,i_1}, 0, \ldots, 0, \Delta x_{p_t,i_t}, 0, \ldots, 0) \rightarrow (0, \ldots, 0, \Delta y_{q_1,j_1}, 0, \ldots, 0, \Delta y_{q_t,j_t}, 0, \ldots, 0)
\]

is a 4-round impossible differential of Rijndael-like cipher.

**Proof.** Assume the input difference is \( \Delta X = (0, \ldots, 0, \Delta x_{p_1,i_1}, 0, \ldots, 0, \Delta x_{p_t,i_t}, 0, \ldots, 0) \), we
will bound the number of active S-boxes in
\[(SR_2 \circ SB_2) \circ (ARK_1 \circ MC_1 \circ SR_i \circ SB_j)(\Delta X).\]

Since \(\{(p_i, i_i), \cdots, (p_i, i_i)\} \subseteq \bigcup_{a=1}^{z_1} \Omega_{k_a}\), then the active S-boxes in \((MC_i \circ SR_i \circ SB_j)(\Delta X)\) only appear in the \(k_i, \cdots, k_i - \text{th}\) columns. Thus there are at most \(nz_1\) active S-boxes in
\[(SR_2 \circ SB_2) \circ (ARK_1 \circ MC_1 \circ SR_i \circ SB_j)(\Delta X).\]

From the decrypt direction, assume the output difference is \(\Delta Y = (0, \cdots, 0, \Delta y_{q_j - h}, 0, \cdots, 0, \Delta y_{q_j - h}, 0, \cdots, 0)\), and we will discuss the number of active S-boxes in
\[ARK_2^{-1} \circ (SB_1^{-1} \circ SR_3^{-1} \circ MC_3^{-1} \circ ARK_3^{-1}) \circ (SB_4^{-1} \circ SR_4^{-1} \circ ARK_4^{-1})(\Delta Y).\]

Since \(\{(q_i, j_i), \cdots, (q_i, j_i)\} \subseteq \bigcup_{z_2} \Phi_{l_i}\), then the active S-boxes of
\[(MC_3^{-1} \circ ARK_3^{-1}) \circ (SB_4^{-1} \circ SR_4^{-1} \circ ARK_4^{-1})(\Delta Y)\]
only appear in the \(h_i, \cdots, h_i\) th columns. Hence there are at most \(nz_2\) active S-boxes in
\[ARK_2^{-1} \circ (SB_1^{-1} \circ SR_3^{-1} \circ MC_3^{-1} \circ ARK_3^{-1}) \circ (SB_4^{-1} \circ SR_4^{-1} \circ ARK_4^{-1})(\Delta Y).\]

Taking \(MC_2\) into consideration: in the input state matrix of \(MC_2\), we affirm that there is at least one column \(\alpha\) satisfies
\[w(\alpha) + w(MC_2(\alpha)) \leq d\]
(otherwise the total number of active S-boxes in the state matrices before and after \(MC_2\) will be at least \(nd \geq nz_1 + nz_2\), this leads contradiction). On the other hand, we notice that \(Br(MC_2) = d + 1\), this indicates \(w(\alpha) + w(MC_2(\alpha)) \geq d + 1\). Thus \(\Delta X \rightarrow \Delta Y\) is a 4-round impossible differential of Rijndael-like cipher.

\[\square\]

In Rijndael cipher (see Appendix A), the branch number of the Mixcolumn transformation reaches 5 [7]. By applying Theorem 1, we find various impossible differentials. For briefness, we denote the input word matrix of Rijndael by
\[
X = \begin{bmatrix}
  x_0 & x_4 & x_8 & x_{12} \\
  x_1 & x_5 & x_9 & x_{13} \\
  x_2 & x_6 & x_{10} & x_{14} \\
  x_3 & x_7 & x_{11} & x_{15}
\end{bmatrix}
\]
and the output word matrix of 4-round Rijndael encryption by
\[
Y = \begin{bmatrix}
  y_0 & y_4 & y_8 & y_{12} \\
  y_1 & y_5 & y_9 & y_{13} \\
  y_2 & y_6 & y_{10} & y_{14} \\
  y_3 & y_7 & y_{11} & y_{15}
\end{bmatrix}.
\]

