A Security Analysis of Deoxys and its Internal Tweakable Block Ciphers

Carlos Cid[1], Tao Huang[2],
Thomas Peyrin[2], Yu Sasaki[3], Ling Song[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

Outline

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

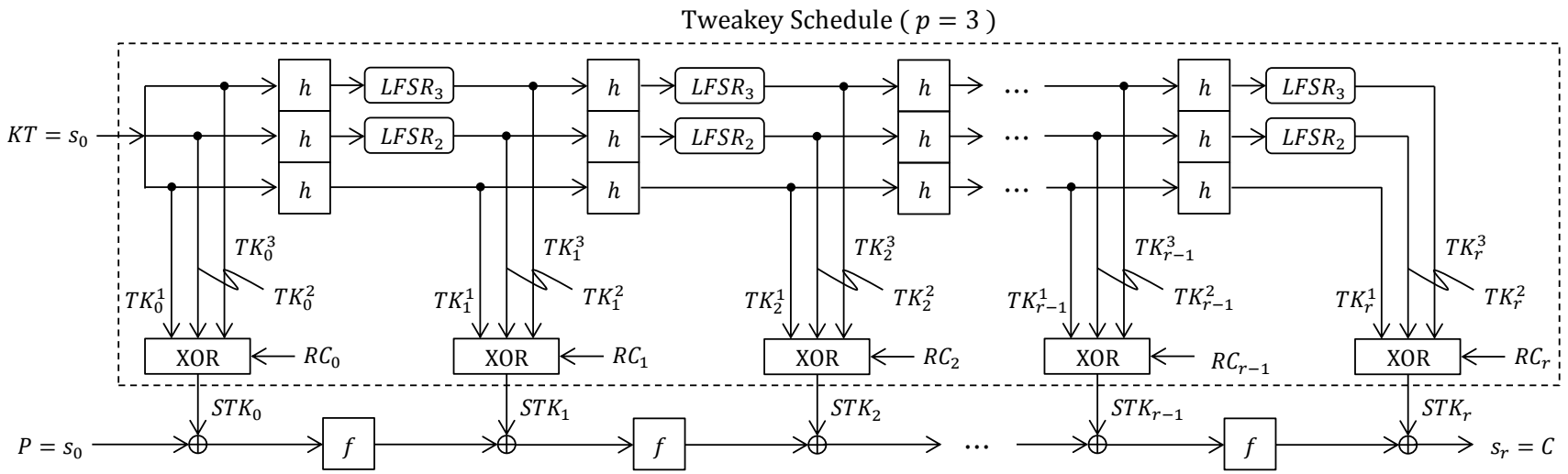


Figure: Instantiation of the TWEAKEY framework for Deoxys-BC-384.

Deoxys-BC

- Sub-tweakeys
  - Deoxys-BC-256: $STK_i = TK_i^1 \oplus TK_i^2 \oplus RC_i$
  - Deoxys-BC-384: $STK_i = TK_i^1 \oplus TK_i^2 \oplus TK_i^3 \oplus RC_i$
- Update of TK
  - $TK_{i+1}^1 = h(TK_i^1)$, $TK_{i+1}^2 = h(LFSR_2(TK_i^2))$, $TK_{i+1}^3 = h(LFSR_3(TK_i^3))$
  - 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

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

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	-	-	-	-	-	**22**	-	-	-	-
simple model	0	0	0	1	4	8	10	14	18	21	24	**28**	31	35	37	45
incompatibility	0	0	0	1	5	9	13	18	22	27	31	**35**	40	44	48	52

Main Results

- Attacks on Deoxys-BC and Deoxys

Deoxys **internal primitives**

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

Deoxys **AE schemes**

Deoxys-I-128-128	9/14	-	128	2^{118}	2^{117}	2^{117}	rectangle	this
Deoxys-II-128-128	-	-	128	-	-	-	-	-
Deoxys-I-256-128	12/16	-	256	2^{236}	2^{126}	2^{124}	rectangle	this
Deoxys-II-256-128	-	-	256	-	-	-	-	-

Outline

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 Σx_i."

