NTT

Innovative R&D by NTT

Boomerang Connectivity Table: A New Cryptanalysis Tool

Carlos Cid[1], Tao Huang[2], Thomas Peyrin[2],
Yu Sasaki[3] and Ling Song[2,4]

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

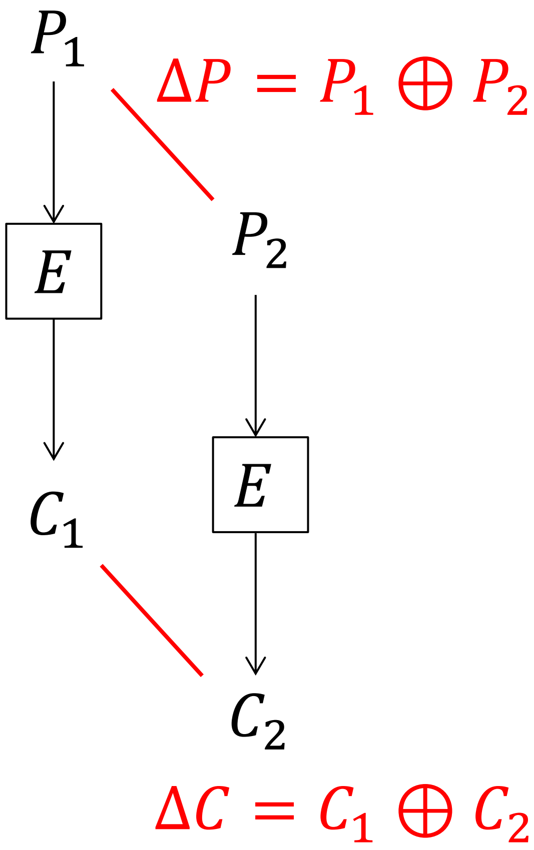
02 May 2018 Eurocrypt @ Tel Aviv

Differential Cryptanalysis

[Biham-Shamir1990]

- Prepare two input values P_1, P_2 with (usually) small difference $\Delta P = P_1 \oplus P_2$.
- Expecting some output differences $\Delta C = C_1 \oplus C_2$ with a high probability.

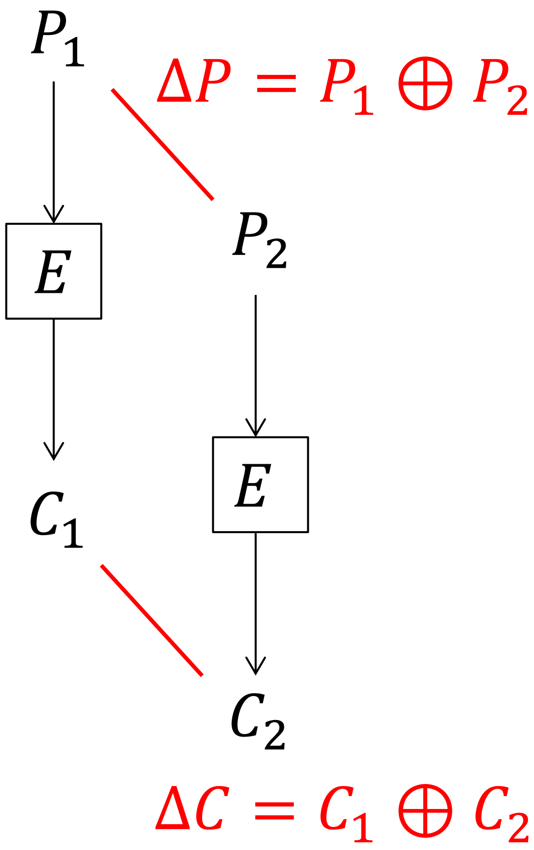
Solid methods to evaluate probability are evaluated.



Differential Cryptanalysis

[Biham-Shamir1990]

- Prepare two input values P_1, P_2 with (usually) small difference $\Delta P = P_1 \oplus P_2$.
- Expecting some output differences $\Delta C = C_1 \oplus C_2$ with a high probability.