**Corollary 1.** Let \(\Delta X = (x_0, \cdots, x_{15}), \Delta Y = (y_0, \cdots, y_{15})\) be input difference and output difference of 4-round Rijndael, respectively. If \(\{i: \Delta x_i \neq 0\} \subseteq I, I \in Input_k\) and \(\{j: \Delta y_j \neq 0\} \subseteq O, O \in Output_k\) hold for some \(1 \leq k \leq 3\), then \(\Delta X \rightarrow \Delta Y\) is a 4-round
impossible differential of Rijndael. Where the index set $Input_k$ and $Output_k$ are listed in Table 1.

<table>
<thead>
<tr>
<th>$k$</th>
<th>$Input_k$</th>
<th>$Output_k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${0,5,10,15}$, ${3,4,9,14}$, ${2,7,8,13}$, ${1,6,11,12}$</td>
<td>${0,7,10,13}$, ${1,4,11,14}$, ${2,5,8,15}$, ${3,6,9,12}$</td>
</tr>
<tr>
<td>2</td>
<td>${0,3,4,5,9,10,14,15}$, ${0,2,5,7,8,10,13,15}$, ${0,1,5,6,10,11,12,15}$, ${2,3,4,7,8,9,13,14}$, ${1,3,4,6,9,11,12,14}$, ${1,2,6,7,8,11,12,13}$</td>
<td>${0,1,4,7,10,11,13,14}$, ${0,2,5,7,8,10,13,15}$, ${0,3,6,7,9,10,12,13}$, ${1,2,4,5,8,11,14,15}$, ${1,3,4,6,9,11,12,14}$, ${2,3,5,6,8,9,12,15}$</td>
</tr>
<tr>
<td>3</td>
<td>${1,2,3,4,6,7,8,9,11,12,13,14}$, ${0,1,2,5,6,7,8,10,11,12,13,15}$, ${0,1,3,4,5,6,9,10,11,12,14,15}$, ${0,2,3,4,5,7,8,9,10,13,14,15}$</td>
<td>${0,1,2,4,5,7,8,10,11,13,14,15}$, ${0,1,3,4,6,7,9,10,11,12,13,14}$, ${0,2,3,5,6,7,8,9,10,12,13,15}$, ${1,2,3,4,5,6,8,9,11,12,14,15}$</td>
</tr>
</tbody>
</table>

**Example 2.** We choose input difference whose $0,3,5,9,10,14,15$-th words are nonzero, and output difference whose $0,1,4,7,10,11,13,14$-th words are nonzero, thus we can construct impossible differential

$$(\Delta_0, 0,0,\Delta_5,0,\Delta_9,\Delta_{10},0,0,\Delta_{14},\Delta_{13})$$

$$\rightarrow (\delta_0,\delta_5,0,0,\delta_9,0,0,\delta_{10},0,\delta_{11},0,\delta_{13},\delta_{14},0)$$

via Corollary 1. We depict such impossible differential of Rijndael in Fig. 2, where we ignore the KeyAddition operation since it does not affect the differential state.
By observation, the impossible differentials proposed by [9] and [10] (see Fig.3) are special cases of ours.

Fig. 3. Typical 4-round impossible differential of Rijndael in [9] and [10]

4. Retrieving Impossible Differentials for 3D-like Cipher

In this section, we will provide some 6-round impossible differentials for 3D-like structure by using the inconsistency of the $\pi$ layer in the $3^{rd}$ round function. The cipher which we study excludes the last $\pi$ operation, i.e.

$$T(X) = (\theta \circ \gamma \circ \kappa) \circ (\pi \circ \theta_{\text{mod}2+1} \circ \gamma \circ \kappa)(X)$$

