Boomerang Connectivity Table Revisited

Ling Song[1,2], Xianrui Qin[3], Lei Hu[2]

1. Nanyang Technological University, Singapore
2. Institute of Information Engineering, CAS, China
3. Shandong University, China

FSE 2019 @ Paris

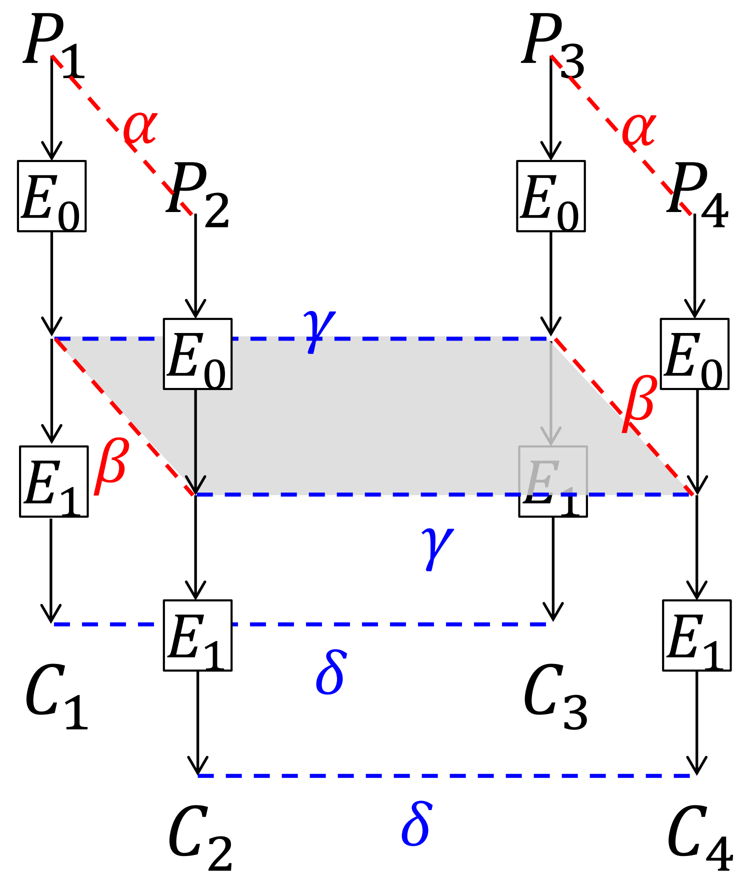
Boomerang Attacks

Proposed by [Wag99] to combine two diff. trails:

- E_0: $\Pr[\alpha \rightarrow \beta] = p$
- E_1: $\Pr[\gamma \rightarrow \delta] = q$

Distinguishing probability:

$$p^2q^2$$



Boomerang Attacks

Proposed by [Wag99] to combine two diff. trails:

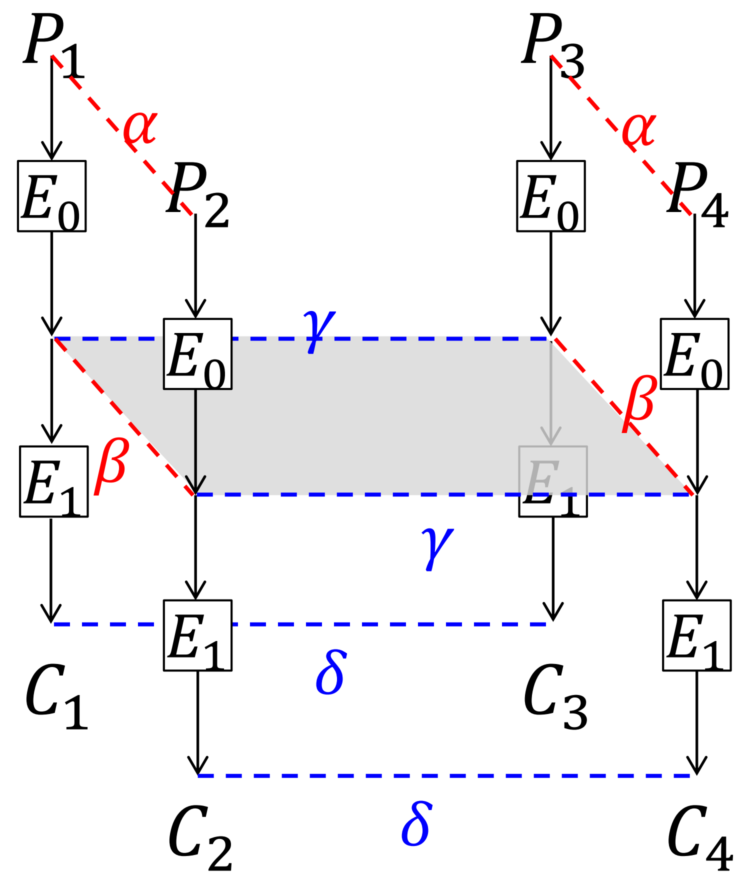
- $E_0 : \Pr[\alpha \rightarrow \beta] = p$
- $E_1 : \Pr[\gamma \rightarrow \delta] = q$

Distinguishing probability:

$$p^2 q^2$$

Boomerang attacks: *When you send it properly, it always comes back to you.*

https://www.australiathegift.com.au/shop/boomerang-with-stand/



Boomerang Attacks

Proposed by [Wag99] to combine two diff. trails:

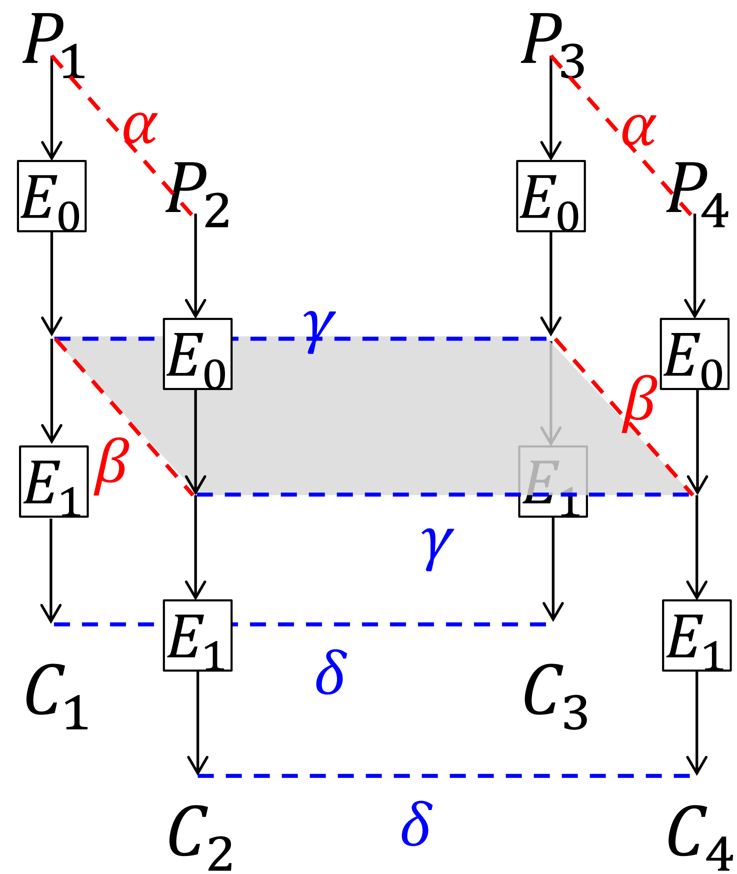
- $E_0 : \Pr[\alpha \rightarrow \beta] = p$
- $E_1 : \Pr[\gamma \rightarrow \delta] = q$

Distinguishing probability:

$$p^2 q^2$$

Boomerang attacks: *When you send it properly, it always comes back to you.*

https://www.australiathegift.com.au/shop/boomerang-with-stand/



[Wag99]: *Assumed two trails are independent.*

NOT always correct

Two Trails in Boomerang Attacks

Dependency can help attackers

- [BDD03]: Middle-round S-box trick
- [BK09]: Boomerang switch: Ladder switch / Feistel switch / S-box switch

Dependency can spoil attacks.