Solid methods to evaluate probability are evaluated.

Boomerang Attacks

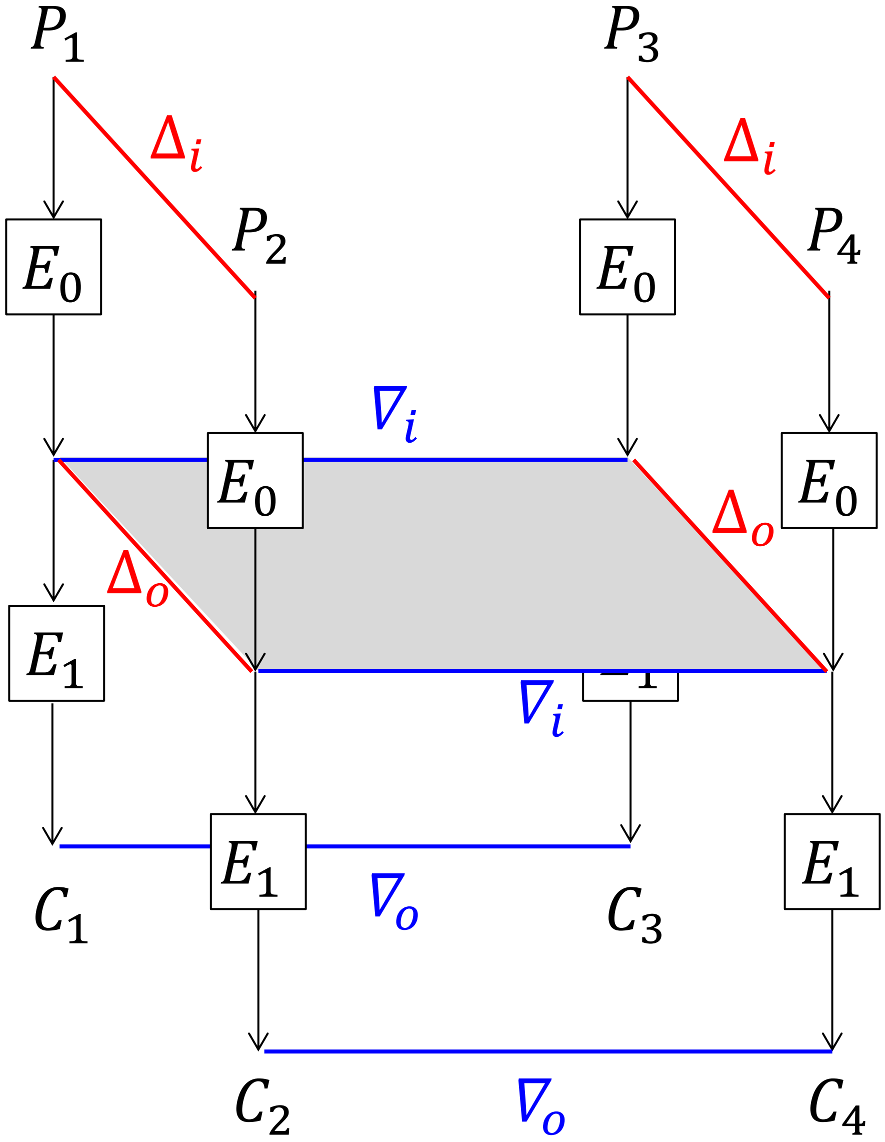
Proposed by [Wag99] to combine independent two characteristics.

- $E_0 : \Pr[\Delta_i \rightarrow \Delta_o] = p$
- $E_1 : \Pr[\nabla_i \rightarrow \nabla_o] = q$

Two pairs are analyzed.

Distinguish probability:

$$p^2 q^2$$



Two Trails in Boomerang Attacks

[Wag99]: Assumed two trails are independent.

→ not always correct

- Dependency can help attackers.