Related-Tweakey with TK^1

- Define 16 variables $stk_i \in \{0, 1\}$, where

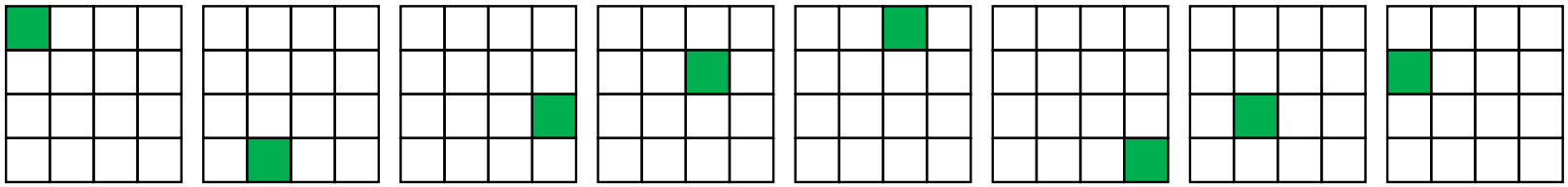
$$stk_i = \begin{cases} 1, & \text{the } i\text{-th subtweakey byte is active;} \\ 0, & \text{the } i\text{-th subtweakey byte is inactive.} \end{cases}$$

- Related-tweakey with TK^1
  - Exclude $(x_i, stk_i, y_i) \in \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$ with

$$x_i + stk_i - y_i \geq 0, \qquad x_i - stk_i + y_i \geq 0, \qquad -x_i + stk_i + y_i \geq 0.$$

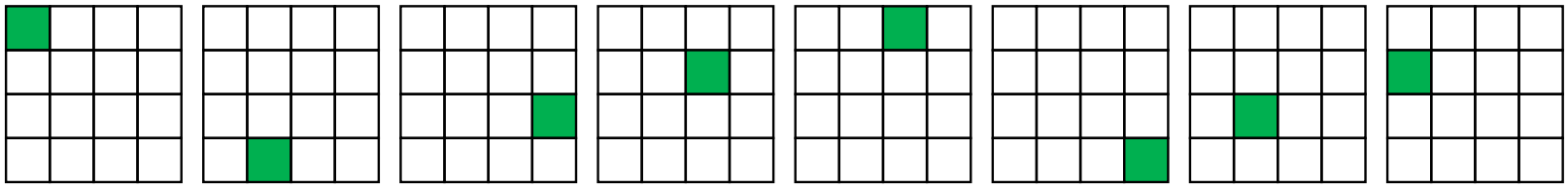
Related-Tweakey with TK^2 and TK^3

- 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.

$$\mathrm{LANE}_i - stk_i \geq 0,\ \mathrm{LANE}_i - stk_{16+h_{inv}(i)} \geq 0,\ \cdots,\ \mathrm{LANE}_i - stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq 0,$$
$$stk_i + stk_{16+h_{inv}(i)} + stk_{32+h_{inv}^2(i)} + \cdots + stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq r \cdot \mathrm{LANE}_i - \mathbf{1}.$$

or

$$\mathrm{LANE}_i - stk_i \geq 0,\ \mathrm{LANE}_i - stk_{16+h_{inv}(i)} \geq 0,\ \cdots,\ \mathrm{LANE}_i - stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq 0,$$
$$stk_i + stk_{16+h_{inv}(i)} + stk_{32+h_{inv}^2(i)} + \cdots + stk_{16(r-1)+h_{inv}^{r-1}(i)} \geq r \cdot \mathrm{LANE}_i - \mathbf{2}.$$