- [Mer09]: Incompatible trails

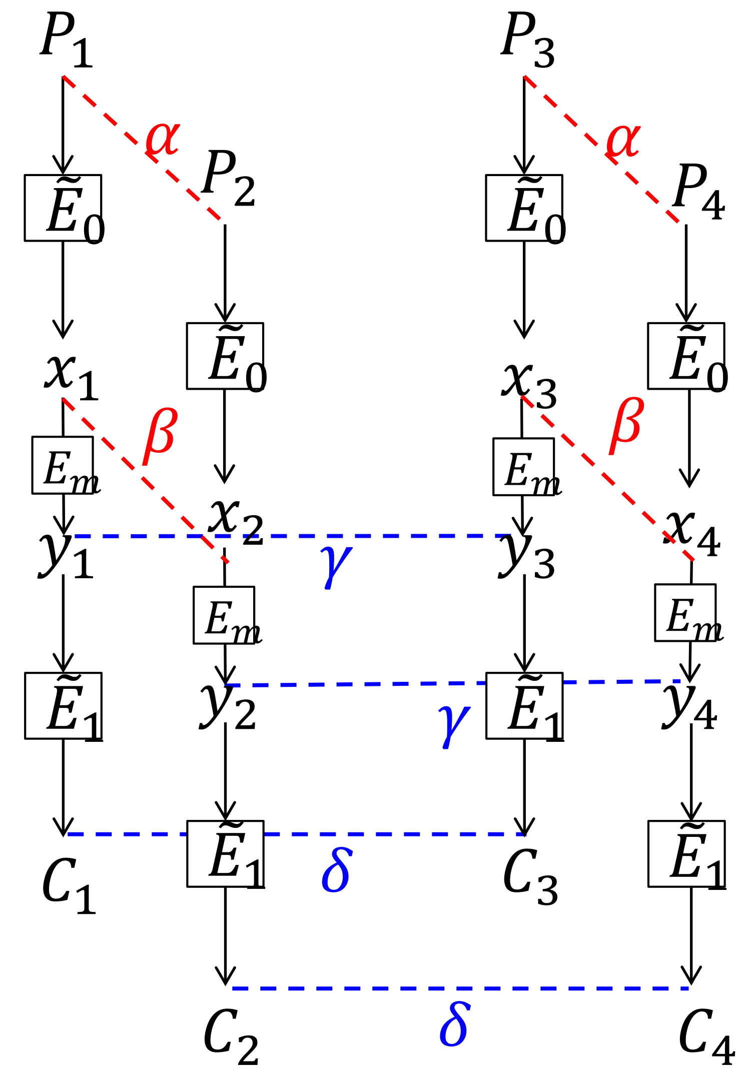
Sandwich Attacks [DKS10]

Decompose the cipher into three parts

- E_m handles the dependency.
- $\tilde{E}_0 \leftarrow E_0 \backslash E_m$: $\Pr[\alpha \rightarrow \beta] = \tilde{p}$
- $\tilde{E}_1 \leftarrow E_1 \backslash E_m$: $\Pr[\gamma \rightarrow \delta] = \tilde{q}$

Distinguishing probability:

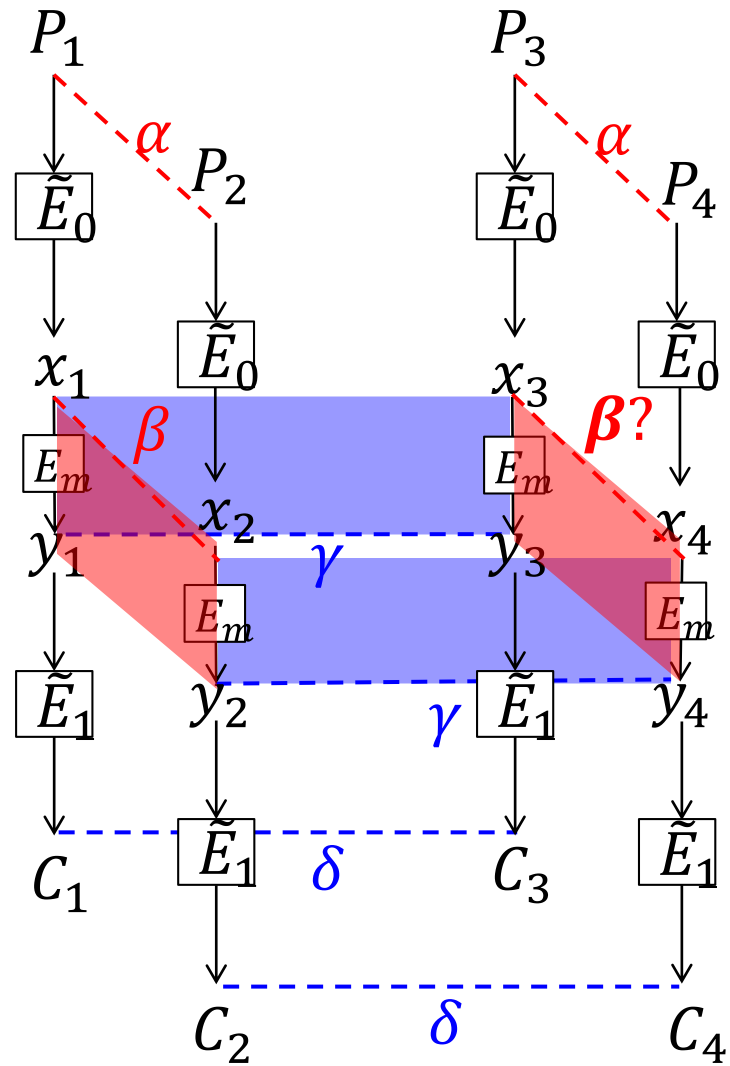
$$\tilde{p}^2 \tilde{q}^2 r$$



Sandwich Attacks [DKS10]

Decompose the cipher into three parts

- E_m handles the dependency.
- $\tilde{E}_0 \leftarrow E_0 \setminus E_m$: $\Pr[\alpha \rightarrow \beta] = \tilde{p}$
- $\tilde{E}_1 \leftarrow E_1 \setminus E_m$: $\Pr[\gamma \rightarrow \delta] = \tilde{q}$



Distinguishing probability:

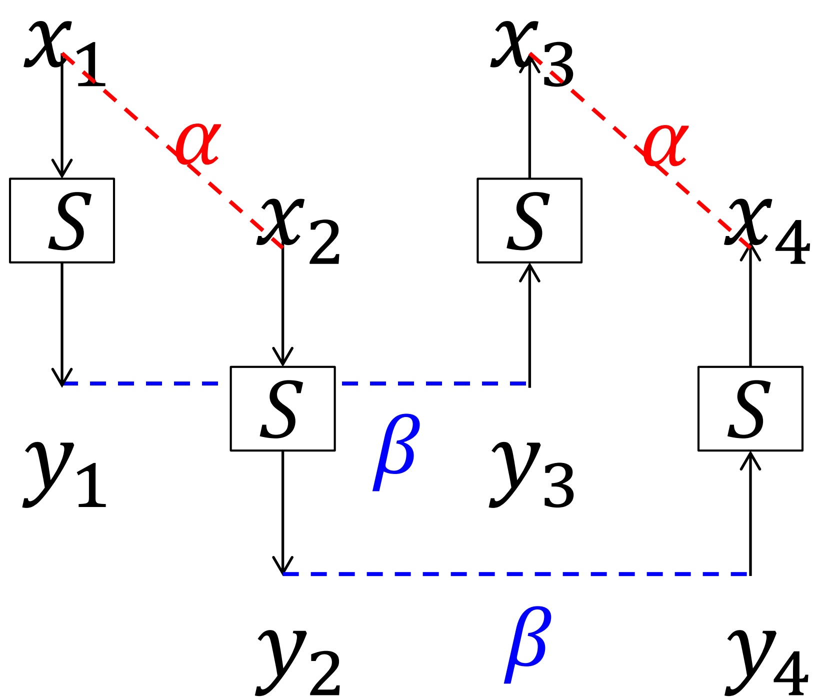
$$\tilde{p}^2\tilde{q}^2 r$$

$$r = \Pr[x_3 \oplus x_4 = \beta \mid (x_1 \oplus x_2 = \beta) \wedge (y_1 \oplus y_3 = \gamma) \wedge (y_2 \oplus y_4 = \gamma)]$$

BCT [CHP+18]

Boomerang Connectivity Table (BCT)

- Calculate r theoretically when E_m is composed of a single S–box layer.
- Unify previous observations on the S-box (incompatibilities and switches)



Our Work

Motivation

- The actual boundaries of E_m which contains dependency
- How to calculate r when E_m contains multiple rounds?

Contribution

- Generalized framework of BCT
  - Determine the boundaries of E_m
  - Calculate r of E_m in the sandwich attack

DDT: Difference Distribution Table

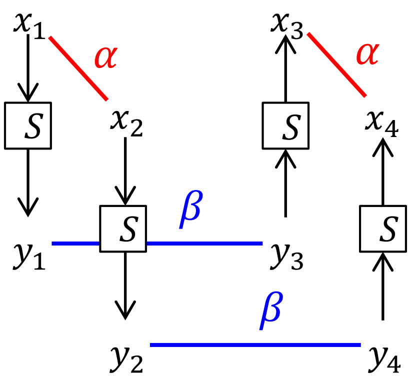
$$DDT(\alpha,\beta) = \#\{x \in \{0,1\}^n | S(x) \oplus S(x \oplus \alpha) = \beta\}$$

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

SKINNY's 4-bit S-box

BCT: Boomerang Connectivity Table

$$BCT(\alpha,\beta) = \#\{x \in \{0,1\}^n \mid S^{-1}(S(x) \oplus \beta) \oplus S^{-1}(S(x \oplus \alpha) \oplus \beta) = \alpha\}$$



β

α

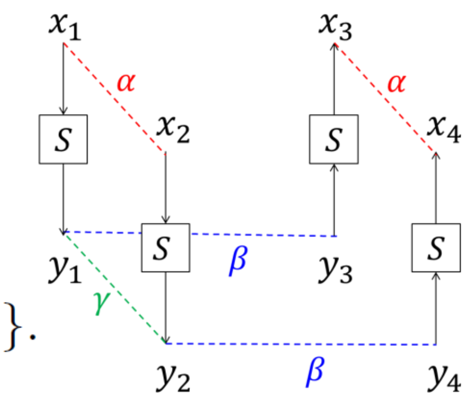
α \ β	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	0	16	0	0	0	0	0	8	8	8	8	0	0	0	0
2	16	8	0	8	8	16	8	0	0	0	0	0	0	0	0	0
3	16	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2
4	16	0	8	0	0	0	2	2	4	4	4	4	2	2	0	0
5	16	0	8	0	0	0	2	2	4	4	4	4	2	2	0	0
6	16	2	0	2	2	0	0	2	2	0	2	0	0	2	2	0
7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

SKINNY's 4-bit S-box

Relation between DDT and BCT

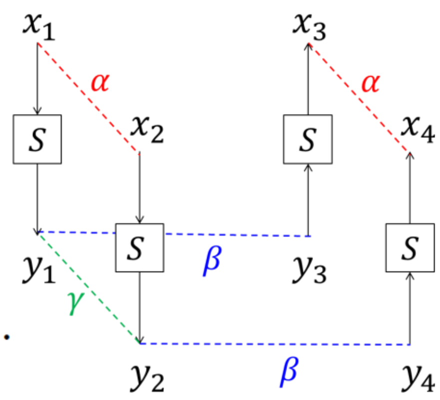
Let

$$\mathcal{X}_{\mathrm{DDT}}(\alpha,\beta) \triangleq \{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\},$$
$$\mathcal{Y}_{\mathrm{DDT}}(\alpha,\beta) \triangleq \{S(x) \in \mathbb{F}_2^n : x \in \mathbb{F}_2^n, S(x) \oplus S(x \oplus \alpha) = \beta\}.$$



Relation between DDT and BCT

Let



$$\mathcal{X}_{\mathtt{DDT}}(\alpha,\beta) \triangleq \{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\},$$
$$\mathcal{Y}_{\mathtt{DDT}}(\alpha,\beta) \triangleq \{S(x) \in \mathbb{F}_2^n : x \in \mathbb{F}_2^n, S(x) \oplus S(x \oplus \alpha) = \beta\}.$$

Proposition 1 ([BC18]). *For any permutation S of $\mathbb{F}_2^n$, for all $\alpha, \beta \in \mathbb{F}_2^n$, we have*

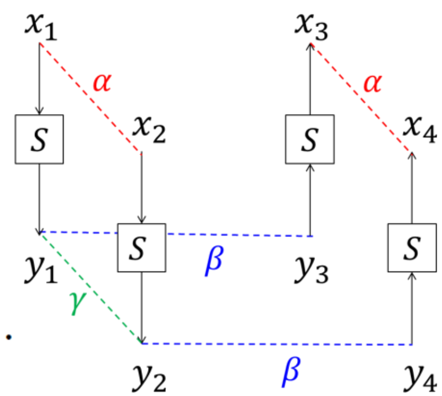
$$\mathtt{BCT}(\alpha,\beta) = \mathtt{DDT}(\alpha,\beta) + \sum_{\gamma \neq 0,\beta} \#(\mathcal{Y}_{\mathtt{DDT}}(\alpha,\gamma) \cap (\mathcal{Y}_{\mathtt{DDT}}(\alpha,\gamma) \oplus \beta)). \tag{1}$$