[BDD03]: Middle-round S-box trick

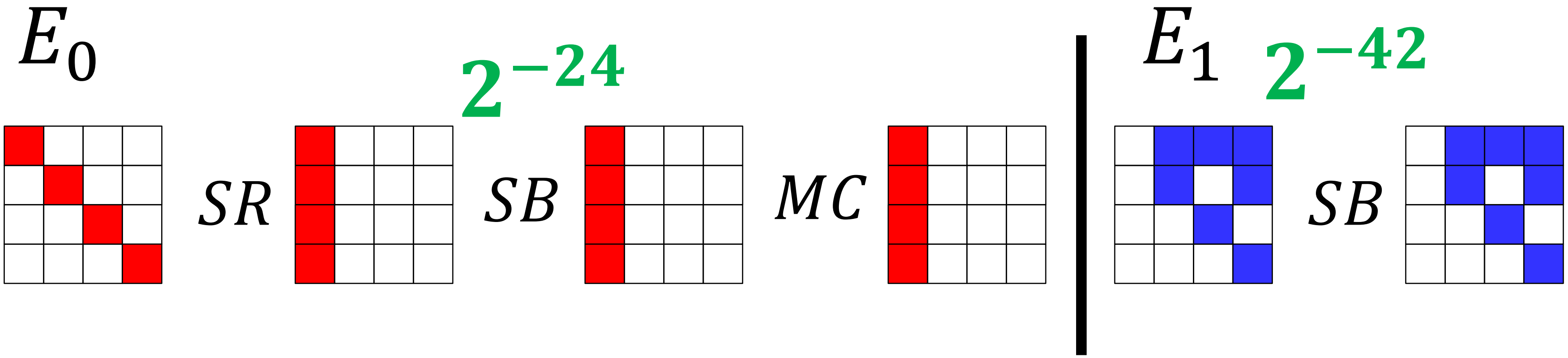
[BK09]: Boomerang switch

Ladder switch / Feistel switch / S-box switch

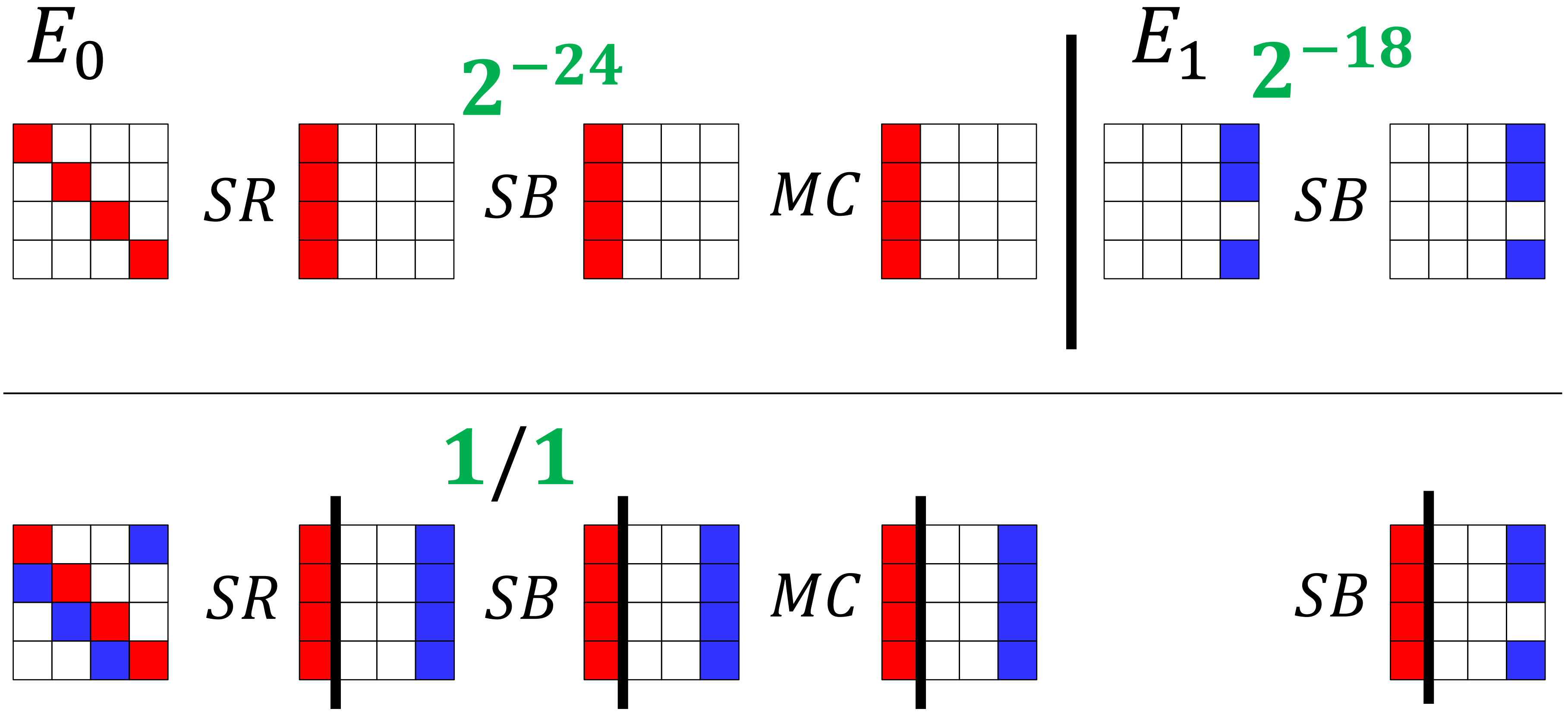
- Dependency can spoil attacks.

