On the Boomerang Uniformity of Cryptographic Sboxes

Christina Boura and Anne Canteaut

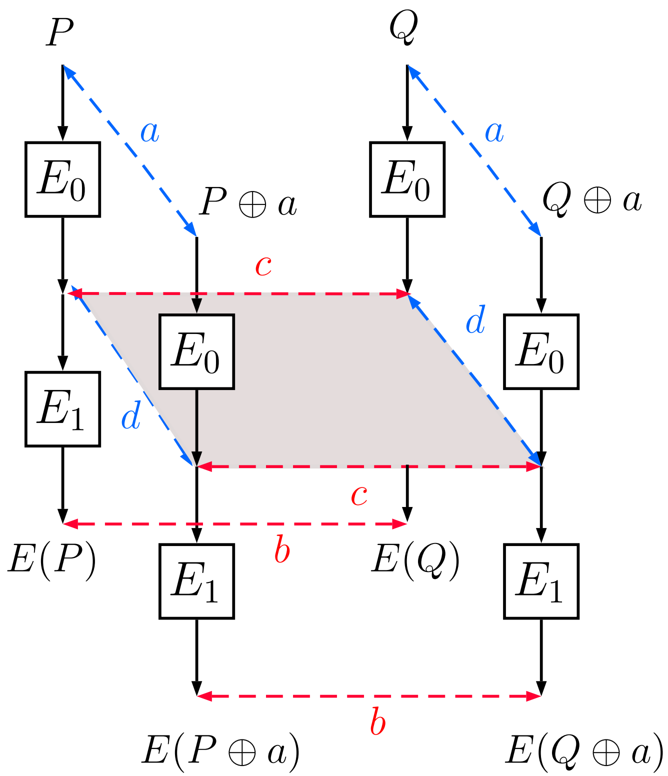
University of Versailles, France
Inria Paris, France

FSE 2019, Paris

Boomerang attacks [Wagner 99]

Combine differentials for two sub-ciphers:

$$a \xrightarrow{E_0} d \text{ with proba } p \text{ and } c \xrightarrow{E_1} b \text{ with proba } q$$

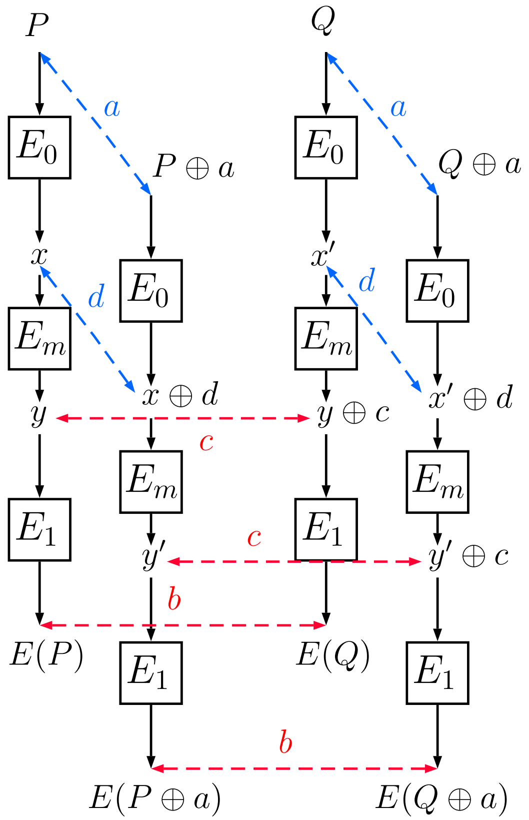


$$\mathbf{Pr}_x[E^{-1}(E(x) \oplus b) \oplus E^{-1}(E(x \oplus a) \oplus b) = a] = p^2q^2$$

The independence assumption may fail! [Murphy 11]