Application of the Simple Model

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

Deoxys-BC-256

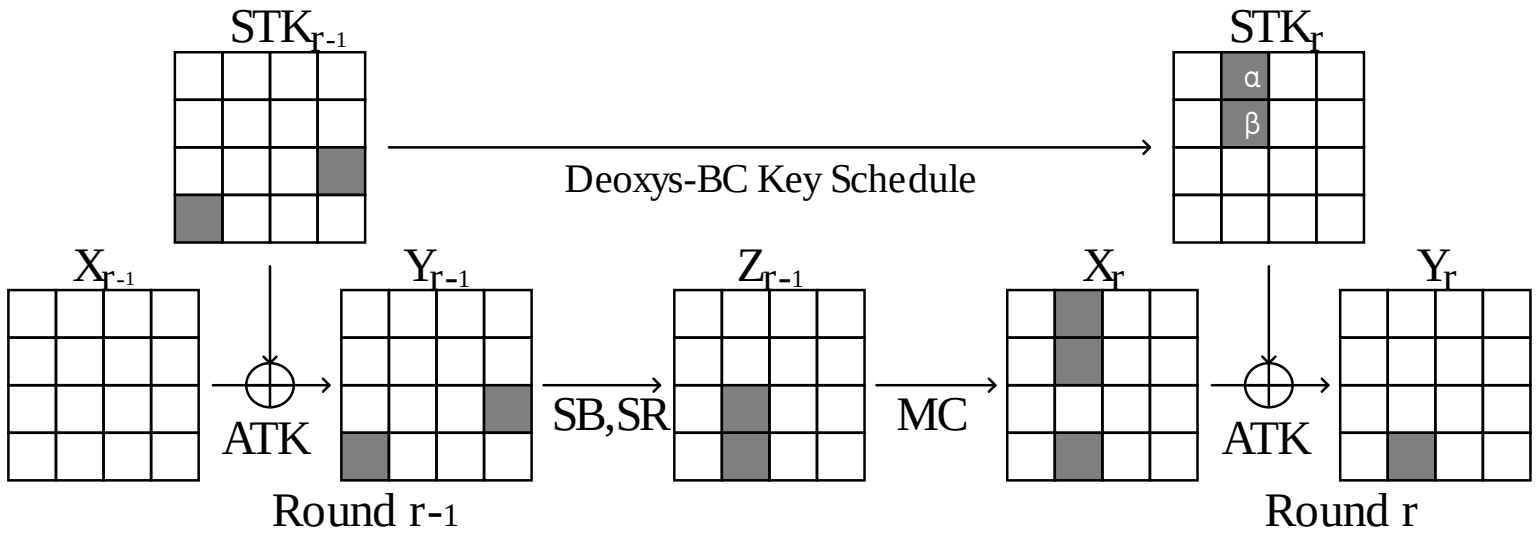
lower bounds	1	2	3	4	5	6	7	8	9	10	11	12	13	14
[JNPS16]	0	0	1	5	9	12	16	17	-	**22**	-	-	-	-
simple model	0	0	1	5	9	12	16	19	23	**26**	29	32	35	38

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	-	-	-	-	-	**22**	-	-	-	-
simple model	0	0	0	1	4	8	10	14	18	21	24	**28**	31	35	37	45