[Mer09]: Incompatible trails

Ladder Switch



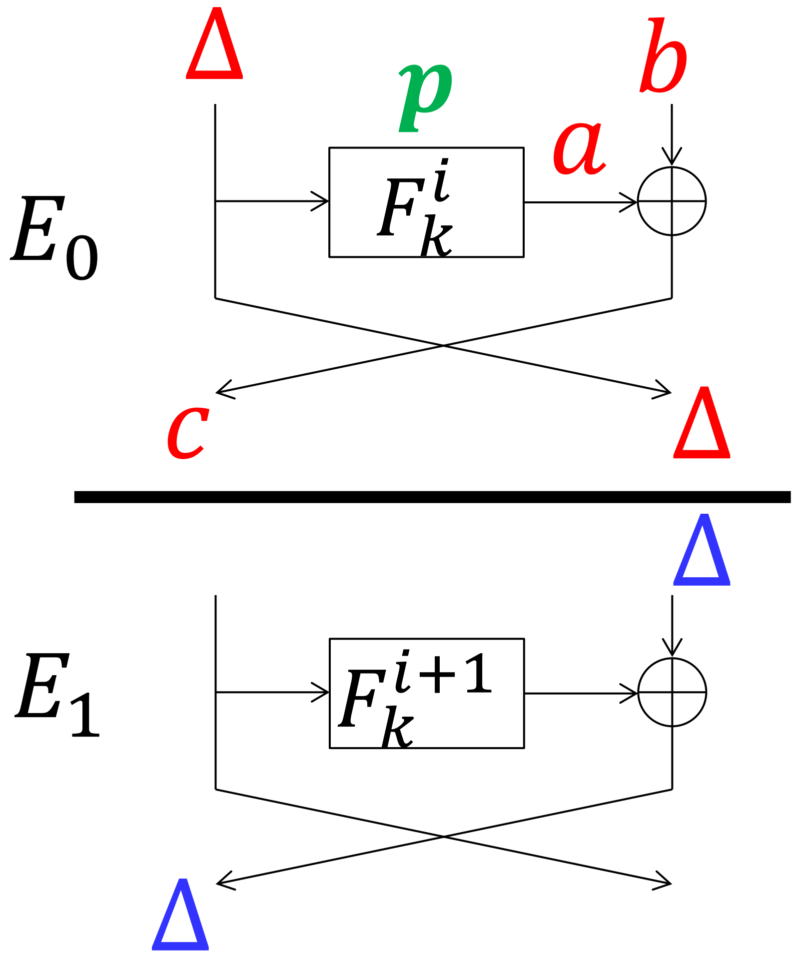
Ladder Switch



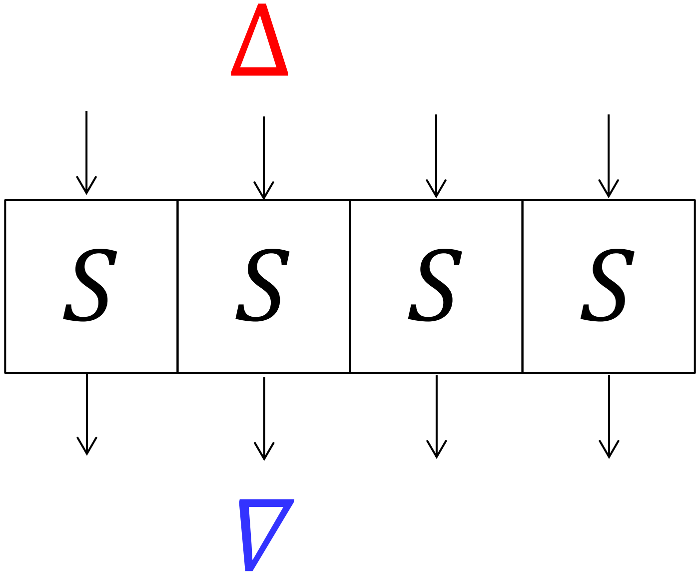
E_0: Columns 3: no active S-box for E_0