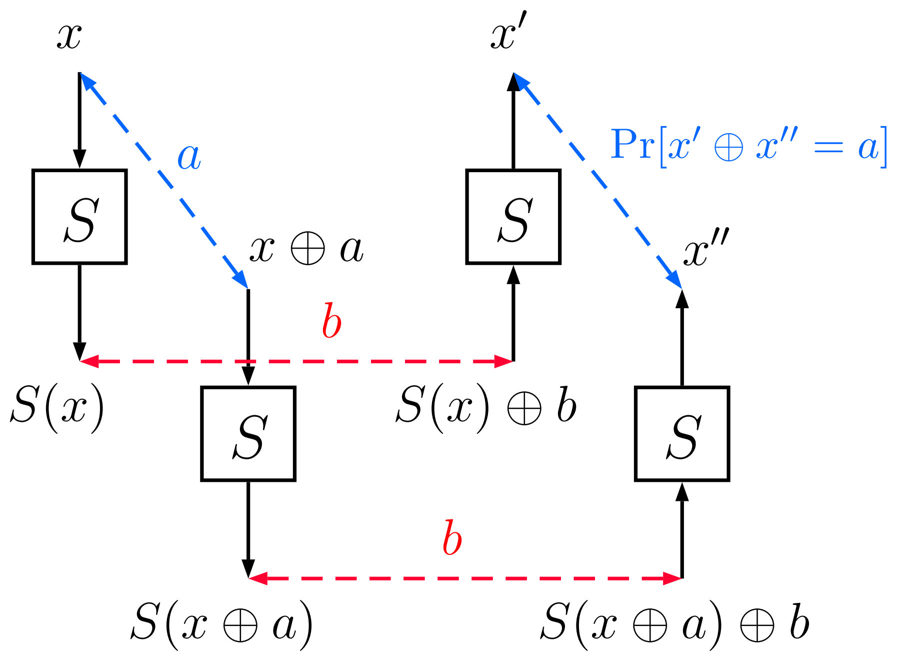
Sandwich attack [Dunkelman Keller Shamir 10]:

add one middle subcipher $\boldsymbol{E_m}$ to handle the dependencies



Compute $\mathbf{Pr}_{\boldsymbol{x}}[\boldsymbol{E_m^{-1}}(\boldsymbol{E_m}(\boldsymbol{x}) \oplus \boldsymbol{c}) \oplus \boldsymbol{E_m^{-1}}(\boldsymbol{E_m}(\boldsymbol{x} \oplus \boldsymbol{d}) \oplus \boldsymbol{c}) = \boldsymbol{d}]$

Boomerang Connectivity Table [Cid Huang Peyrin Sasaki Song 18]



$$\beta(a, b) = \{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}$$

Example

DDT $\delta(a,b)$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	4	.	.	.	.	2	2	.	2	.	2	.	2	2	.
2	.	.	.	2	.	.	.	2	.	4	2	.	2	2	.	2
3	.	.	2	.	.	.	.	2	2	.	2	2	2	.	4	.
4	.	.	.	.	.	2	2	.	2	.	2	.	.	4	2	2
5	.	.	.	.	2	.	2	.	2	2	.	4	2	.	.	2
6	.	2	.	.	2	2	2	4	.	.	2	.	2	.	.	.
7	.	2	2	2	.	.	4	2	2	.	.	.	.	.	.	2
8	.	.	.	2	2	2	.	2	.	.	.	2	.	.	2	4
9	.	2	4	.	.	2	.	.	.	2	.	.	2	.	2	2
a	.	.	2	2	2	.	2	.	.	.	.	.	4	2	2	.
b	.	2	.	2	.	4	.	.	2	.	.	2	2	2	.	.
c	.	.	2	2	.	2	2	.	.	2	4	2	.	.	.	.
d	.	2	2	.	4	.	.	.	.	.	2	2	.	2	.	2
e	.	2	.	4	2	.	.	.	2	2	2	.	.	.	2	.
f	.	.	2	.	2	2	.	2	4	2	.	.	.	2	.	.

