New Properties of the Double Boomerang Connectivity Table

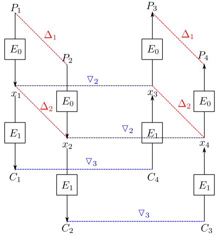
Qianqian Yang, Ling Song*, Siwei Sun, Danping Shi, Lei Hu

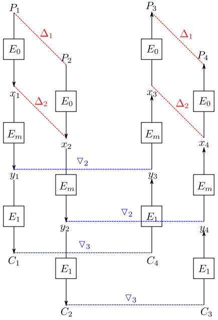
Institute of Information Engineering
Jinan University
University of Chinese Academy of Sciences

Outline

1. Preliminary
2. New Properties of the Double Boomerang Connectivity Table
3. Application of the New Properties
4. MILP Model to Search for Boomerangs with Cluster Probability
5. Conclusion

Preliminary





- Boomerang attack:
  - a long differential ⇐ two short ones with high probability
  - the two trails are **independent**
- Sandwich attack:
  - takes into account the **dependency** between the differentials
  - handles it in a middle part E_m

Tables

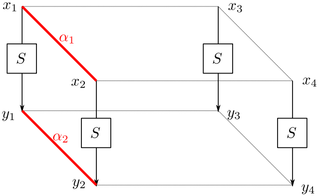


Figure: The Difference Distribution Table (DDT)

$$\mathtt{DDT}(\alpha_1, \alpha_2) = \#\{x \in \mathbb{F}_2^n | S(x) \oplus S(x \oplus \alpha_1) = \alpha_2\}.$$

Tables

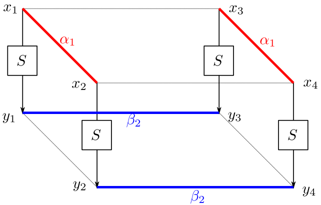


Figure: The Boomerang Connectivity Table (BCT)

$$\texttt{BCT}(\alpha_1, \beta_2) = \#\{x \in \mathbb{F}_2^n | S^{-1}(S(x) \oplus \beta_2) \oplus S^{-1}(S(x \oplus \alpha_1) \oplus \beta_2) = \alpha_1\}.$$

Tables

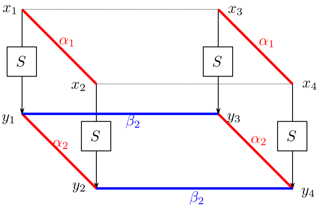


Figure: The Upper BCT (UBCT)

$$\texttt{UBCT}(\alpha_1, \alpha_2, \beta_2) = \\ \#\left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l} S(x) \oplus S(x \oplus \alpha_1) = \alpha_2 \\ S^{-1}(S(x) \oplus \beta_2) \oplus S^{-1}(S(x \oplus \alpha_1) \oplus \beta_2) = \alpha_1 \end{array} \right\}$$

Tables

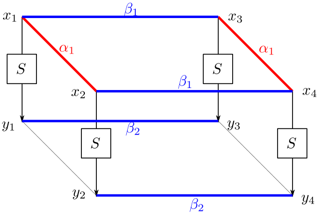


Figure: The Lower BCT (LBCT)

$$\texttt{LBCT}(\alpha_1, \beta_1, \beta_2) = \\ \#\left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l} S(x) \oplus S(x \oplus \beta_1) = \beta_2 \\ S^{-1}(S(x) \oplus \beta_2) \oplus S^{-1}(S(x \oplus \alpha_1) \oplus \beta_2) = \alpha_1 \end{array} \right\}$$

Tables

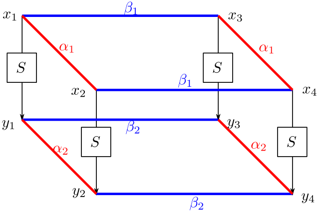


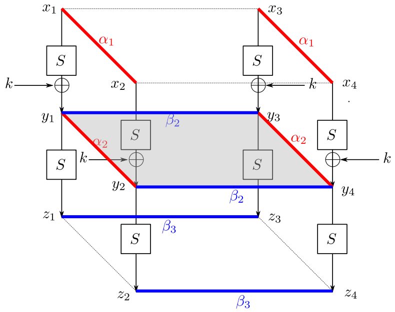
Figure: The Extended BCT (EBCT)

$$\texttt{EBCT}(\alpha_1, \beta_1, \alpha_2, \beta_2) =$$
$$\# \left\{ x \in \mathbb{F}_2^n \middle| \begin{array}{l} S(x) \oplus S(x \oplus \alpha_1) = \alpha_2 \\ S(x) \oplus S(x \oplus \beta_1) = \beta_2 \\ S^{-1}(S(x) \oplus \beta_2) \oplus S^{-1}(S(x \oplus \alpha_1) \oplus \beta_2) = \alpha_1 \end{array} \right\}.$$

Outline

1. Preliminary
2. New Properties of the Double Boomerang Connectivity Table
3. Application of the New Properties
4. MILP Model to Search for Boomerangs with Cluster Probability
5. Conclusion

How about two continuous S-boxes?
t continuous S-boxes?