E_1: Columns 0: no active S-box for E_1

Feistel Switch / S-box Switch



$$\Pr[\Delta \xrightarrow{S} \nabla] = p$$



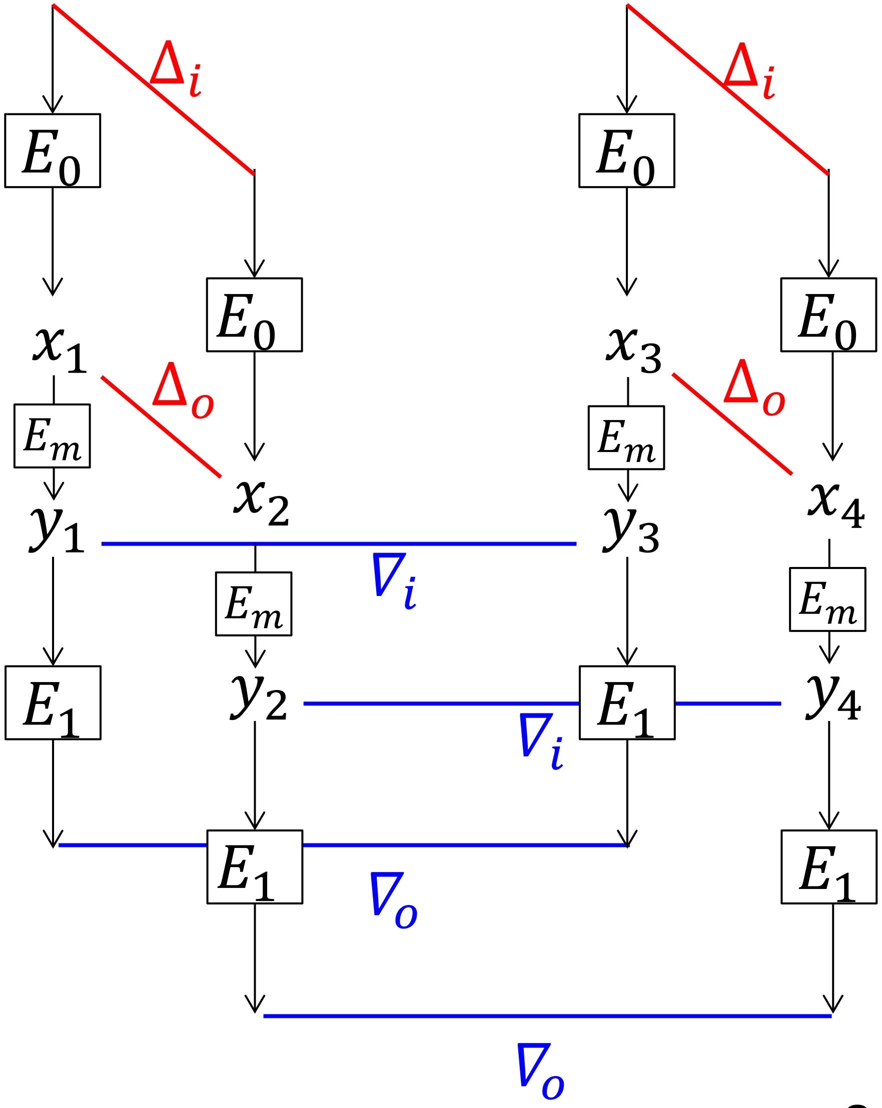
prob to be a right quartet is p (not p^2)

