A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers

Carlos Cid\textsuperscript{1}, Tao Huang\textsuperscript{2}, Thomas Peyrin\textsuperscript{2}, Yu Sasaki\textsuperscript{3}, Ling Song\textsuperscript{2,4}

1. University of London, UK
2. Nanyang Technological University, Singapore
3. NTT Secure Platform Laboratories, Japan
4. Institute of Information Engineering, Chinese Academy of Sciences, China

FSE 2018, Belgium
Outlines

1. Introduction
2. Improved Differential Bounds
3. Boomerang Attacks
4. Conclusion
Outline

1 Introduction
   - Deoxys
   - Deoxys-BC
   - Main Results

2 Improved Differential Bounds

3 Boomerang Attacks

4 Conclusion
Deoxys

- A third-round candidate of the CAESAR competition
- Designed by Jérémy Jean, Ivica Nikolić, Thomas Peyrin, Yannick Seurin
- Two AEAD modes:
  - Deoxys-I, the nonce-respecting mode
  - Deoxys-II, the nonce-misuse resistant mode
- Deoxys-BC: AES-based tweakable block cipher
  - Deoxys-BC-256, 14 rounds
  - Deoxys-BC-384, 16 rounds
Deoxys-BC

- AES round function
  - AddRoundTweakey
  - SubBytes
  - ShiftRows
  - MixColumns
- TWEAKEY framework

Figure: Instantiation of the TWEAKEY framework for Deoxys-BC-384.
Deoxys-BC

- **Sub-tweakeys**
  - Deoxys-BC-256: \( STK_i = TK^1_i \oplus TK^2_i \oplus RC_i \)
  - Deoxys-BC-384: \( STK_i = TK^1_i \oplus TK^2_i \oplus TK^3_i \oplus RC_i \)

- **Update of TK**
  - \( TK^1_{i+1} = h(TK^1_i) \), \( TK^2_{i+1} = h(LFSR_2(TK^2_i)) \), \( TK^3_{i+1} = h(LFSR_3(TK^3_i)) \)
  - Byte permutation \( h \)
    - \[
      \begin{pmatrix}
        0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\
        1 & 6 & 11 & 12 & 5 & 10 & 15 & 0 & 9 & 14 & 3 & 4 & 13 & 2 & 7 & 8
      \end{pmatrix}
    \]
  - **LFSRs**

| LFSR_2  | \((x_7||x_6||x_5||x_4||x_3||x_2||x_1||x_0) \rightarrow (x_6||x_5||x_4||x_3||x_2||x_1||x_0||x_7 \oplus x_5)\) |
|---------|----------------------------------------------------------------------------------------------------------------------------------|
| LFSR_3  | \((x_7||x_6||x_5||x_4||x_3||x_2||x_1||x_0) \rightarrow (x_0 \oplus x_6||x_7||x_6||x_5||x_4||x_3||x_2||x_1)\) |
Main Results

- New lower bounds on the number of active S-boxes

### Deoxys-BC-256

<table>
<thead>
<tr>
<th>lower bounds</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>[JNPS16]</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>-</td>
<td>22</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>simple model</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>12</td>
<td>16</td>
<td>19</td>
<td>23</td>
<td>26</td>
<td>29</td>
<td>32</td>
<td>35</td>
<td>38</td>
</tr>
<tr>
<td>incompatibility</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>22</td>
<td>27</td>
<td>31</td>
<td>35</td>
<td>40</td>
<td>44</td>
<td>48</td>
</tr>
</tbody>
</table>

### Deoxys-BC-384

<table>
<thead>
<tr>
<th>lower bounds</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>[JNPS16]</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>8</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>22</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>simple model</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>8</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>21</td>
<td>24</td>
<td>28</td>
<td>31</td>
<td>35</td>
<td>37</td>
<td>45</td>
</tr>
<tr>
<td>incompatibility</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>13</td>
<td>18</td>
<td>22</td>
<td>27</td>
<td>31</td>
<td>35</td>
<td>40</td>
<td>44</td>
<td>48</td>
<td>52</td>
</tr>
</tbody>
</table>
## Main Results