Note that, due to symmetry, Eq. 1 is equivalent to

$$\mathtt{BCT}(\alpha,\beta) = \mathtt{DDT}(\alpha,\beta) + \sum_{\gamma \neq 0,\alpha} \#(\mathcal{X}_{\mathtt{DDT}}(\gamma,\beta) \cap (\mathcal{X}_{\mathtt{DDT}}(\gamma,\beta) \oplus \alpha)).$$

Relation between DDT and BCT

Let



$$\mathcal{X}_{\mathrm{DDT}}(\alpha,\beta) \triangleq \{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \alpha) = \beta\},$$
$$\mathcal{Y}_{\mathrm{DDT}}(\alpha,\beta) \triangleq \{S(x) \in \mathbb{F}_2^n : x \in \mathbb{F}_2^n, S(x) \oplus S(x \oplus \alpha) = \beta\}.$$

Proposition 1 ([BC18]). *For any permutation S of $\mathbb{F}_2^n$, for all $\alpha, \beta \in \mathbb{F}_2^n$, we have*

$$\mathrm{BCT}(\alpha,\beta) = \mathrm{DDT}(\alpha,\beta) + \sum_{\gamma \neq 0,\beta} \#(\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) \cap (\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) \oplus \beta)). \quad (1)$$

Note that, due to symmetry, Eq. 1 is equivalent to

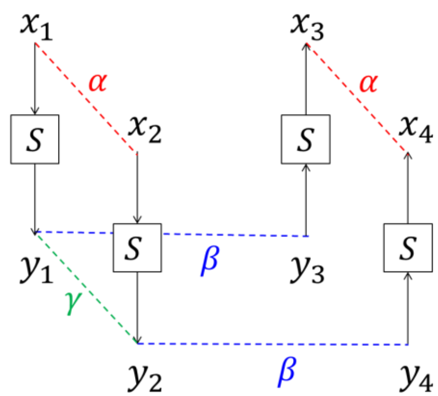
$$\mathrm{BCT}(\alpha,\beta) = \mathrm{DDT}(\alpha,\beta) + \sum_{\gamma \neq 0,\alpha} \#(\mathcal{X}_{\mathrm{DDT}}(\gamma,\beta) \cap (\mathcal{X}_{\mathrm{DDT}}(\gamma,\beta) \oplus \alpha)).$$

Eq. 1 can be re-written as

$$\mathrm{BCT}(\alpha,\beta) = \sum_{\gamma} \#(\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) \cap (\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) \oplus \beta)).$$

New Explanation of BCT

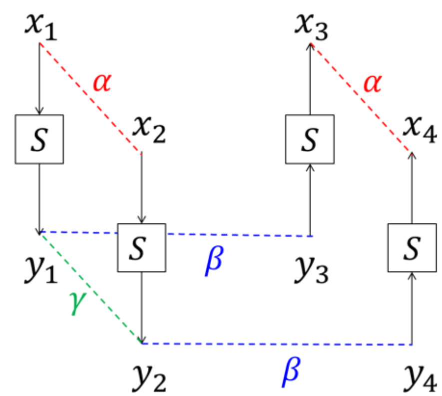
r for E_m with one S-box layer at the boundary of E_0 and E_1



$$\mathrm{BCT}(\alpha,\beta)=\sum_{\gamma}\#(\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\cap(\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\oplus\beta)).$$

$$r=\frac{\mathrm{BCT}(\alpha,\beta)}{2^n}=\sum_{\gamma}\frac{\mathrm{DDT}(\alpha,\gamma)}{2^n}\cdot\frac{\#\{y\in\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma):y\oplus\beta\in\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\}}{\#\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)}$$

New Explanation of BCT



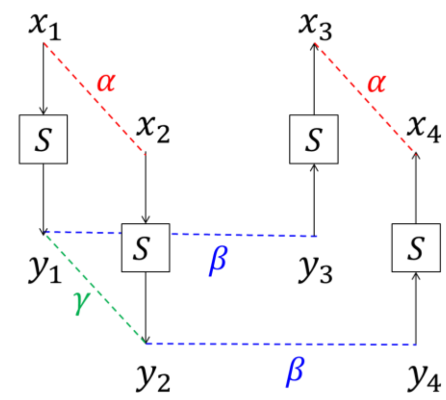
r for E_m with one S-box layer at the boundary of E_0 and E_1

$$r = \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} = \sum_{\gamma} \frac{\mathrm{DDT}(\alpha,\gamma)}{2^n} \cdot \frac{\#\{y \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) : y \oplus \beta \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\}}{\#\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)}$$

Similarly,

$$r = \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} = \sum_{\gamma'} \frac{\mathrm{DDT}(\gamma',\beta)}{2^n} \cdot \frac{\#\{x \in \mathcal{X}_{\mathrm{DDT}}(\gamma',\beta) : x \oplus \alpha \in \mathcal{X}_{\mathrm{DDT}}(\gamma',\beta)\}}{\#\mathcal{X}_{\mathrm{DDT}}(\gamma',\beta)}$$

New Explanation of BCT



r for E_m with one S-box layer at the boundary of E_0 and E_1

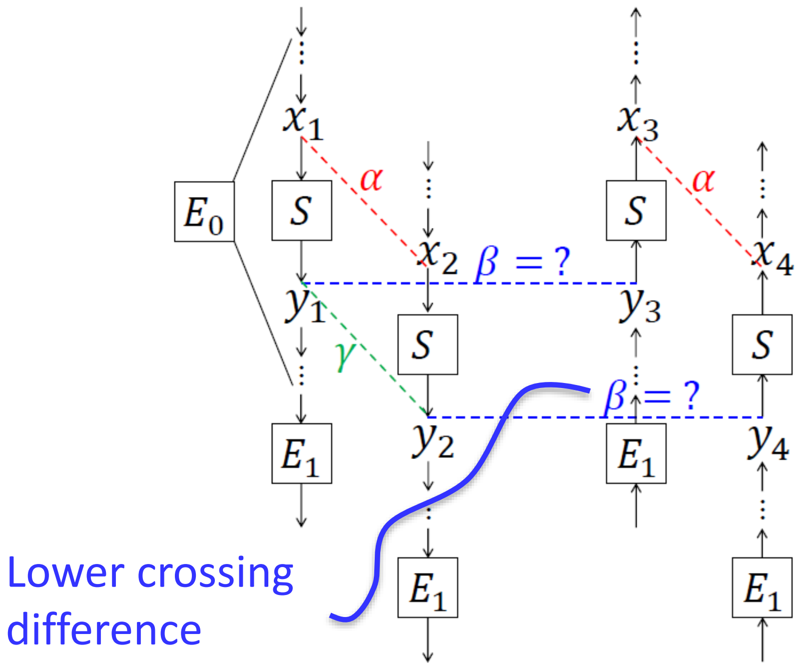
$$r = \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} = \sum_{\gamma} \frac{\mathrm{DDT}(\alpha,\gamma)}{2^n} \cdot \frac{\#\{y \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) : y \oplus \beta \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\}}{\#\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)}$$