Definition 5 (collection set of SWS). Let $\theta_1 : (x_{k,i,j})_{\text{nona}} \rightarrow (y_{k,i,j})_{\text{nona}}$ with $y_{k,i,j} = x_{k,i,j+t,i} \mod n$ be the SWS of 3D-like cipher, then the $(k,j)$-collection set of $\theta_1$ is defined as

$$\Omega_{1(k,j)} = \{(k,i,(j+t,i) \mod n) : 0 \leq i \leq n-1\}.$$

Definition 6 (collection set of SBS). Let $\theta_2 : (x_{k,i,j})_{\text{nona}} \rightarrow (z_{k,i,j})_{\text{nona}}$ with $z_{k,i,j} = x_{k,i,j+c,n,i,j} \mod n$ be the SBS of 3D-like cipher, then the $(k,j)$-collection set of $\theta_2$ is defined as

$$\Omega_{2(k,j)} = \{(k+c,i) \mod n,i,j) : 0 \leq i \leq n-1\}.$$

For the cube $X = (x_{k,i,j})_{\text{nona}}$, if the subscripts of $x_{k_1,i_1,j_1}$ and $x_{k_2,i_2,j_2}$ satisfies $(k_1,i_1,j_1),(k_2,i_2,j_2) \in \Omega_{(k,j)}$, then transformation $\theta_i \in \{1,2\}$ will move $x_{k_1,i_1,j_1}$ and $x_{k_2,i_2,j_2}$ to the $j$-th column of the $k$-th slice.

Similar to Rijndael-like cipher, we have the following properties for 3D-like ciphers.

Property 2. For a given input difference state cube:

1. $\kappa, \gamma, \kappa^{-1}, \gamma^{-1}$ change neither the number nor the coordinates of differential active S-boxes;
2. $\theta_1, \theta_2, \theta_1^{-1}, \theta_2^{-1}$ do not change the number of active S-boxes;
3. $\pi, \pi^{-1}$ only influence the current column;
4. $\theta_1, \theta_1^{-1}$ only influence the current slice.

Theorem 2. Let $M_{\text{non}}$ be the matrix representation of the $\pi$ layer with branch number
Let collection sets of \( \theta_i \) and \( \theta_i^{-1} \) be \( \Omega_i^{0,0}, \Omega_i^{0,1}, \ldots, \Omega_i^{n-1,n-1} \) and \( \Phi_i^{0,0}, \Phi_i^{0,1}, \cdots, \Phi_i^{n-1,n-1} \) respectively, collection sets of \( \theta_2 \) and \( \theta_2^{-1} \) are \( \Omega_2^{0,0}, \Omega_2^{0,1}, \ldots, \Omega_2^{n-1,n-1} \) and \( \Phi_2^{0,0}, \Phi_2^{0,1}, \cdots, \Phi_2^{n-1,n-1} \), respectively. If \( \Delta x_{i_1 p_1 q_1}, \Delta x_{i_2 p_2 q_2}, \ldots, \Delta y_{i_1 p_1 q_1}, \ldots, \Delta y_{i_2 p_2 q_2}, \ldots, \Delta y_{i_3 p_3 q_3}, \ldots, \Delta y_{i_4 p_4 q_4} \) are nonzero value, then for any \( z_1 + z_2 \leq d \), such that

1. \( \{ (o_1, p_1, i_1), \ldots, (o_s, p_s, i_s) \} \subseteq \bigcup_{u=1}^{z_1} \bigcup_{i=1}^{C_u} \Omega_i^{k_u, T(u)} \),
2. \( \{ (k_u, w, T(u)) : 1 \leq u \leq z_1, 0 \leq w \leq n - 1, 1 \leq i \leq C_u \} \subseteq \bigcup_{u=1}^{z_1} \bigcup_{i=1}^{C_u} \Omega_i^{k_u, T(u)} \),
3. \( \{ (g_1, q_1, j_1), \ldots, (g_r, q_r, j_r) \} \subseteq \bigcup_{v=1}^{z_2} \bigcup_{j=1}^{C_v} \Phi_j^{h_v, B(v)} \),
4. \( \{ (h_v, w, B(v)) : 1 \leq v \leq z_2, 0 \leq w \leq n - 1, 1 \leq j \leq S_r \} \subseteq \bigcup_{v=1}^{z_2} \bigcup_{j=1}^{C_v} \Phi_j^{h_v, B(v)} \).

hold synchronously, then

\[ (0, \ldots, 0, \Delta x_{i_1 p_1 q_1}, \ldots, 0, \Delta x_{i_2 p_2 q_2}, \ldots, 0) \rightarrow (0, \ldots, 0, \Delta y_{i_1 p_1 q_1}, \ldots, 0, \Delta y_{i_2 p_2 q_2}, \ldots, 0) \]

is a 6-round impossible differential of 3D-like cipher.