- **Attacks on Deoxys-BC and Deoxys**

### Deoxys internal primitives

<table>
<thead>
<tr>
<th></th>
<th>number of rounds</th>
<th>tweak size</th>
<th>key size</th>
<th>time</th>
<th>data</th>
<th>memory</th>
<th>attack type</th>
<th>ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deoxys-BC-256</strong></td>
<td>8/14</td>
<td>128</td>
<td>128</td>
<td>$\leq 2^{128}$</td>
<td>-</td>
<td>-</td>
<td>MitM</td>
<td>[JNPS16]</td>
</tr>
<tr>
<td></td>
<td>$\leq 8/14$</td>
<td>128</td>
<td>128</td>
<td>$\leq 2^{128}$</td>
<td>-</td>
<td>-</td>
<td>differential rectangle [JNPS16]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9/14</td>
<td>128</td>
<td>128</td>
<td>$2^{118}$</td>
<td>$2^{117}$</td>
<td>$2^{117}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td></td>
<td>10/14</td>
<td>$t &lt; 52$</td>
<td>$k &gt; 204$</td>
<td>$2^{204}$</td>
<td>$2^{127.58}$</td>
<td>$2^{127.58}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td><strong>Deoxys-BC-384</strong></td>
<td>8/16</td>
<td>128</td>
<td>256</td>
<td>$\leq 2^{256}$</td>
<td>-</td>
<td>-</td>
<td>MitM</td>
<td>[JNPS16]</td>
</tr>
<tr>
<td></td>
<td>12/16</td>
<td>128</td>
<td>256</td>
<td>$2^{127}$</td>
<td>$2^{127}$</td>
<td>$2^{125}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td></td>
<td>13/16</td>
<td>$t &lt; 114$</td>
<td>$k &gt; 270$</td>
<td>$2^{270}$</td>
<td>$2^{127}$</td>
<td>$2^{144}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
</tbody>
</table>

### Deoxys AE schemes

<table>
<thead>
<tr>
<th></th>
<th>number of rounds</th>
<th>tweak size</th>
<th>key size</th>
<th>time</th>
<th>data</th>
<th>memory</th>
<th>attack type</th>
<th>ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deoxys-I-128-128</strong></td>
<td>9/14</td>
<td>-</td>
<td>128</td>
<td>$2^{118}$</td>
<td>$2^{117}$</td>
<td>$2^{117}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td><strong>Deoxys-II-128-128</strong></td>
<td>-</td>
<td>-</td>
<td>128</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Deoxys-I-256-128</strong></td>
<td>12/16</td>
<td>-</td>
<td>256</td>
<td>$2^{236}$</td>
<td>$2^{126}$</td>
<td>$2^{124}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td><strong>Deoxys-II-256-128</strong></td>
<td>-</td>
<td>-</td>
<td>256</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Outline

1 Introduction

2 Improved Differential Bounds
   - Simple Model
   - Improved Model

3 Boomerang Attacks

4 Conclusion
Single-Key for AES

- For each round, one defines 16 variables $x_i \in \{0, 1\}$, where

$$x_i = \begin{cases} 
1, & \text{the } i\text{-th byte is active;} \\
0, & \text{the } i\text{-th byte is inactive.}
\end{cases}$$

- Incorporate the property of branch number 5 of MixColumns:

Suppose $(x_0, x_5, x_{10}, x_{15}) \xrightarrow{\text{MixColumns}} (x_{16}, x_{17}, x_{18}, x_{19})$

$$x_0 + x_5 + x_{10} + x_{15} + x_{16} + x_{17} + x_{18} + x_{19} \geq 5d_j,$$

$$d \geq x_0, \ d \geq x_5, \ d \geq x_{10}, \ d \geq x_{15}, \ d \geq x_{16}, \ d \geq x_{17}, \ d \geq x_{18}, \ d \geq x_{19}.$$  

- The objective function:

"minimise $\sum x_i.$"
Related-Tweakey with $TK^1$

- Define 16 variables $stk_i \in \{0, 1\}$, where
  \[
  stk_i = \begin{cases} 
  1, & \text{the } i\text{-th subtweakey byte is active;} \\
  0, & \text{the } i\text{-th subtweakey byte is inactive.}
  \end{cases}
  \]