Similarly,

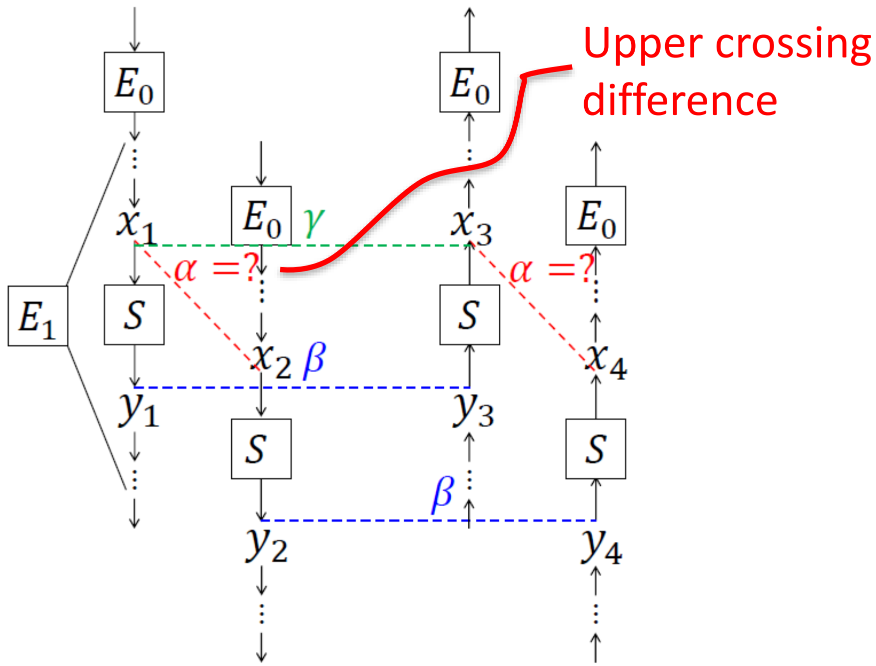
$$r = \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} = \sum_{\gamma'} \frac{\mathrm{DDT}(\gamma',\beta)}{2^n} \cdot \frac{\#\{x \in \mathcal{X}_{\mathrm{DDT}}(\gamma',\beta) : x \oplus \alpha \in \mathcal{X}_{\mathrm{DDT}}(\gamma',\beta)\}}{\#\mathcal{X}_{\mathrm{DDT}}(\gamma',\beta)}$$

In this case, α and β are regarded as fixed.

Generalization: S-box in E_0 or E_1

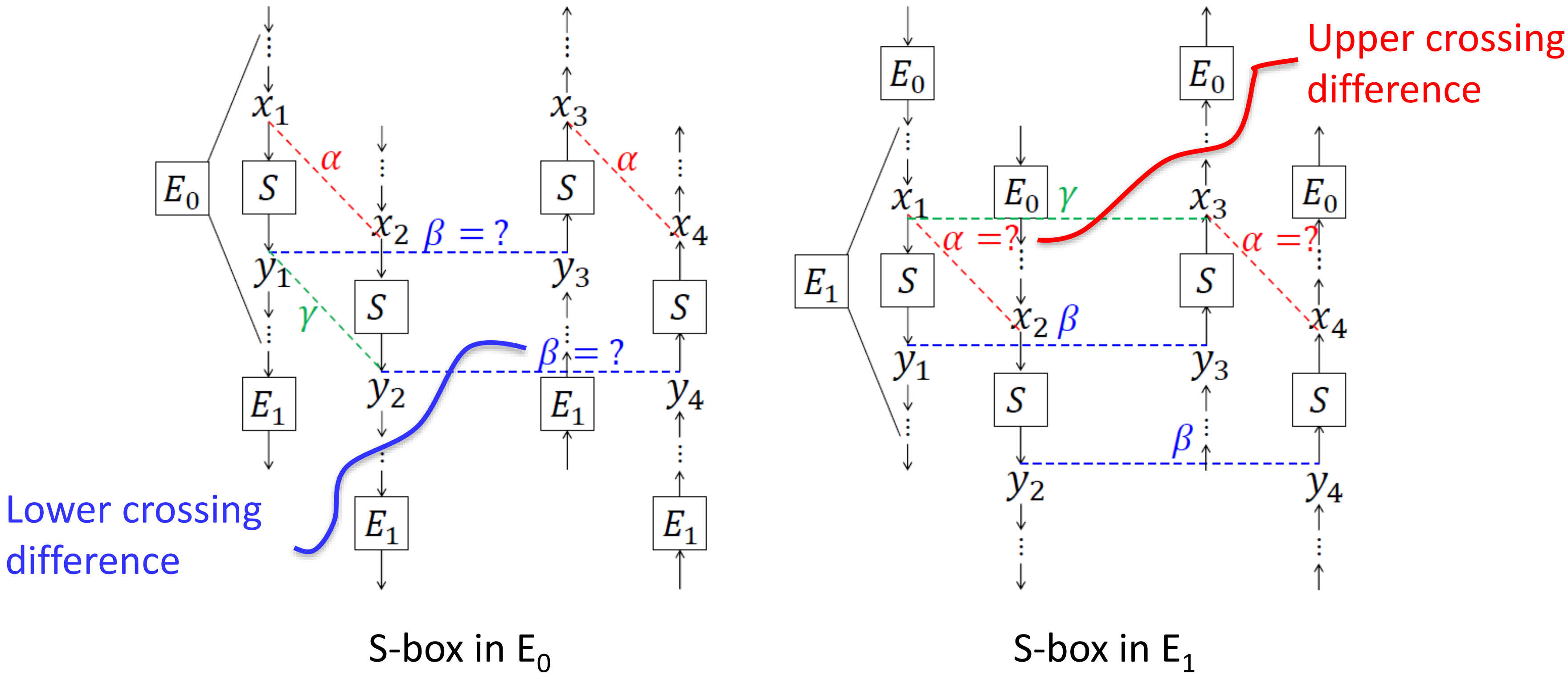


S-box in E_0



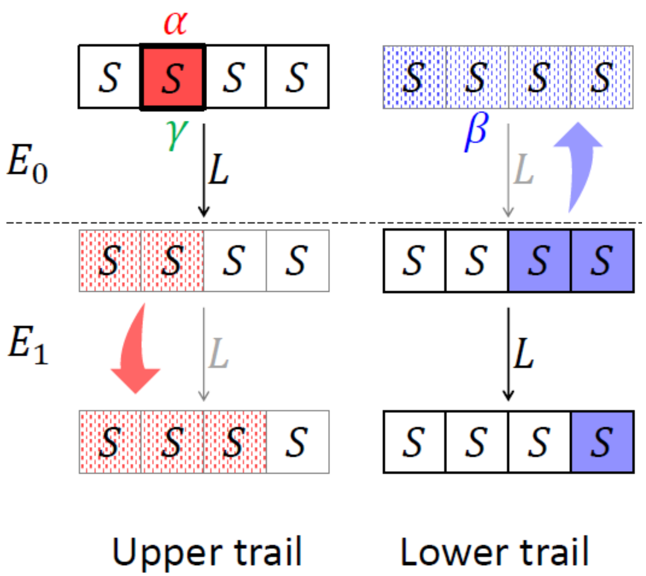
S-box in E_1

Generalization: S-box in E_0 or E_1



What if α or β (crossing differences) are not fixed?