DBCT

Definition

Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. The double boomerang connectivity table (DBCT) is defined as

$$\mathtt{DBCT}(\alpha_1, \beta_3) = \sum_{\alpha_2, \beta_2} \mathtt{dbct}(\alpha_1, \alpha_2, \beta_2, \beta_3),$$

where $\mathtt{dbct}(\alpha_1, \alpha_2, \beta_2, \beta_3) = \mathtt{UBCT}(\alpha_1, \alpha_2, \beta_2) \cdot \mathtt{LBCT}(\alpha_2, \beta_2, \beta_3)$.

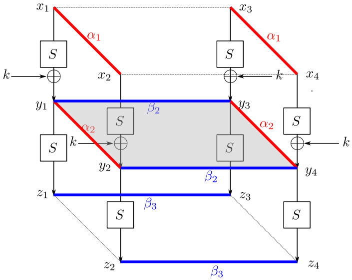


Figure: DBCT of general S-box

Property

Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For $\forall \alpha_1, \alpha_2, \beta_2, \beta_3 \in \mathbb{F}_2^n \backslash 0$, **nonzero** $\texttt{dbct}(\alpha_1, \alpha_2, \beta_2, \beta_3)$ occurs **mainly** when $\alpha_2 = \beta_2$. Consequently,

$$\begin{aligned}
\texttt{DBCT}(\alpha_1, \beta_3) &= \sum_{\alpha_2, \beta_2} \texttt{UBCT}(\alpha_1, \alpha_2, \beta_2) \cdot \texttt{LBCT}(\alpha_2, \beta_2, \beta_3) \\
&\geq \sum_{\alpha_2 = \beta_2} \texttt{UBCT}(\alpha_1, \alpha_2, \beta_2) \cdot \texttt{LBCT}(\alpha_2, \beta_2, \beta_3) \\
&= \sum_{\alpha_2} \texttt{DDT}(\alpha_1, \alpha_2) \cdot \texttt{DDT}(\alpha_2, \beta_3).
\end{aligned}$$

- **ladder switch; S-box switch**

Hard S-box

Definition

Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. S is hard if the following holds, for $\forall \alpha_1, \beta_3 \neq 0$,

$$\begin{aligned}
\mathtt{DBCT}(\alpha_1, \beta_3) &= \sum_{\alpha_2, \beta_2} \mathtt{UBCT}(\alpha_1, \alpha_2, \beta_2) \cdot \mathtt{LBCT}(\alpha_2, \beta_2, \beta_3) \\
&= \sum_{\alpha_2 = \beta_2} \mathtt{UBCT}(\alpha_1, \alpha_2, \beta_2) \cdot \mathtt{LBCT}(\alpha_2, \beta_2, \beta_3) \\
&= \sum_{\alpha_2} \mathtt{DDT}(\alpha_1, \alpha_2) \cdot \mathtt{DDT}(\alpha_2, \beta_3).
\end{aligned}$$

- **obtain a relationship btween** DBCT **and** DDT
- **reduce the time complexity**

DBCT

- **Hard S-box**: `PRESENT`, `LBlock-s0`, `LBlock-s1`, `MIBS`, `TWINE`...
- Others: `CRAFT`,`SKINNY`, `PRIDE`, `QARMA`...

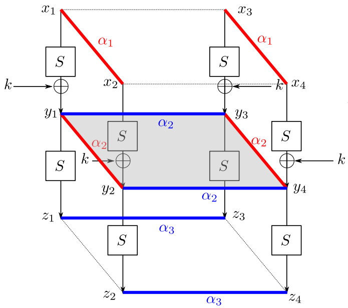


Figure: DBCT of **hard** S-box

Extensions

- **Multiple S-boxes**:(hard S-box)

$$t\text{-}\texttt{BCT}(\alpha, \beta) = \sum_{\alpha_2, \ldots, \alpha_t} \texttt{DDT}(\alpha, \alpha_2) \cdot \texttt{DDT}(\alpha_2, \alpha_3) \cdot \ldots \cdot \texttt{DDT}(\alpha_t, \beta).$$

Extensions

- **Multiple S-boxes**:

  $$t\text{-}\texttt{BCT}(\alpha,\beta) = \sum_{\alpha_2,\ldots,\alpha_t} \texttt{DDT}(\alpha,\alpha_2)\cdot\texttt{DDT}(\alpha_2,\alpha_3)\cdot\ldots\cdot\texttt{DDT}(\alpha_t,\beta).$$