**Proof.** Let \( \Delta X = (0, \ldots, 0, \Delta x_{i_1 p_1 q_1}, \ldots, 0, \Delta x_{i_2 p_2 q_2}, \ldots, 0, 0, \ldots, 0) \) be the input difference of 3D-like cipher. Since

\[ \{ (o_1, p_1, i_1), \ldots, (o_s, p_s, i_s) \} \subseteq \bigcup_{u=1}^{z_1} \bigcup_{i=1}^{C_u} \Omega_i^{k_u, T(u)} \],

according to Property 2, the active S-boxes of \( \gamma_2 \circ \kappa_2 \circ (\pi_1 \circ \theta_2 \circ \gamma_1 \circ \kappa_1)(\Delta X) \) only appear in the \( T(u)_{i_1}, \cdots, T(u)_{i_s} \)-th columns of the \( k_u \)-th slice, where \( 1 \leq u \leq z_1 \).

Further, since

\[ \{ (k_u, w, T(u)) : 1 \leq u \leq z_1, 0 \leq w \leq n - 1, 1 \leq i \leq C_u \} \subseteq \bigcup_{u=1}^{z_1} \bigcup_{i=1}^{C_u} \Omega_i^{k_u, T(u)} \],

then the active S-boxes in \( \gamma_3 \circ \kappa_3 \circ (\pi_2 \circ \theta_2 \circ \gamma_2 \circ \kappa_2) \circ (\pi_1 \circ \theta_2 \circ \gamma_1 \circ \kappa_1)(\Delta X) \) only located in the \( t(u)_{j_1}, \cdots, t(u)_{j_r} \)-th column of \( k_u \)-th slice, where \( u = 1, \cdots, z_2 \). So in the state cube, at most \( \sum_{u=1}^{z_2} C_u \) columns have active S-boxes, i.e., there are at most \( n \sum_{u=1}^{z_2} C_u \left( \leq n^2 z_1 \right) \) active S-boxes in

\[ (\gamma_3 \circ \kappa_3) \circ (\pi_2 \circ \theta_2 \circ \gamma_2 \circ \kappa_2) \circ (\pi_1 \circ \theta_2 \circ \gamma_1 \circ \kappa_1)(\Delta X) \].

Note \( \theta_2 \) does not change the number of active S-boxes, we claim that state cube of \( (\theta_2 \circ \gamma_3 \circ \kappa_3) \circ (\pi_2 \circ \theta_2 \circ \gamma_2 \circ \kappa_2) \circ (\pi_1 \circ \theta_2 \circ \gamma_1 \circ \kappa_1)(\Delta X) \), i.e. the cube before the \( \pi_3 \) layer, has at most \( n^2 z_1 \) differential active S-boxes.

Let the output difference be \( \Delta Y = (0, \ldots, 0, \Delta y_{i_1 p_1 q_1}, \ldots, 0, \Delta y_{i_2 p_2 q_2}, \ldots, 0, 0, \ldots, 0) \), we firstly focus on
\[
\pi_3^{-1} \circ (\kappa_4^{-1} \circ \gamma_4^{-1} \circ \theta_1^{-1} \circ \pi_4^{-1}) \circ (\kappa_5^{-1} \circ \gamma_5^{-1} \circ \theta_2^{-1} \circ \pi_5^{-1}) \circ (\kappa_6^{-1} \circ \gamma_6^{-1} \circ \theta_1^{-1})(\Delta Y).
\]
Since \( \{(g_1, q_1, j_1), \ldots, (g_r, q_r, j_r)\} \subseteq \bigcup_{v=1}^{S} \left( \Phi_{(h_v, B(v))}^1 \right) \), by Property 2 we know active S-boxes of \( \pi_3^{-1} \circ (\kappa_6^{-1} \circ \gamma_6^{-1} \circ \theta_1^{-1})(\Delta Y) \) could only exist in the \( B(v)_1, \ldots, B(v)_{c_v} \)-th column of the \( h_v \)-th slice (for \( v = 1, \ldots, S_v \)). Since