Generalization: S-box in E_0

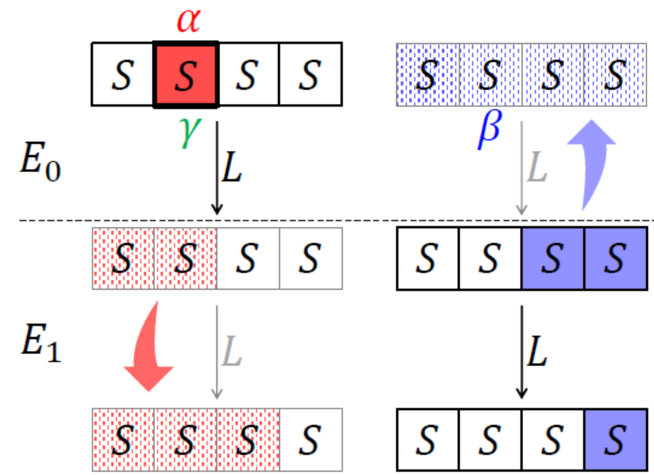


Generalization: S-box in E_0

(1) β is independent of the upper trail

$$\bar{r} = \frac{\mathrm{DDT}(\alpha,\gamma)}{2^n} \cdot \sum_{\beta} \frac{\#\{y \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) : y \oplus \beta \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\}}{\#\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)} \boxed{\cdot \Pr(y_1 \oplus y_3 = \beta).}$$

$$r = \sum_{\gamma} \bar{r} = \sum_{\beta} \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} \boxed{\cdot \Pr(y_1 \oplus y_3 = \beta)}$$



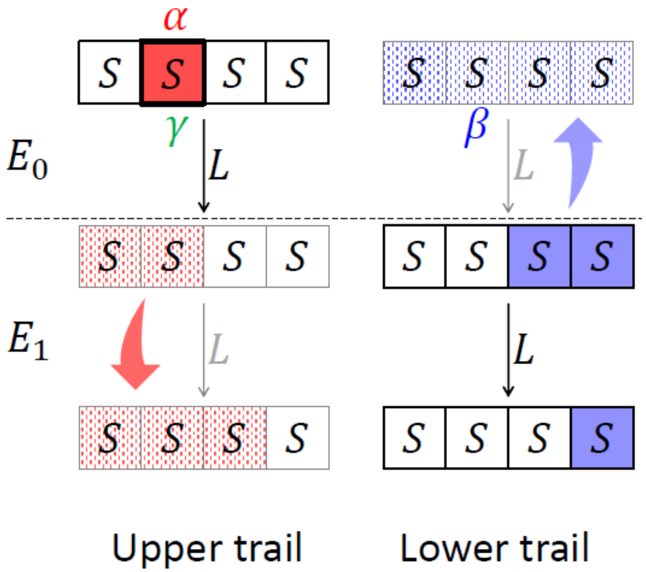
Upper trail Lower trail

Generalization: S-box in E_0

(1) β is independent of the upper trail

$$\bar{r} = \frac{\mathrm{DDT}(\alpha,\gamma)}{2^n} \cdot \sum_{\beta} \frac{\#\{y \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) : y \oplus \beta \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\}}{\#\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)} \boxed{\cdot \Pr(y_1 \oplus y_3 = \beta).}$$

$$r = \sum_{\gamma} \bar{r} = \sum_{\beta} \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} \boxed{\cdot \Pr(y_1 \oplus y_3 = \beta)}$$



(2) β is uniformly distributed

$$\bar{r} = \left(\frac{\mathrm{DDT}(\alpha,\gamma)}{2^n}\right)^2$$

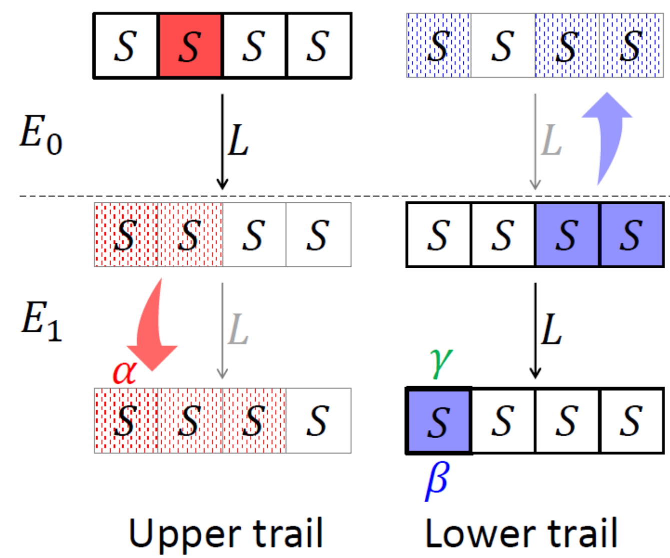
which becomes identical to p^2q^2 in the classical boomerang attack.

Generalization: S-box in E_1

(1) α is independent of the lower trail

$$\bar{r} = \frac{\mathrm{DDT}(\gamma,\beta)}{2^n} \cdot \sum_{\alpha} \frac{\#\{x \in \mathcal{X}_{\mathrm{DDT}}(\gamma,\beta) : x \oplus \alpha \in \mathcal{X}_{\mathrm{DDT}}(\gamma,\beta)\}}{\#\mathcal{X}_{\mathrm{DDT}}(\gamma,\beta)} \boxed{\cdot \Pr(x_1 \oplus x_2 = \alpha)}$$

$$r = \sum_{\gamma} \bar{r} = \sum_{\alpha} \frac{\mathrm{BCT}(\alpha,\beta)}{2^n} \boxed{\cdot \Pr(x_1 \oplus x_2 = \alpha)}$$

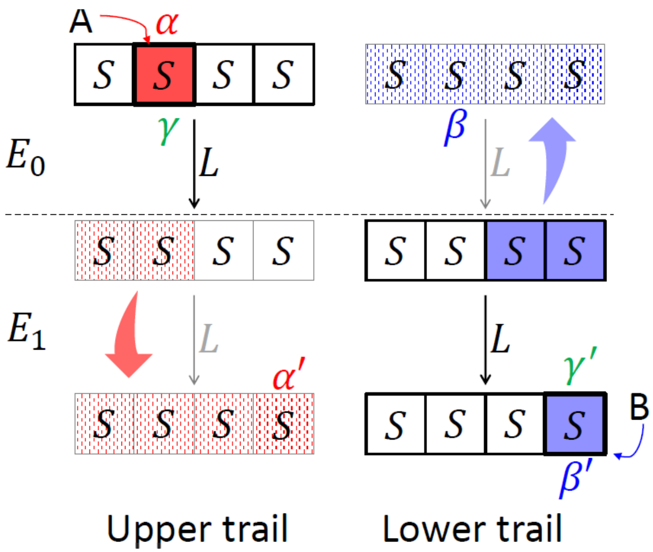


(2) α is uniformly distributed

$$\bar{r} = \left(\frac{\mathrm{DDT}(\gamma,\beta)}{2^n}\right)^2$$

which becomes identical to p^2q^2 in the classical boomerang attack.