BCT $\beta(a,b)$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	4	.	.	.	.	6	6	.	2	.	2	.	2	2	.
2	16	.	.	6	.	.	.	2	.	4	6	.	2	2	.	2
3	16	.	6	.	.	.	.	2	2	.	2	2	6	.	4	.
4	16	.	.	.	.	6	2	.	6	.	2	.	.	4	2	2
5	16	.	.	.	6	.	2	.	2	2	.	4	2	.	.	6
6	16	6	.	.	2	2	6	4	.	.	2	.	2	.	.	.
7	16	6	2	2	.	.	4	6	2	.	.	.	.	.	.	2
8	16	.	.	2	6	2	.	2	.	.	.	6	.	.	2	4
9	16	2	4	.	.	2	.	.	.	2	.	.	6	.	6	2
a	16	.	6	2	2	.	2	.	.	.	.	.	4	2	6	.
b	16	2	.	2	.	4	.	.	6	.	.	2	2	6	.	.
c	16	.	2	6	.	2	2	.	.	6	4	2	.	.	.	.
d	16	2	2	.	4	.	.	.	.	.	2	6	.	2	.	6
e	16	2	.	4	2	.	.	.	2	6	6	.	.	.	2	.
f	16	.	2	.	2	6	.	2	4	2	.	.	.	6	.	.

Basic properties [Cid Huang Peyrin Sasaki Song 18]

$$\beta(a, b) = \{x \in \mathbb{F}_2^n : S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}$$

$$\beta(a, 0) = 2^n \text{ and } \beta(0, b) = 2^n$$

Relevant parameter: boomerang uniformity of S

$$\beta_S = \max_{a,b \neq 0} \beta(a, b)$$

For nonzero a and b:

$$\beta(a, b) \geq \delta(a, b)$$

with equality for all pairs (a, b) when S is an APN permutation, i.e. all $\delta(a, b) \leq 2$.

Open problem:

Find a permutation of $\mathbb{F}_2^n$, n even, with the lowest possible boomerang uniformity.

Our contributions

1. Lowest boomerang uniformity for 4-bit Sboxes
2. An alternative formulation
3. BCT of the inverse mapping
4. BCT of quadratic power functions

Invariance under equivalence

Affine equivalence:

Let F and G be such that

$$G = A_2 \circ F \circ A_1$$

with $A_1 : x \mapsto L_1(x) \oplus a_1$ and $A_2 : x \mapsto L_2(x) \oplus a_2$ affine permutations.
Then,

$$\beta_G(a, b) = \beta_F\left(L_1(a), L_2^{-1}(b)\right)$$

Inversion:

$$\beta_{S^{-1}}(a, b) = \beta_S(b, a)$$

Other equivalences: the boomerang uniformity is not preserved by extended affine equivalence, i.e. $G = A_2 \circ F \circ A_1 \oplus A_0$

BCT of 4-bit permutations with $\delta = 4$

	$\mathcal{L}(S)$	[DeCan 07]	[LP07]	n_0	n_2	n_4	n_6	n_8	n_{10}	n_{16}	β_S
1	8	3	G_3	120	60	15	30	0	0	0	6
2	8	6	G_5	108	72	27	18	0	0	0	6
3	8	2	G_6	104	80	27	10	4	0	0	8
4	8	8	G_{11}	100	85	30	5	5	0	0	8
5	8	1	G_{13}	105	78	28	11	2	1	0	10
6	8	4	G_4	112	72	23	14	0	4	0	10
7	8	5	G_7	105	80	30	5	0	5	0	10
8	8	7	G_{12}	110	75	25	10	0	5	0	10
9	8	9	G_9	108	69	28	14	5	1	0	10
10	8	10	G_{14}	108	70	27	13	6	1	0	10
11	8	12	G_{10}	108	69	30	12	3	3	0	10
12	8	13	G_2	107	64	32	8	12	0	2	16
13	8	14	G_1	107	60	36	12	8	0	2	16
14	8	15	G_8	103	72	32	0	16	0	2	16
15	12	34	–	112	57	35	14	0	7	0	10
16	12	35	–	109	60	34	15	4	3	0	10
17	12	36	–	109	60	34	15	4	3	0	10
18	12	37	–	110	58	30	14	12	0	1	16
19	12	38	–	106	62	36	8	10	2	1	16

Boomerang uniformity of 4-bit permutations

Proposition.

The smallest boomerang uniformity for a 4-bit permutation is 6.