\[
\{(h_v, w, B(v)_j) : 1 \leq v \leq S_v, 0 \leq w \leq n - 1, 1 \leq j \leq S_v \} \subseteq \bigcup_{v=1}^{S_v} \left( \Phi_{(h_v, b(v)_{c_v})}^2 \right).
\]

the active S-boxes of \( (\kappa_5^{-1} \circ \gamma_5^{-1} \circ \theta_2^{-1} \circ \pi_5^{-1}) \circ (\kappa_6^{-1} \circ \gamma_6^{-1} \circ \theta_1^{-1})(\Delta Y) \) could only appear in the \( b(v)_{c_v} \)-th columns of \( H_v \)-th slice. So there are at most \( \sum c_v \) columns have active S-boxes. This indicates that there are at most \( n \sum c_v \leq n^2 z_2 \) active S-boxes after \( \pi_3 \) layer, i.e. in

\[
(\kappa_4^{-1} \circ \gamma_4^{-1} \circ \theta_1^{-1} \circ \pi_4^{-1}) \circ (\kappa_5^{-1} \circ \gamma_5^{-1} \circ \theta_2^{-1} \circ \pi_5^{-1}) \circ (\kappa_6^{-1} \circ \gamma_6^{-1} \circ \theta_1^{-1})(\Delta Y).
\]

In the input differential cube of \( \pi_3 \), we affirm there exists one column who has \( \alpha \) active S-box, where \( \alpha \) satisfies \( w(\alpha) + w(\pi_3 \alpha) \leq d \) (otherwise the total number of active S-boxes in the differential cubes before and after \( \pi_3 \) will be at least \( n^2 d > n^2 z_1 + n^2 z_2 \), this leads a contradiction). Notice that the branch number of \( \pi_3 \) is \( d + 1 \), this indicates \( w(\alpha) + w(\pi_3 \alpha) \geq d \). By this mean, \( \Delta X \to \Delta Y \) is a 6-round impossible differential of 3D-like cipher.

\[\square\]

A typical example of impossible differential in 3D block cipher is described in Fig. 4.

\[\text{Fig. 4. A 6-round impossible differential of 3D.}\]

\(\blacksquare\) denotes a nonzero difference, \(\square\) denotes a zero difference, \(\blacksquare\) denotes a difference unsure
By observation, the impossible differential characteristics proposed by [11,15] (see Fig.5) are special cases of Theorem 2.

![Typical 6-round impossible differential of 3D in [11] and [15]](image)

**Fig. 5.** Typical 6-round impossible differential of 3D in [11] and [15]

### 5 Conclusions

Since IDC is very powerful in analyzing the security of block ciphers, it is worthwhile for us to evaluate the resistance of block cipher against IDC. The existence of impossible differentials is an evaluation of block cipher against IDC. This paper proposed methods to find impossible differentials of AES and 3D structures and lots of new impossible differentials could be searched out. Our work can be used as a tool to evaluate the vulnerability of new block ciphers employ these two structures against IDC. Although we are not sure that whether these new impossible differentials can improve attacks on AES and 3D, we hope this will be helpful in future.