Generalization: Interrelated S-boxes

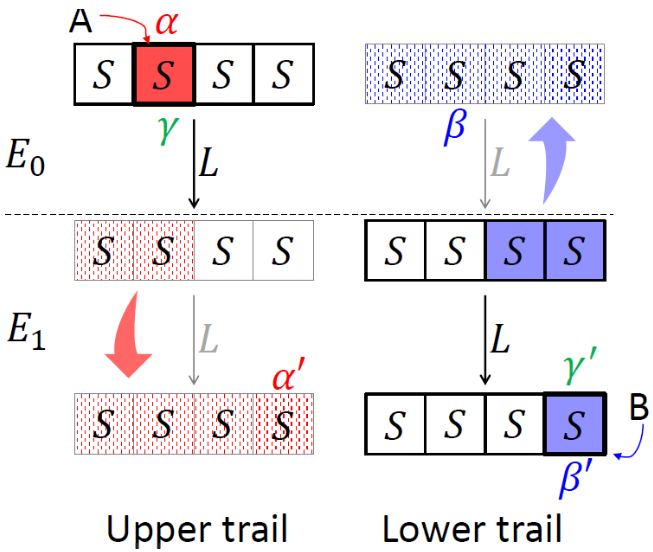


Lower crossing diff. (β) of A comes from B.

Upper crossing diff. (α') of B comes from A.

S-boxes A and B are interrelated.

Generalization: Interrelated S-boxes

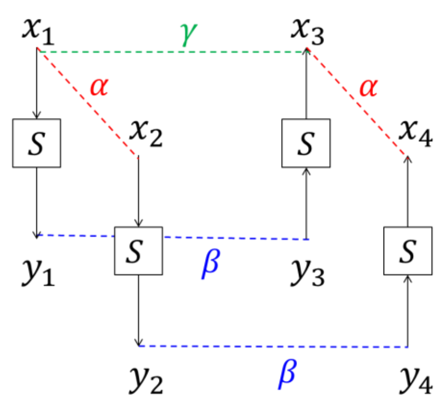


Lower crossing diff. (β) of A comes from B.

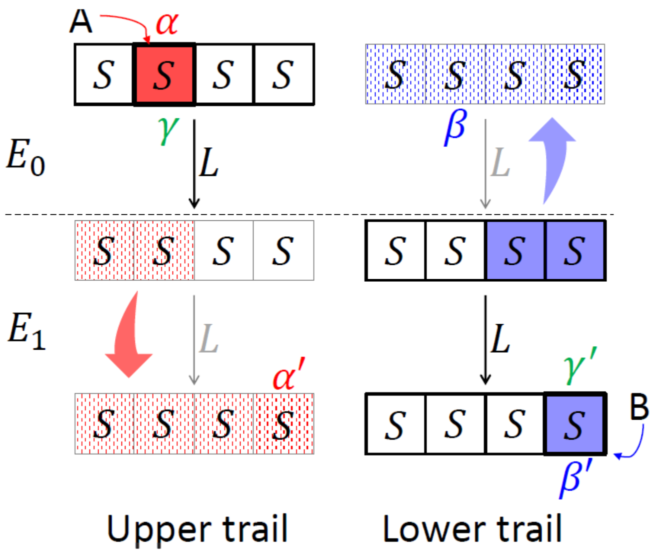
Upper crossing diff. (α') of B comes from A.

S-boxes A and B are interrelated.

$$\mathcal{D}_{\mathrm{BCT}}(\alpha,\beta,\gamma) \triangleq \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x)\oplus\beta)\oplus S^{-1}(S(x\oplus\alpha)\oplus\beta)=\alpha,$$
$$x \oplus S^{-1}(S(x)\oplus\beta)=\gamma\}.$$



Generalization: Interrelated S-boxes



Lower crossing diff. (β) of A comes from B.

Upper crossing diff. (α') of B comes from A.

S-boxes A and B are interrelated.

$$\mathcal{D}_{\mathrm{BCT}}(\alpha,\beta,\gamma) \triangleq \#\{x \in \mathbb{F}_2^n : S^{-1}(S(x)\oplus\beta)\oplus S^{-1}(S(x\oplus\alpha)\oplus\beta)=\alpha,$$
$$x \oplus S^{-1}(S(x)\oplus\beta)=\gamma\}.$$

$$\bar{r} = \sum_{\alpha'} \frac{\mathrm{DDT}(\alpha,\gamma)}{2^n} \cdot \Pr(\gamma\to\alpha') \frac{\mathcal{D}_{\mathrm{BCT}}(\alpha',\beta',\gamma')}{2^n} \cdot \Pr(\gamma'\to\beta) \cdot \qquad r = \sum_{\gamma}\sum_{\gamma'} \bar{r}.$$

$$\frac{\#\{y \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma) : y\oplus\beta \in \mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)\}}{\#\mathcal{Y}_{\mathrm{DDT}}(\alpha,\gamma)}.$$

Generalized Framework of BCT

1. Initialization: $E_m \leftarrow E_1^{first} || E_0^{last}$.
2. Extend both trails: $\left(\alpha \overset{E_0}{\rightarrow} \beta\right) \xrightarrow[\Pr = 1]{E_1}$, $\xleftarrow[\Pr = 1]{E_0} (\gamma \overset{E_1}{\leftarrow} \delta)$.
3. Prepend E_m with one more round
   a) If the lower crossing differences are distributed uni formly, peel off the first round and go to Step 4.
   b) Go to Step 3
4. Append E_m with one more round
   a) If the upper crossing differences are distributed uni formly, peel off the last round and go to Step 5.
   b) Go to Step 4.
5. Calculate r using formulas in the previous slides

Boundaries of E_m: where crossing differences are distr ibuted (almost) uniformly.

Applications

Re-evaluate prob of four BM dist. of SKINNY

- Prev: prob evaluated by $\hat{p}^2\hat{q}^2$
- New: prob evaluated by the generalized BCT

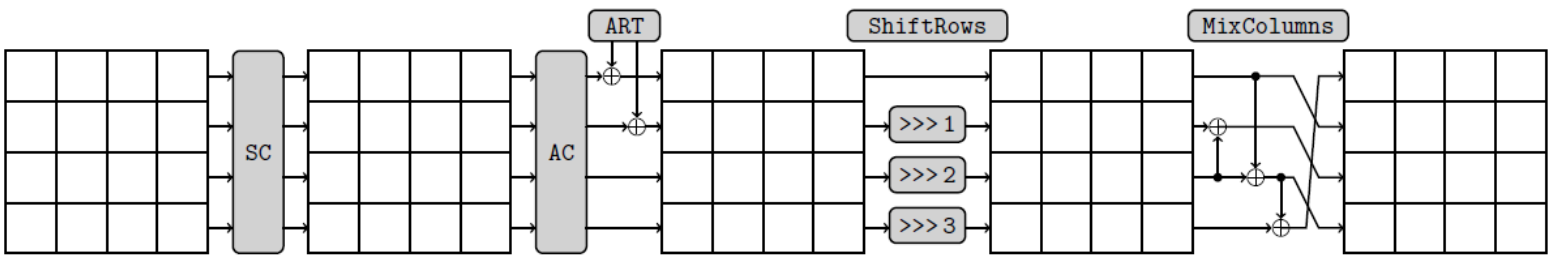
Construct related-subkey BM dist. Of AES-128

- Prev: related-subkey BM dist. Of AES-192/256
- New: 6-round related-subkey BM dist. Of AES-128 with $2^{-109.42}$

SKINNY

SKINNY [BJK+16] is an SPN cipher, with a linear key schedule.