- Related-tweakey with $TK^1$
  - Exclude $(x_i, stk_i, y_i) \in \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$ with
    \[
    x_i + stk_i - y_i \geq 0, \quad x_i - stk_i + y_i \geq 0, \quad -x_i + stk_i + y_i \geq 0.
    \]
Related-Tweakey with $TK^2$ and $TK^3$

- Differential cancellations may happen.
  - For $TK^2$, there is at most 1 cancellation for each active byte.
  - For $TK^3$, there are at most 2 cancellations for each active byte.
Related-Tweakey with $TK^2$ and $TK^3$

- Differential cancellations may happen.
  - For $TK^2$, there is at most 1 cancellation for each active byte.
  - For $TK^3$, there are at most 2 cancellations for each active byte.

Let $h_{inv}$ be the inverse of $h$.

\[
\text{LANE}_i - stk_i \geq 0, \quad \text{LANE}_i - stk_{16+h_{inv}(i)} \geq 0, \quad \cdots, \quad \text{LANE}_i - stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq 0,
\]

\[
stk_i + stk_{16+h_{inv}(i)} + stk_{32+h_{inv}^2(i)} + \cdots + stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq r \cdot \text{LANE}_i - 1.
\]

Or

\[
\text{LANE}_i - stk_i \geq 0, \quad \text{LANE}_i - stk_{16+h_{inv}(i)} \geq 0, \quad \cdots, \quad \text{LANE}_i - stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq 0,
\]

\[
stk_i + stk_{16+h_{inv}(i)} + stk_{32+h_{inv}^2(i)} + \cdots + stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq r \cdot \text{LANE}_i - 2.
\]
Application of the Simple Model

- New lower bounds on the number of active S-boxes

<table>
<thead>
<tr>
<th>Deoxys-BC-256</th>
</tr>
</thead>
<tbody>
<tr>
<td>lower bounds</td>
</tr>
<tr>
<td>[JNPS16]</td>
</tr>
<tr>
<td>simple model</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deoxys-BC-384</th>
</tr>
</thead>
<tbody>
<tr>
<td>lower bounds</td>
</tr>
<tr>
<td>[JNPS16]</td>
</tr>
<tr>
<td>simple model</td>
</tr>
</tbody>
</table>
Limitation of the Simple Model

- There may exist linear incompatibilities.
- Difference cancellations between $STK$ and the state imposes some linear relation of key bytes.
  - E.g., $0xF2 \cdot \alpha + 0xF6 \cdot \beta = 0$

Cid et al. A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers FSE 2018, Belgium 12 / 26
Limitation of the Simple Model

- There may exist linear incompatibilities.
- Difference cancellations between $STK$ and the state imposes some linear relation of key bytes.
  - E.g., $0xF2 \cdot \alpha + 0xF6 \cdot \beta = 0$

Cost additional $b + c - a$ bytes of degree of freedom

- $a$: Number of active bytes before MC. E.g., $a = 2$
- $b$: Number of inactive bytes after MC. E.g., $b = 1$
- $c$: Number of cancellations in ATK. E.g., $c = 2$
Degrees of Freedom

- Degrees of freedom available
  - $s \cdot \sum \text{LANE}_i$
  - $s = 2$ for $TK^2$ and $s = 3$ for $TK^3$

- Degrees of consumption
  - **Type 1** Cancellations in $STK$,
    - $TK^1[i] \oplus TK^2[i] = 0$ or $TK^1[i] \oplus TK^2[i] \oplus TK^3[i] = 0$
  - **Type 2** Cancellations between $STK$ and the state
    - Consume $b + c - a$ bytes of degree of freedom
Representation with MILP

- Degrees of consumption Type 1 for $r$ rounds

\[ r \cdot \sum_{i=0}^{15} \text{LANE}_i - \sum_{i=0}^{16r-1} \text{stk}_i \]

- Degrees of consumption Type 2:
  Suppose that \((x_0, x_5, x_{10}, x_{15}) \xrightarrow{MC} (x_{16}, x_{17}, x_{18}, x_{19})\)