### References

6. Ruilin Li, Bing Sun, Chao Li, “Impossible differential cryptanalysis of SPN ciphers,” *IET Information Security*, vol.5, issue.2, pp.111-120, June, 2011. [Article (CrossRef Link)]
Article (CrossRef Link)


Appendix

A.1 Brief Description of Rijndael Cipher

**Rijndael:**

Rijndael is an SPN cipher. The length of the block and the length of the key can be specified to be 128, 192 or 256 bits, independently of each other. In this paper we discuss the variant with 128-bit blocks and 128-bit keys. In this variant, the cipher consists of 10 rounds. We represent 128-bit data

\[ X = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}) \]

in 4×4 matrix as

\[
\begin{bmatrix}
 x_0 & x_1 & x_2 & x_3 \\
 x_4 & x_5 & x_6 & x_7 \\
 x_8 & x_9 & x_{10} & x_{11} \\
 x_{12} & x_{13} & x_{14} & x_{15}
\end{bmatrix}
\]

Each round except for the last consists of 4 transformation:
- **ByteSubstitution** is applied to each byte separately and is a nonlinear byte-wise substitution to use the S-box.
- **ShiftRow** is a cyclic shift of the bytes of each row by 0, 1, 2, or 3, respectively.
- **MixColumn** is a linear transformation applied to columns of the matrix. The branch number of this layer is 5.
- **AddRoundKey** is a key XOR. Before the first round AddRoundKey is performed using the key as the round key. In the last round the MixColumn is omitted.

A.2 Brief Description of 3D Cipher

**3D:**

The 3D block cipher operates on 512-bit blocks and uses 512-bit keys, both of which are represented as a 4×4×4 state of bytes (a 3-dimensional cube). The state for a 64-byte data
block \( A = (a_0, \cdots, a_{63}) \) is denoted
\[
A = \begin{pmatrix}
    a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\
    a_1 & a_5 & a_9 & a_{13} & a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} \\
    a_2 & a_{10} & a_{14} & a_{18} & a_{22} & a_{26} & a_{30} & a_{34} & a_{38} & a_{42} & a_{46} & a_{50} & a_{54} & a_{58} & a_{62} \\
    a_3 & a_7 & a_{11} & a_{15} & a_{19} & a_{23} & a_{27} & a_{31} & a_{35} & a_{39} & a_{43} & a_{47} & a_{51} & a_{55} & a_{59} & a_{63}
\end{pmatrix}
\]
with bytes inserted columnwise. Each square set of 16 bytes is called a slice of the state. Then the \( i \)-th round of 3D is calculated by
\[
\tau_i(X) = \pi \circ \theta_1 \circ \gamma \circ k_i(X),
\]
where
- \( k_i \): subkey XOR to the \( i \)-th round state;
- \( \gamma \): nonlinear byte-wise substitution to use the S-box;
- \( \pi \): linear transformation applied to columns of \( A \) with branch number 5;
- \( \theta_1, \theta_2 \): cyclic shifts of the bytes:

\[
\theta_1(A) = \begin{pmatrix}
    a_0 & a_4 & a_8 & a_{12} & a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\
    a_5 & a_9 & a_{13} & a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} & a_{65} \\
    a_{10} & a_{14} & a_2 & a_6 & a_{10} & a_{14} & a_2 & a_6 & a_{10} & a_{14} & a_2 & a_6 & a_{10} & a_{14} & a_2 & a_6 \\
    a_{15} & a_3 & a_7 & a_{11} & a_{15} & a_3 & a_7 & a_{11} & a_{15} & a_3 & a_7 & a_{11} & a_{15} & a_3 & a_7 & a_{11} \\
    a_{16} & a_{20} & a_{24} & a_{28} & a_{32} & a_{36} & a_{40} & a_{44} & a_{48} & a_{52} & a_{56} & a_{60} \\
    a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49} & a_{53} & a_{57} & a_{61} \\
    a_{34} & a_{38} & a_{42} & a_{46} & a_{50} & a_{54} & a_{58} & a_{62} & a_{66} & a_{70} & a_{74} & a_{78} \\
    a_{51} & a_{55} & a_{59} & a_{63} & a_5 & a_9 & a_{13} & a_{17} & a_{21} & a_{25} & a_{29} & a_{33} & a_{37} & a_{41} & a_{45} & a_{49}
\end{pmatrix}
\]

Ting Cui was born in 1985. He is currently pursuing for the Ph.D degree in Applied Mathematics at the Information Science Technology Institute. His current research interests include block cipher design and cryptanalysis.

Chen-hui Jin was born in 1965. He is currently professor at the Information Science Technology Institute. His current research interests are cryptography and information security.