- SKINNY-n-t where n is block size and t tweakey size



Example E_m of SKINNY-64-128 in the related-tweakey setting

- Upper trail: 2 rounds, 2^{-8}
- Lower trail: 4 rounds, 2^{-14}
- $p^2q^2 = 2^{-44}$

E_m with 6 Middle Rounds

Rd	Diff before and after SB	ΔK	∇K	Pr.
R1	0,0,0,0, 0,0,0,0, 0,0,0,b, 0,0,0,0 0,0,0,0, 0,0,0,0, 0,0,0,1, 0,0,0,0	0,0,0,0, 0,0,0,0	b,0,0,0, 0,0,0,0	2^{-2}
R2	0,1,0,0, 0,0,0,0, 0,1,0,0, 0,1,0,0 0,8,0,0, 0,0,0,0, 0,8,0,0, 0,8,0,0	0,0,0,0, 0,c,0,0	0,0,0,0, 5,0,0,0	2^{-2*3}
R3	0,0,0,0, 0,0,0,0, 0,0,0,0, 0,0,0,2 0,0,0,0, 0,0,0,0, 0,0,0,0, 0,0,0,3	0,0,0,0, 0,0,0,0	0,0,3,0, 0,0,0,0	2^{-2}
R4	0,0,0,0, 0,0,3,0, 0,0,0,0, 0,0,3,0 0,0,0,0, 0,0,d,0, 0,0,0,0, 0,0,c,0	0,0,0,3, 0,0,0,0	0,0,0,0, 0,0,9,0	2^{-3*2}
R5	0,c,0,0, 0,0,0,0, 0,0,0,4, 0,0,0,0 0,2,0,0, 0,0,0,0, 0,0,0,2, 0,0,0,0	0,0,0,0, 0,0,0,0	0,0,0,0, 2,0,0,0	2^{-2*2}
R6	0,0,0,0, 0,2,0,0, 0,0,0,0, 0,0,0,0 0,0,0,0, 0,1,0,0, 0,0,0,0, 0,0,0,0	0,0,0,0, 0,0,0,d	0,0,0,0, 0,1,0,0	2^{-2}

Evaluation of r

Rounds	p^2q^2	$\hat{p}^2\hat{q}^2$	r (new)
1+1	2^{-16}	$2^{-8.41}$	2^{-2}
2+1	2^{-20}	...	$2^{-2.79}$
2+2	2^{-32}	...	$2^{-5.69}$
2+3	2^{-40}	...	$2^{-10.56}$
2+4	2^{-44}	$2^{-29.91}$	$2^{-12.96}$

Experiments confirm the results of r.

Summary of the results on SKINNY

Prob. of BM dist. and comparison

Ver.	n	E_m		$E = \widetilde{E}_1 \circ E_m \circ \widetilde{E}_0$		
		$\lvert E_m \rvert$	r	$\lvert E \rvert$	$\tilde{p}^2\tilde{q}^2 r$	$\hat{p}^2\hat{q}^2$[LGS17]
n-2n	64	6(13)	$2^{-12.96}$	17	$2^{-29.78}$	$2^{-48.72}$
	128	5(12)	$2^{-11.45}$	18	$2^{-77.83}$	$2^{-103.84}$
n-3n	64	5(17)	$2^{-10.50}$	22	$2^{-42.98}$	$2^{-54.94}$
	128	5(17)	$2^{-9.88}$	22	$2^{-48.30}$	$2^{-76.84}$

- Take seconds to calculate r

Summary of the results on SKINNY

Prob. of BM dist. and comparison

Ver.	n	E_m		$E = \widetilde{E}_1 \circ E_m \circ \widetilde{E}_0$		
		$\|E_m\|$	r	$\|E\|$	$\tilde{p}^2\tilde{q}^2 r$	$\hat{p}^2\hat{q}^2$[LGS17]
n-2n	64	6(13)	$2^{-12.96}$	17	$2^{-29.78}$	$2^{-48.72}$
	128	5(12)	$2^{-11.45}$	18	$2^{-77.83}$	$2^{-103.84}$
n-3n	64	5(17)	$2^{-10.50}$	22	$2^{-42.98}$	$2^{-54.94}$
	128	5(17)	$2^{-9.88}$	22	$2^{-48.30}$	$2^{-76.84}$

- Take seconds to calculate r
- Experiments confirm the results of r and the 17-round dist. of SKINNY-64-128

6-round related-subkey BM dist. Of AES-128

3-round related-key differential trails:

- 2 trails, 5 active S-boxes, 2^{-31}
- 18 trails, 6 active S-boxes, $2^{-36}, 2^{-37}, 2^{-38}$

	Round	Before AK	Subkey diff.	Before SB	After SB	After SR	p_r
2^{-31}	R1	8c 1f 8c 00 01 99 01 00 8d 00 8d c2 37 00 8d 00	8c 00 8c 00 01 00 01 00 8d 00 8d 00 8d 00 8d 00	00 1f 00 00 00 99 00 00 00 00 00 c2 ba 00 00 00	00 a3 00 00 00 8d 00 00 00 00 00 46 97 00 00 00	00 a3 00 00 8d 00 00 00 00 46 00 00 00 97 00 00	$(2^{-6})^8$
	R2	8c 8c 00 00 01 fe 00 00 8d 8d 00 00 8d 8d 00 00	8c 8c 00 00 01 01 00 00 8d 8d 00 00 8d 8d 00 00	00 00 00 00 00 ed 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 8d 00 00 00 00 00 00 00 00 00 00	00 00 00 00 8d 00 00 00 00 00 00 00 00 00 00 00	$(2^{-7})^2$
	R3	8c 00 00 00 01 00 00 00 8d 00 00 00 8d 00 00 00	8c 00 00 00 01 00 00 00 8d 00 00 00 8d 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1
	R4	0a 87 0a 00 0c bc f6 00 06 00 06 fb 23 00 06 00	0a 00 0a 00 0c 00 0c 00 06 00 06 00 06 00 06 00	00 87 00 00 00 bc fa 00 00 00 00 fb 19 00 00 00	00 74 00 00 00 06 4e 00 00 00 00 6c 5c 00 00 00	00 74 00 00 06 4e 00 00 00 6c 00 00 00 5c 00 00	$2^{-33.42}$
2^{-37}	R5	0a 0a 00 00 0c 00 00 00 06 06 00 00 06 06 00 00	0a 0a 00 00 0c 0c 00 00 06 06 00 00 06 06 00 00	00 00 00 00 00 0c 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 00	00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00	$(2^{-7})^2$
	R6	0a 00 00 00 0c 00 00 00 06 00 00 00 06 00 00 00	0a 00 00 00 0c 00 00 00 06 00 00 00 06 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	1

$$\left.\begin{matrix}\text{R3}\\\text{R4}\end{matrix}\right\} \quad E_m, r = 2^{-33.42}$$

$$\tilde{p}^2\tilde{q}^2 r = 2^{-109.42}$$

Discussion

Length of E_m:

- Mainly determined by the diffusion effect of the linear la yer
- Density of active cells of the trails

r:

Strongly affected by the DDT and BCT of the S-box

Limitation of the generalized BCT:

For a long E_m with large and strong S-boxes, calculating r mig ht be a time-consuming task, e.g., $T>2^{35}$.

Concluding Remarks

Generalized BCT: for calculating r in the sandwich attack

1: identify the boundaries of dependency

2: calculate r

Problems to investigate:

– Extension to non S-box based ciphers

– Improving previous boomerang attacks

Thank you for your attention!!

Slides credit to Yu Sasaki