  - $a = x_0 + x_5 + x_{10} + x_{15}$
  - $b = 4d - x_{16} - x_{17} - x_{18} - x_{19}$ where $d = 1$ means the column is active.
  - For each byte of the column \((x_i, \text{stk}_i, y_i)\)
    \[-x_i - \text{stk}_i + y_i + c_i \geq -1, \quad x_i + \text{stk}_i + y_i - c_i \geq 0,\]
    \[-x_i - \text{stk}_i - y_i - c_i \geq -3, \quad -x_i + \text{stk}_i - y_i - c_i \geq -2, \quad x_i - \text{stk}_i - y_i - c_i \geq -2.\]
  - $b + c - a$

\[4d - x_{16} - x_{17} - x_{18} - x_{19} + (c_{16} + c_{17} + c_{18} + c_{19}) - (x_0 + x_5 + x_{10} + x_{15}).\]
Representation in the MILP model

- **Total consumption of degrees**
  \[ s \cdot \sum_{i=0}^{15} \text{LANE}_i \geq \left( r \cdot \sum_{i=0}^{15} \text{LANE}_i - \sum_{i=0}^{16r-1} \text{stk}_i \right) + \sum_{j=0}^{4r-1} \text{TYPE2}_j. \]

- **New lower bounds on the number of active S-boxes**

<table>
<thead>
<tr>
<th>Deoxys-BC-256</th>
<th>lower bounds</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>[JNPS16]</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>12</td>
<td>16</td>
<td>17</td>
<td>-</td>
<td>22</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>simple model</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>9</td>
<td>12</td>
<td>16</td>
<td>19</td>
<td>23</td>
<td>26</td>
<td>29</td>
<td>32</td>
<td>35</td>
<td>38</td>
</tr>
<tr>
<td>incompatibility</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>14</td>
<td>18</td>
<td>22</td>
<td>27</td>
<td>31</td>
<td>35</td>
<td>40</td>
<td>44</td>
<td>48</td>
</tr>
</tbody>
</table>

| Deoxys-BC-384 | lower bounds | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |11 |12 |13 |14 |15 |16 |
|---------------|--------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|
| [JNPS16]      |              | 0 | 0 | 0 | 1 | 4 | 8 | - | - | - | -  | -  | -  | -  | -  | -  |
| simple model  |              | 0 | 0 | 0 | 1 | 4 | 8 |10 |14 |18 |21  |24  |28  |31  |35  |37  |45  |
| incompatibility |            | - | - | - | - | - | - | - | - | - | -  | -  | -  | -  | -  | -  | -  |

† Bounds for linear incompatibility are obtained under certain assumptions.
Outline

1 Introduction

2 Improved Differential Bounds

3 Boomerang Attacks
   - Boomerang Switch
   - Search for Trails

4 Conclusion
Introduction of Boomerang attacks

- \( E = E_1 \circ E_0 \)
- Two trails \( \alpha \xrightarrow{E_0} \beta, \gamma \xrightarrow{E_1} \delta \) with probabilities \( p \) and \( q \) respectively
- A right quartet can be obtained with probability \( p^2 q^2 \)
  - Choose \( P_1, P_2 = P_1 \oplus \alpha \)
  - \( C_1 = E(P_1), C_2 = E(P_2) \)
  - Let \( C_3 = C_1 \oplus \delta, C_4 = C_2 \oplus \delta \)
  - \( P_3 = E^{-1}(C_3), P_4 = E^{-1}(C_4) \)
  - Test \( P_3 \oplus P_4 = \alpha \)
Boomerang Switch

Figure: The ladder switch in a toy three S-box block [BK09].
An Example of the Boomerang Switch