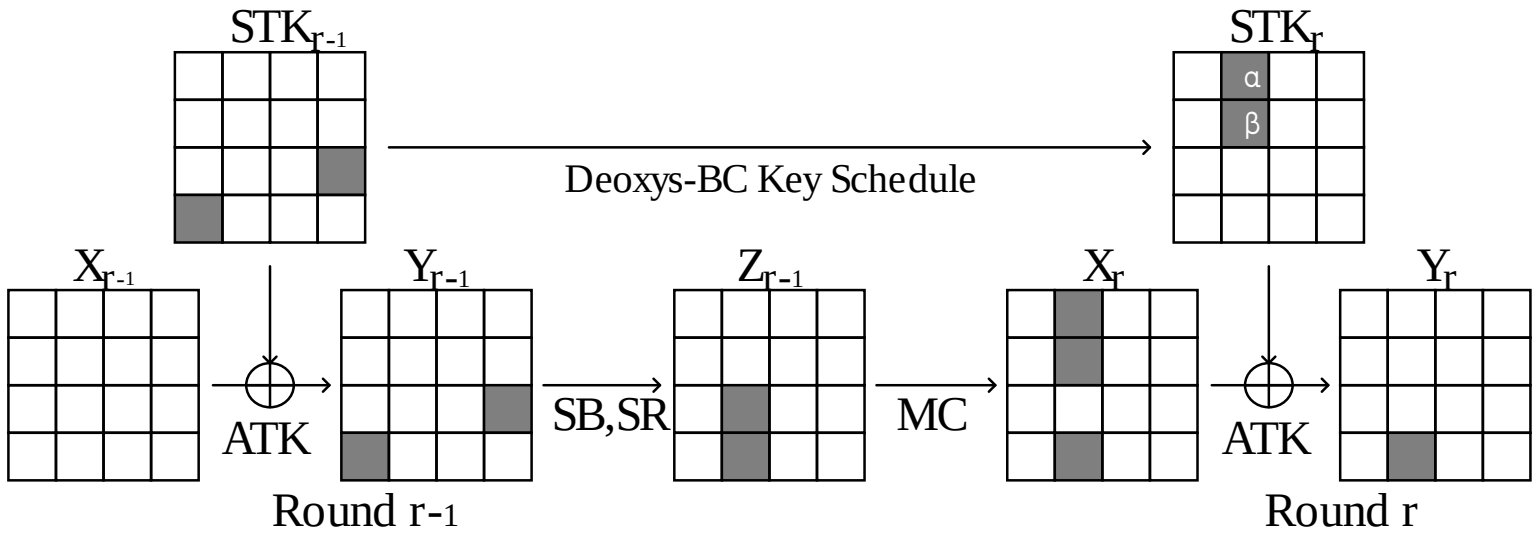
Limitation of the Simple Model

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



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
  - $s \cdot \sum \mathrm{LANE}_i$
  - $s = 2$ 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

$$r \cdot \sum_{i=0}^{15} \mathrm{LANE}_i - \sum_{i=0}^{16r-1} stk_i$$

- 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, stk_i, y_i)

$$-x_i - stk_i + y_i + c_i \geq -1, \quad x_i + stk_i + y_i - c_i \geq 0,$$
$$-x_i - stk_i - y_i - c_i \geq -3, \; -x_i + stk_i - y_i - c_i \geq -2, \quad x_i - stk_i - y_i - c_i \geq -2.$$

  - $b + c - a$

$$4d - x_{16} - x_{17} - x_{18} - x_{19} + (c_{16} + c_{17} + c_{18} + c_{19}) - (x_0 + x_5 + x_{10} + x_{15}).$$

Representation in the MILP model

- Total consumption of degrees

$$s \cdot \sum_{i=0}^{15} \mathrm{LANE}_i \geq \left(r \cdot \sum_{i=0}^{15} \mathrm{LANE}_i - \sum_{i=0}^{16r-1} stk_i \right) + \sum_{j=0}^{4r-1} \mathrm{TYPE2}_j.$$

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

`Deoxys-BC-256`

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

`Deoxys-BC-384`

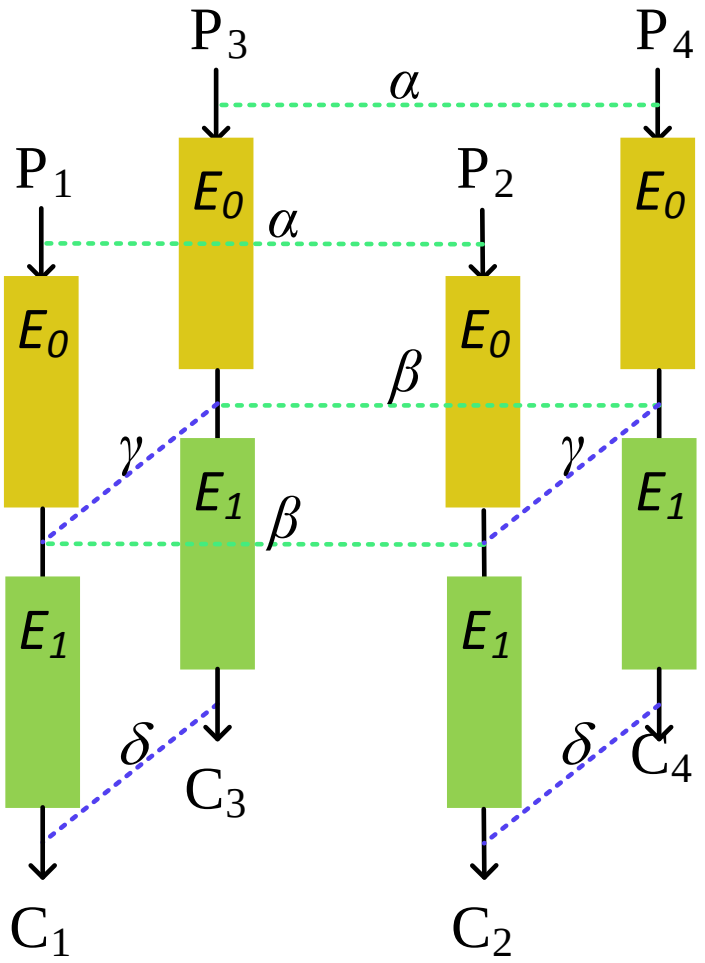
lower bounds	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
[JNPS16]	0	0	0	1	4	8	-	-	-	-	-	**22**	-	-	-	-
simple model	0	0	0	1	4	8	10	14	18	21	24	**28**	31	35	37	45
incompatibility†	0	0	0	1	5	9	13	18	22	27	31	**35**	40	44	48	52

†Bounds for linear incompatibility are obtained under certain assumptions.