- **Complex linear layer**:

  eg: `AES`

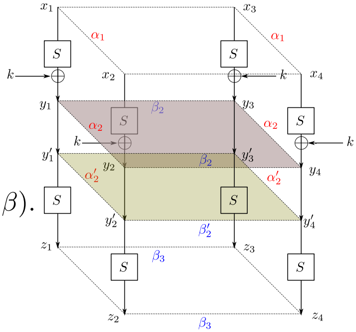


Figure: General `DBCT` with a complex linear layer in between

Table: Number of entries for each value for the $\texttt{DBCT}^{i,j}$ and the basic DBCT for the AES S-box

M	Table	65536	16	8	0	192-332
MC	$\texttt{DBCT}^{0,0}$	511	8	882	64135	-
	$\texttt{DBCT}^{0,1}$	511	3	252	64770	-
	$\texttt{DBCT}^{0,2}$	511	1	-	65024	-
	$\texttt{DBCT}^{0,3}$	511	3	126	64896	-
XOR	basic DBCT	511	-	-	-	65025

- the basic DBCT, the AES S-box is **hard** without zero values
- $\texttt{DBCT}^{i,j}$ with complex linear layer, most values are zero

Outline

1 Preliminary

2 New Properties of the Double Boomerang Connectivity Table

3 Application of the New Properties

4 MILP Model to Search for Boomerangs with Cluster Probability

5 Conclusion

Revisiting Boomerang Attack on CRAFT

- **Through the same boomerang distinguisher with the different S-boxes, how DBCT uniformity and hard S-box matter?**
  - eg: 7-round distinguisher of CRAFT

Table: Probability of the 7-round distinguisher with different S-boxes

S-box	DDT uni.	BCT uni.	DBCT uni.	Hard	Probability		
					Max	Min	Average
CRAFT	4	16	128	✗	$2^{-10.39}$	$2^{-14.97}$	$2^{-13.37}$
QARMA	4	10	48	✗	$2^{-13.99}$	$2^{-15.18}$	$2^{-14.65}$
PRESENT	4	16	40	✓	$2^{-15.47}$	$2^{-15.63}$	$2^{-15.57}$
LBlock-s0	4	16	40	✓	$2^{-15.51}$	$2^{-15.62}$	$2^{-15.56}$
LBlock-s1	4	16	40	✓	$2^{-15.41}$	$2^{-15.63}$	$2^{-15.56}$
MIBS	4	6	32	✓	$2^{-15.59}$	$2^{-15.62}$	$2^{-15.60}$
TWINE	4	6	28	✓	$2^{-15.58}$	$2^{-15.62}$	$2^{-15.60}$

Table: Probability of the 7-round distinguisher with different S-boxes

S-box	DDT uni.	BCT uni.	DBCT uni.	Hard	Probability		
					Max	Min	Average
CRAFT	4	16	128	✗	$2^{-10.39}$	$2^{-14.97}$	$2^{-13.37}$
PRESENT	4	16	40	✓	$2^{-15.47}$	$2^{-15.63}$	$2^{-15.57}$

- CRAFT and PRESENT share the same DDT and BCT
- PRESENT with the smaller DBCT has a lower probability

Table: Probability of the 7-round distinguisher with different S-boxes

S-box	DDT uni.	BCT uni.	DBCT uni.	Hard	Probability		
					Max	Min	Average
QARMA	4	10	48	✗	$2^{-13.99}$	$2^{-15.18}$	$2^{-14.65}$
PRESENT	4	16	40	✓	$2^{-15.47}$	$2^{-15.63}$	$2^{-15.57}$

- QARMA has better BCT than PRESENT
- PRESENT with the smaller DBCT has the lower probability

Table: Probability of the 7-round distinguisher with different S-boxes

S-box	DDT uni.	BCT uni.	DBCT uni.	Hard	Probability		
					Max	Min	Average
PRESENT	4	16	40	✓	$2^{-15.47}$	$2^{-15.63}$	$2^{-15.57}$
LBlock-s0	4	16	40	✓	$2^{-15.51}$	$2^{-15.62}$	$2^{-15.56}$
LBlock-s1	4	16	40	✓	$2^{-15.41}$	$2^{-15.63}$	$2^{-15.56}$

- They share the same DDT, BCT and DBCT
- They have almost the same probability

Table: Probability of the 7-round distinguisher with different S-boxes

S-box	DDT uni.	BCT uni.	DBCT uni.	Hard	Probability		
					Max	Min	Average
MIBS	4	6	32	✓	$2^{-15.59}$	$2^{-15.62}$	$2^{-15.60}$
TWINE	4	6	28	✓	$2^{-15.58}$	$2^{-15.62}$	$2^{-15.60}$

- MIBS and TWINE have the small BCT and small DBCT
- They have the low probability

- **Observation:** Apart from the uniformity of `BCT` and `DDT`, the uniformity of `DBCT` is a new measure criterion to evaluate the performance of S-box for resisting boomerang attacks.