10-round distinguisher of Deoxys-BC-384

<table>
<thead>
<tr>
<th>$R$</th>
<th>$X$</th>
<th>$K$</th>
<th>$Y$</th>
<th>$Z$</th>
<th>$p_r$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>00 00 00 00</td>
<td>69 00 00 00</td>
<td>69 00 00 00</td>
<td>** 00 00 00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 bb 00 00</td>
<td>00 bb 00 00</td>
<td>** 00 00 00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 d2 00</td>
<td>00 00 d2 00</td>
<td>** 00 00 00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00 00 00 00</td>
<td>00 00 00 69</td>
<td>00 00 00 69</td>
<td>** 00 00 00</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>** 00 00 00</td>
<td>00 10 00 00</td>
<td>** 10 00 00</td>
<td>** ** 00 00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>** 00 00 00</td>
<td>00 9e 00 00</td>
<td>** 9e 00 00</td>
<td>** 00 00 **</td>
<td></td>
</tr>
<tr>
<td></td>
<td>** 00 00 00</td>
<td>00 8e 00 00</td>
<td>** 8e 00 00</td>
<td>00 00 ** **</td>
<td></td>
</tr>
<tr>
<td></td>
<td>** 00 00 00</td>
<td>00 8e 00 00</td>
<td>** 8e 00 00</td>
<td>00 ** ** 00</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>00 ** ** **</td>
<td>00 ee 00 00</td>
<td>00 ** ** **</td>
<td>00 ** ** **</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>** 00 ** **</td>
<td>00 00 00 00</td>
<td>** 00 ** **</td>
<td>00 ** ** **</td>
<td></td>
</tr>
<tr>
<td></td>
<td>** ** 00 **</td>
<td>00 00 00 00</td>
<td>** ** 00 **</td>
<td>00 ** ** **</td>
<td></td>
</tr>
<tr>
<td></td>
<td>** ** ** **</td>
<td>00 00 00 11</td>
<td>** ** ** 00</td>
<td>00 ** ** **</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>00 00 00 00</td>
<td>2$^{-6}$</td>
</tr>
<tr>
<td></td>
<td>00 9e 00 00</td>
<td>00 00 00 00</td>
<td>00 9e 00 00</td>
<td>68 00 00 00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00 0a ab 00</td>
<td>00 0a 00 00</td>
<td>00 00 ab 00</td>
<td>01 00 00 00</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00 00 93 7a</td>
<td>00 00 93 00</td>
<td>00 00 00 7a</td>
<td>b9 00 00 00</td>
<td></td>
</tr>
</tbody>
</table>
Properties of Truncated Differential Trails

- A few degrees of freedom are left for the master tweakey difference.
- Once the master tweakey difference is fixed, many active bytes of the state are also fixed.

Deoxys-BC Key Schedule
Round $r-1$

$X_{r-1}$ → $Y_{r-1}$ → $Z_{r-1}$ → $X_r$ → $Y_r$

ATK, SB, SR, MC
Search for Differential Trails

- Define two types of S-box
  - **Type i** the input and output differences are determined.
  - **Type ii** the input or output differences are not determined but some constraints are imposed by the subtweakey differences.

- Given a truncated differential trail

![Diagram of the search for differential trails process]

1. Set \( p = 0 \)
2. Choose a master tweakey difference
3. Compute STK
4. Derive partial state differences
5. If the differences are of Type i, continue; otherwise, go to the next step.
6. If \( p = 0 \), update \( p \); otherwise, set \( p = 0 \).

---

Cid et al. A Security Analysis of Deoxys and its Internal Tweakeable Block Ciphers FSE 2018, Belgium
## Boomerang Distinguishers

<table>
<thead>
<tr>
<th>$R_1, R_2$</th>
<th>$#AS$</th>
<th>$pq$</th>
<th>$\hat{p}^2 \hat{q}^2$</th>
<th>$R_1, R_2$</th>
<th>$#AS$</th>
<th>$pq$</th>
<th>$\hat{p}^2 \hat{q}^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4,4</td>
<td>6</td>
<td>$2^{-36}$</td>
<td>$2^{-72}$</td>
<td>5,5</td>
<td>4</td>
<td>$2^{-24}$</td>
<td>$2^{-42}$</td>
</tr>
<tr>
<td>5,4</td>
<td>9</td>
<td>$2^{-61}$</td>
<td>$2^{-122}$</td>
<td>6,5</td>
<td>9</td>
<td>$2^{-60}$</td>
<td>$2^{-120}$</td>
</tr>
<tr>
<td>5,5</td>
<td>16</td>
<td>$2^{-106}$</td>
<td>$2^{-212}$</td>
<td>6,6</td>
<td>15</td>
<td>$2^{-98}$</td>
<td>$2^{-196}$</td>
</tr>
<tr>
<td>6,5</td>
<td>20</td>
<td>$2^{-136}$</td>
<td>$2^{-265}$</td>
<td>7,6</td>
<td>20</td>
<td>$2^{-134}$</td>
<td>$2^{-268}$</td>
</tr>
</tbody>
</table>
# Boomerang Attacks