Outline

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^2q^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

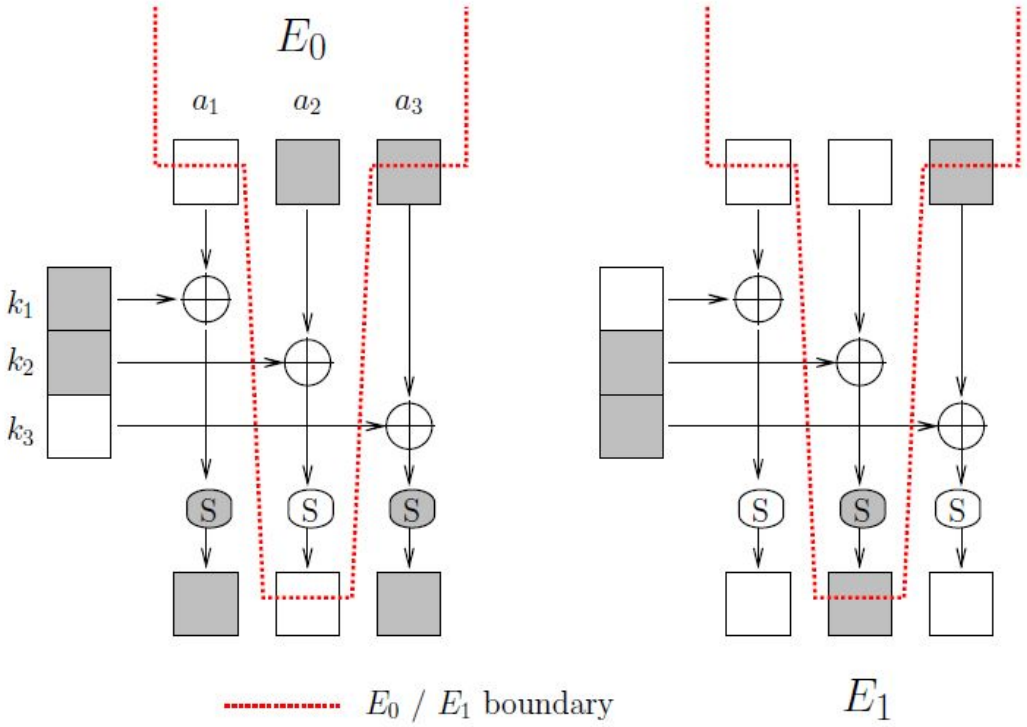


Figure: The ladder switch in a toy three S-box block [BK09].