An alternative formulation

$$\beta(a,b) = \left|\{x : S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\}\right|$$

$$= \sum_{\gamma \neq 0} \left|\{x : S(x) \oplus S(x \oplus a) = \gamma \wedge S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x) \oplus \gamma \oplus b) = a\}\right|$$

When $\gamma = b$: (2) is equivalent to (1)

When $\gamma \neq b$: Let

$$\mathcal{V}_{a,\gamma} = \{S(x) : S(x) \oplus S(x \oplus a) = \gamma\}$$

(1) means that $S(x) \in \mathcal{V}_{a,\gamma}$. (2) means that $(S(x) \oplus b) \in \mathcal{V}_{a,\gamma}$.

$$\Rightarrow \beta(a,b) = \delta(a,b) + \sum_{\gamma \neq 0, b} \left|(\mathcal{V}_{a,\gamma} \cap (\mathcal{V}_{a,\gamma} \oplus b))\right|$$

For planar permutations [Daemen, Rijmen 07]

Any S with $\delta_S \leq 4$ is planar.

In the previous formula:

if S is planar, $\mathcal{V}_{a,\gamma}$ and $(\mathcal{V}_{a,\gamma} \oplus b)$ are 2 cosets of the same $V_{a,\gamma}$.

$\Rightarrow$ They are either equal or disjoint.

$$\begin{aligned}\beta(a,b) &= \delta(a,b) + \sum_{\gamma \neq 0, b} \left|\left(\mathcal{V}_{a,\gamma} \cap (\mathcal{V}_{a,\gamma} \oplus b)\right)\right| \\ &= \sum_{\gamma \neq 0 \,:\, b \in V_{a,\gamma}} \delta(a,\gamma)\end{aligned}$$

Example

DDT $\delta(a,b)$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	4	.	.	.	.	2	2	.	2	.	2	.	2	2	.
2	.	.	.	2	.	.	.	2	.	4	2	.	2	2	.	2
3	.	.	2	.	.	.	.	2	2	.	2	2	2	.	4	.
4	.	.	.	.	.	2	2	.	2	.	2	.	.	4	2	2
5	.	.	.	.	2	.	2	.	2	2	.	4	2	.	.	2
6	.	2	.	.	2	2	2	4	.	.	2	.	2	.	.	.
7	.	2	2	2	.	.	4	2	2	.	.	.	.	.	.	2
8	.	.	.	2	2	2	.	2	.	.	.	2	.	.	2	4
9	.	2	4	.	.	2	.	.	.	2	.	.	2	.	2	2
a	.	.	2	2	2	.	2	.	.	.	.	.	4	2	2	.
b	.	2	.	2	.	4	.	.	2	.	.	2	2	2	.	.
c	.	.	2	2	.	2	2	.	.	2	4	2	.	.	.	.
d	.	2	2	.	4	.	.	.	.	.	2	2	.	2	.	2
e	.	2	.	4	2	.	.	.	2	2	2	.	.	.	2	.
f	.	.	2	.	2	2	.	2	4	2	.	.	.	2	.	.

BCT $\beta(a,b)$

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	4	.	.	.	.	6	6	.	2	.	2	.	2	2	.
2	16	.	.	6	.	.	.	2	.	4	6	.	2	2	.	2
3	16	.	6	.	.	.	.	2	2	.	2	2	6	.	4	.
4	16	.	.	.	.	6	2	.	6	.	2	.	.	4	2	2
5	16	.	.	.	6	.	2	.	2	2	.	4	2	.	.	6
6	16	6	.	.	2	2	6	4	.	.	2	.	2	.	.	.
7	16	6	2	2	.	.	4	6	2	.	.	.	.	.	.	2
8	16	.	.	2	6	2	.	2	.	.	.	6	.	.	2	4
9	16	2	4	.	.	2	.	.	.	2	.	.	6	.	6	2
a	16	.	6	2	2	.	2	.	.	.	.	.	4	2	6	.
b	16	2	.	2	.	4	.	.	6	.	.	2	2	6	.	.
c	16	.	2	6	.	2	2	.	.	6	4	2	.	.	.	.
d	16	2	2	.	4	.	.	.	.	.	2	6	.	2	.	6
e	16	2	.	4	2	.	.	.	2	6	6	.	.	.	2	.
f	16	.	2	.	2	6	.	2	4	2	.	.	.	6	.	.