## Deoxys **internal primitives**

<table>
<thead>
<tr>
<th></th>
<th>number of rounds</th>
<th>tweak size</th>
<th>key size</th>
<th>time</th>
<th>data</th>
<th>memory</th>
<th>attack type</th>
<th>ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deoxys-BC-256</strong></td>
<td>8/14</td>
<td>128</td>
<td>128</td>
<td>$\leq 2^{128}$</td>
<td>-</td>
<td>-</td>
<td>MitM</td>
<td>[JNPS16]</td>
</tr>
<tr>
<td></td>
<td>$\leq 8/14$</td>
<td>128</td>
<td>128</td>
<td>$\leq 2^{128}$</td>
<td>-</td>
<td>-</td>
<td>differential rectangle</td>
<td>[JNPS16]</td>
</tr>
<tr>
<td></td>
<td>9/14</td>
<td>128</td>
<td>128</td>
<td>$2^{118}$</td>
<td>$2^{117}$</td>
<td>$2^{117}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td></td>
<td>10/14</td>
<td>$t &lt; 52$</td>
<td>$k &gt; 204$</td>
<td>$2^{204}$</td>
<td>$2^{127.58}$</td>
<td>$2^{127.58}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td><strong>Deoxys-BC-384</strong></td>
<td>8/16</td>
<td>128</td>
<td>256</td>
<td>$\leq 2^{256}$</td>
<td>-</td>
<td>-</td>
<td>MitM</td>
<td>[JNPS16]</td>
</tr>
<tr>
<td></td>
<td>12/16</td>
<td>128</td>
<td>256</td>
<td>$2^{127}$</td>
<td>$2^{127}$</td>
<td>$2^{125}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td></td>
<td>13/16</td>
<td>$t &lt; 114$</td>
<td>$k &gt; 270$</td>
<td>$2^{270}$</td>
<td>$2^{127}$</td>
<td>$2^{144}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
</tbody>
</table>

## Deoxys **AE schemes**

<table>
<thead>
<tr>
<th></th>
<th>number of rounds</th>
<th>tweak size</th>
<th>key size</th>
<th>time</th>
<th>data</th>
<th>memory</th>
<th>attack type</th>
<th>ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Deoxys-I-128-128</strong></td>
<td>9/14</td>
<td>-</td>
<td>128</td>
<td>$2^{118}$</td>
<td>$2^{117}$</td>
<td>$2^{117}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td><strong>Deoxys-II-128-128</strong></td>
<td>-</td>
<td>-</td>
<td>128</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Deoxys-I-256-128</strong></td>
<td>12/16</td>
<td>-</td>
<td>256</td>
<td>$2^{236}$</td>
<td>$2^{126}$</td>
<td>$2^{124}$</td>
<td>rectangle</td>
<td>this</td>
</tr>
<tr>
<td><strong>Deoxys-II-256-128</strong></td>
<td>-</td>
<td>-</td>
<td>256</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Outline

1. Introduction
2. Improved Differential Bounds
3. Boomerang Attacks
4. Conclusion
Conclusion

- Two improved lower bounds for the number of active S-boxes for Deoxys-BC under the related-tweakey setting
- Algorithm for searching exact differential trails for Deoxys-BC
- Improved attacks on Deoxys-BC and Deoxys
A Misunderstanding

Byte permutation $h$ in the Tweakey Schedule

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

![Byte permutation diagram]
Thank you for your attention!

Thank all the group members at ASK 2016 for fruitful discussion.