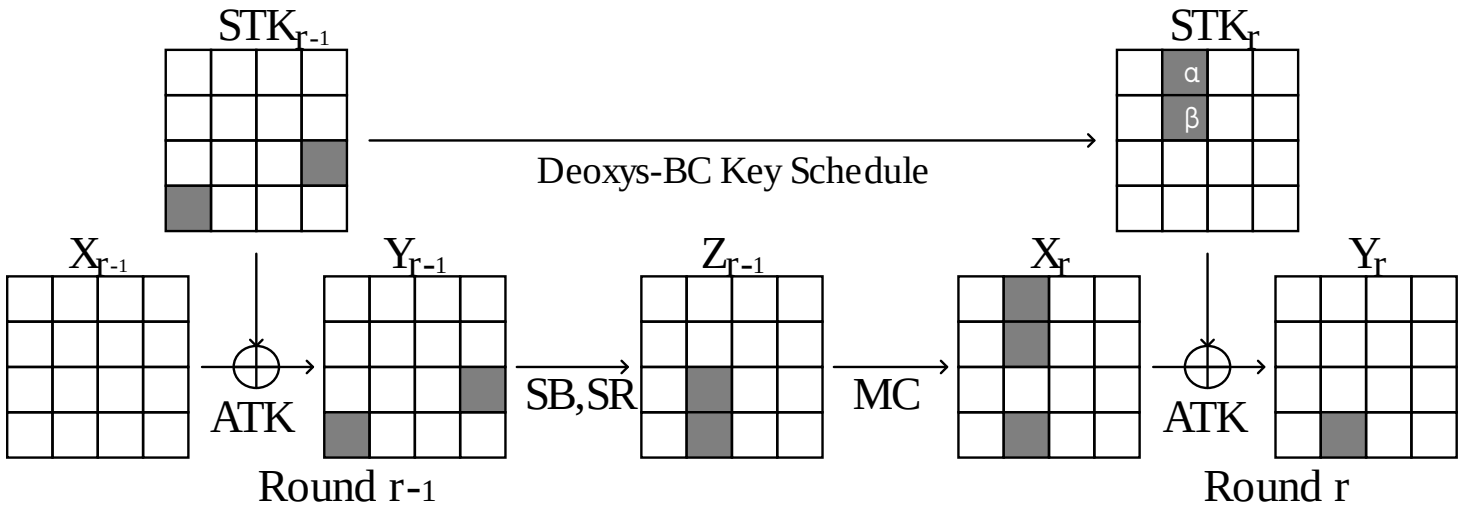
An Example of the Boomerang Switch

10-round distinguisher of Deoxys-BC-384

R	X	K	Y	Z	p_r
5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	69 00 00 00 00 bb 00 00 00 00 d2 00 00 00 00 69	69 00 00 00 00 bb 00 00 00 00 d2 00 00 00 00 69	** 00 00 00 ** 00 00 00 ** 00 00 00 ** 00 00 00	1
6	** 00 00 00 ** 00 00 00 ** 00 00 00 ** 00 00 00	00 10 00 00 00 9e 00 00 00 8e 00 00 00 8e 00 00	** 10 00 00 ** 9e 00 00 ** 8e 00 00 ** 8e 00 00	** ** 00 00 ** 00 00 ** 00 00 ** ** 00 ** ** 00	1
5	00 ** ** ** ** 00 ** ** ** ** 00 ** ** ** ** **	00 ee 00 00 00 00 00 00 00 00 00 00 00 00 00 11	00 ** ** ** ** 00 ** ** ** ** 00 ** ** ** ** 00	00 ** ** ** 00 ** ** ** 00 ** ** ** 00 ** ** **	1
6	00 00 00 00 00 9e 00 00 00 0a ab 00 00 00 93 7a	00 00 00 00 00 00 00 00 00 0a 00 00 00 00 93 00	00 00 00 00 00 9e 00 00 00 00 ab 00 00 00 00 7a	00 00 00 00 68 00 00 00 01 00 00 00 b9 00 00 00	2^{-6}

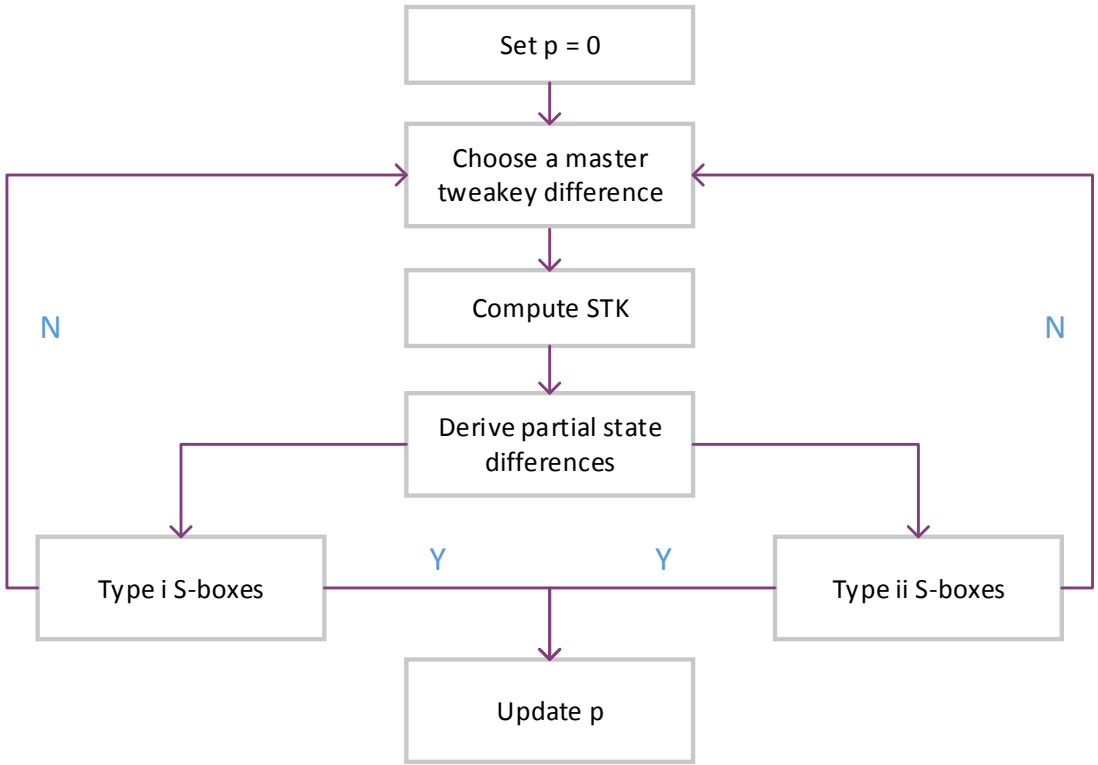
Properties of Truncated Differential Trails