Example

$$\beta(a,b) = \sum_{\gamma \neq 0 \,:\, b \in V_{a,\gamma}} \delta(a,\gamma)$$

$a = 1$

$$\mathcal{V}_{1,1} = \{0,1,6,7\}, \quad \mathcal{V}_{1,6} = \{0,6\} \oplus 11, \quad \mathcal{V}_{1,7} = \{0,7\} \oplus 9$$
$$\mathcal{V}_{1,9} = \{0,9\} \oplus 5, \quad \mathcal{V}_{1,11} = \{0,11\} \oplus 3 \quad \mathcal{V}_{1,13} = \{0,13\} \oplus 2$$
$$\mathcal{V}_{1,14} = \{0,14\} \oplus 4$$

Example

$$\beta(a,b) = \sum_{\gamma \neq 0 \,:\, b \in V_{a,\gamma}} \delta(a,\gamma)$$

$a = 1$

$$\mathcal{V}_{1,1} = \{0,1,6,7\}, \quad \mathcal{V}_{1,6} = \{0,6\} \oplus 11, \quad \mathcal{V}_{1,7} = \{0,7\} \oplus 9$$
$$\mathcal{V}_{1,9} = \{0,9\} \oplus 5, \quad \mathcal{V}_{1,11} = \{0,11\} \oplus 3 \quad \mathcal{V}_{1,13} = \{0,13\} \oplus 2$$
$$\mathcal{V}_{1,14} = \{0,14\} \oplus 4$$

For $b = 6$:

$$\beta(1,6) = \delta(1,1) + \delta(1,6) = 4 + 2 = 6$$

Details on 4-bit Sboxes with $\delta_S = 4$

We can prove:

- If the DDT has a row with at least two values 4, then $\boldsymbol{\beta_S \geq 8}$;
- If each row in the DDT has at most two values 4, then $\boldsymbol{\beta_S \leq 10}$;
- If the DDT has a row with four values 4, then $\boldsymbol{\beta_S = 16}$.

BCT of the inverse mapping

$S : x \mapsto x^{-1}$ over $\mathbb{F}_{2^n}$, n even.

Main result.

$$\beta_S = \begin{cases} 4, & \text{if} \quad n \equiv 2 \mod 4 \\ 6, & \text{if} \quad n \equiv 0 \mod 4 \end{cases}$$

More precisely,

- If $n \equiv 2 \bmod 4$, for any nonzero a, b,

$$\beta_S(a,b) = \begin{cases} 4 & \text{if } b \in \{a^{-1}\omega, a^{-1}(\omega \oplus 1)\} \\ \delta_S(a,b) & \text{otherwise} \end{cases}$$

- If $n \equiv 0 \bmod 4$, for any nonzero a, b,

$$\beta_S(a,b) = \begin{cases} 6 & \text{if } b \in \{a^{-1}\omega, a^{-1}(\omega \oplus 1)\} \\ \delta_S(a,b) & \text{otherwise} \end{cases}$$

where ω is an element in $\mathbb{F}_4 \setminus \mathbb{F}_2$

BCT of quadratic function with $\delta = 4$

General result.

Any quadratic permutation S with differential uniformity 4 satisfies $\beta_S \leq 12$.

Monomial permutations. For $n \equiv 2 \bmod 4$,

$$S : x \mapsto x^{2^t+1} \text{ over } \mathbb{F}_{2^n} \text{ with } \gcd(t,n) = 2$$

satisfies $\delta_S = \beta_S = 4$.

Conclusion

The lowest possible boomerang uniformity for an $\boldsymbol{n}$-bit Sbox is

$\boldsymbol{= 2}$ when $\boldsymbol{n}$ is odd or $\boldsymbol{n = 6}$;

$\leq \mathbf{4}$ when $\boldsymbol{n} \equiv \mathbf{2 \bmod 4}$;

$\leq \mathbf{6}$ when $\boldsymbol{n} \equiv \mathbf{0 \bmod 4}$.