Revisiting Boomerang Attack on TweAES and Deoxys-BC

- **For the AES, the DBCT with complex linear layer has too many zero values.**
  - 7-round boomerang distinguisher of TweAES
  - 8-round boomerang distinguisher of Deoxys-BC in the model RTK1
  - 10-round boomerang disitnguisher of Deoxys-BC in the model RTK2

  Zero probability

- hard S-box with a complex linear layer should be treated carefully

Outline

1 Preliminary

2 New Properties of the Double Boomerang Connectivity Table

3 Application of the New Properties

4 MILP Model to Search for Boomerangs with Cluster Probability

5 Conclusion

Previous

- search for good **truncated** boomerang characteristic with the least active S-boxes
- search for the best **instantiations**

⇒

Our

- formula for the probability of **clusters**
- MILP model to search for good **clusters**

Formula for the Probability of Boomerang clusters

- **Probability in E_0/E_1.** Suppose E_0 covers the first r_0 rounds, E_1 consists of the last r_1 rounds. For $\forall \Delta, \Delta_1, \nabla_1, \nabla \neq 0$, the probability are $\mathbb{P}_{E_0}(\Delta \rightleftarrows \Delta_1) = \hat{p}^2$ and $\mathbb{P}_{E_1}(\nabla_1 \rightleftarrows \nabla) = \hat{q}^2$ on average, *i.e.*,

$$\hat{p} = 2^{-s \cdot c_0} \cdot \frac{1}{|\Delta_1|},$$

$$\hat{q} = 2^{-s \cdot c_1} \cdot \frac{1}{|\nabla_1|},$$

  where c_0 and c_1 are the number of cells which need to be zero from uniformity and s is the cell size.

- **Probability in E_m.** Suppose E_m is composed of the middle r_m rounds. For $\forall \Delta_1, \nabla_1 \neq 0$ the probability is $\mathbb{P}_{E_m}(\Delta_1 \rightleftarrows \nabla_1) = \hat{r}$ on average and

$$\hat{r} = 2^{-s \cdot c_m},$$

where c_m is the *condition* consumed in E_m. (c_m is the sum of the number of cells which need to be zero from uniformity, the number of `UDDT2` and `LDDT2`, the number of $m-$`BCT` and the number of `BCT`.)

eg: CRAFT

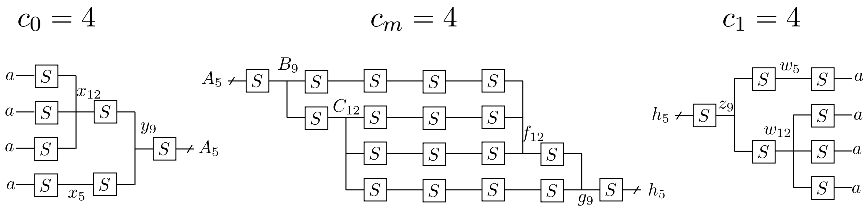


Figure: The difference propagation of E_0(left), the difference propagation of E_m(middle) and the difference propagation of E_1(right)

- the conditions are closely related to the actual probability

MILP Model to Search for Boomerangs with Good Cluster Probabilities

- **The Attribute Propagation**
  - Modeling of the attribute propagation through **subbytes**
  - Modeling of the attribute propagation through **XOR operation** with the condition consuming
  - Modeling of the **table**
  - Modeling of the upper and lower **boundary**

- **Objective Function:** to minimize the number of conditions consuming for E:

$$obj = 2c_0 + 2c_1 + c'_0 + c'_1 + c_m.$$

eg: new 9/10 round boomerang distinguisher of `CRAFT`

Outline

1 Preliminary

2 New Properties of the Double Boomerang Connectivity Table

3 Application of the New Properties

4 MILP Model to Search for Boomerangs with Cluster Probability

5 Conclusion

Conclusion

- **Property of** `DBCT`
  - the ladder switch and S-box switch happen in most cases.
  - **hard S-box**: only the ladder switch and S-box switch are possible.
    eg: evaluate the performance of S-box; hard S-box with a complex linear layer should be treated carefully
- **MILP model**
  - formula for the probability of clusters
  - model with cluster probability
    eg: 9/10-round distinguisher with a higher probability of `CRAFT`

Thank you!

Q & A