- 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.



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



Boomerang Distinguishers

Deoxys-BC-256				Deoxys-BC-384			
R_1, R_2	#AS	pq	$\hat{p}^2\hat{q}^2$	R_1, R_2	#AS	pq	$\hat{p}^2\hat{q}^2$
4,4	6	2^{-36}	2^{-72}	5,5	4	2^{-24}	2^{-42}
5,4	9	2^{-61}	2^{-122}	6,5	9	2^{-60}	2^{-120}
5,5	16	2^{-106}	2^{-212}	6,6	15	2^{-98}	2^{-196}
6,5	20	2^{-136}	2^{-265}	7,6	20	2^{-134}	2^{-268}

Boomerang Attacks

Deoxys **internal primitives**

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

Deoxys **AE schemes**

Deoxys-I-128-128	9/14	-	128	2^{118}	2^{117}	2^{117}	rectangle	this
Deoxys-II-128-128	-	-	128	-	-	-	-	-
Deoxys-I-256-128	12/16	-	256	2^{236}	2^{126}	2^{124}	rectangle	this
Deoxys-II-256-128	-	-	256	-	-	-	-	-

Outline

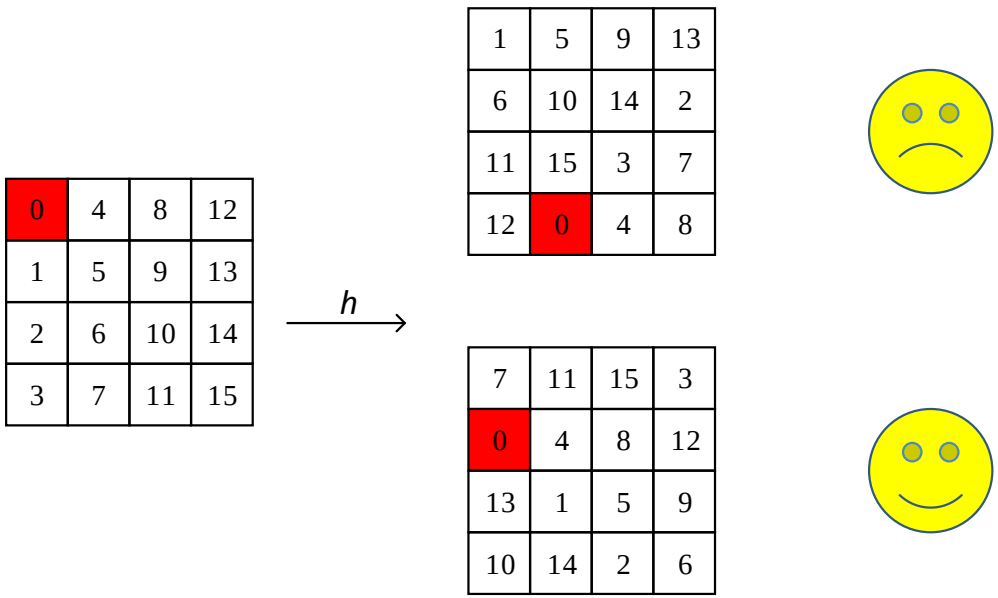
Conclusion

- 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

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



Thank you for your attention!

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