Sandwich Attacks [DKS10]

Generalized framework including dependency of two trails:

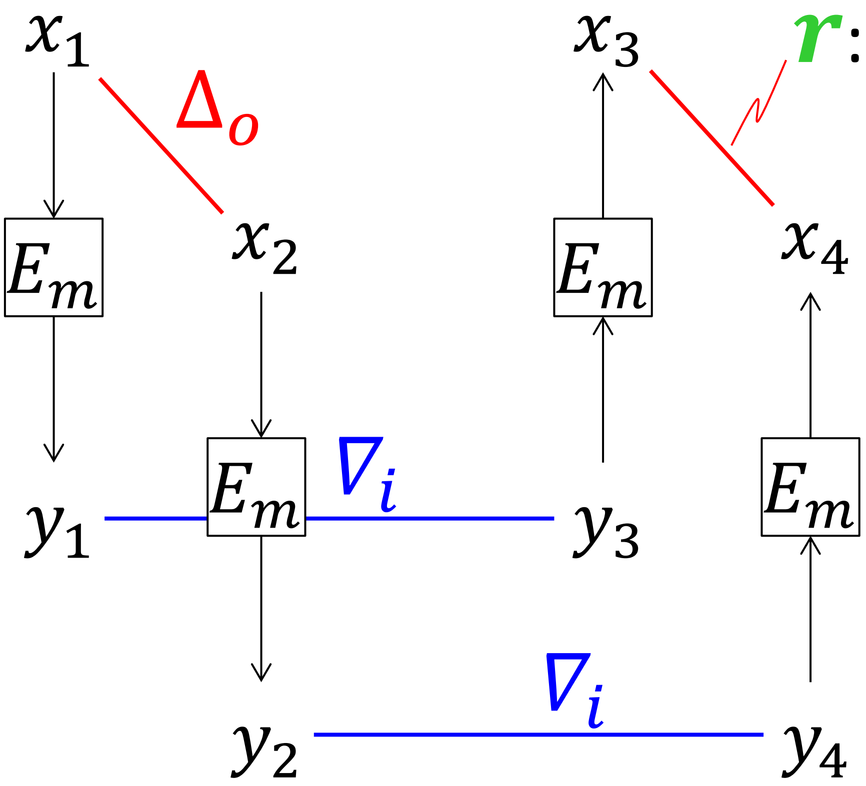
$$E = E_1 \circ E_m \circ E_0$$

Distinguish probability is $\boldsymbol{p^2q^2r}$, with some probability $\boldsymbol{r}$ for E_m.



Probability for E_m

$$r = \frac{\#\{x \in \{0,1\}^n \mid E_m^{-1}(E_m(x) \oplus \nabla_i) \oplus E_m^{-1}(E_m(x \oplus \Delta_o) \oplus \nabla_i) = \Delta_o\}}{2^n}$$

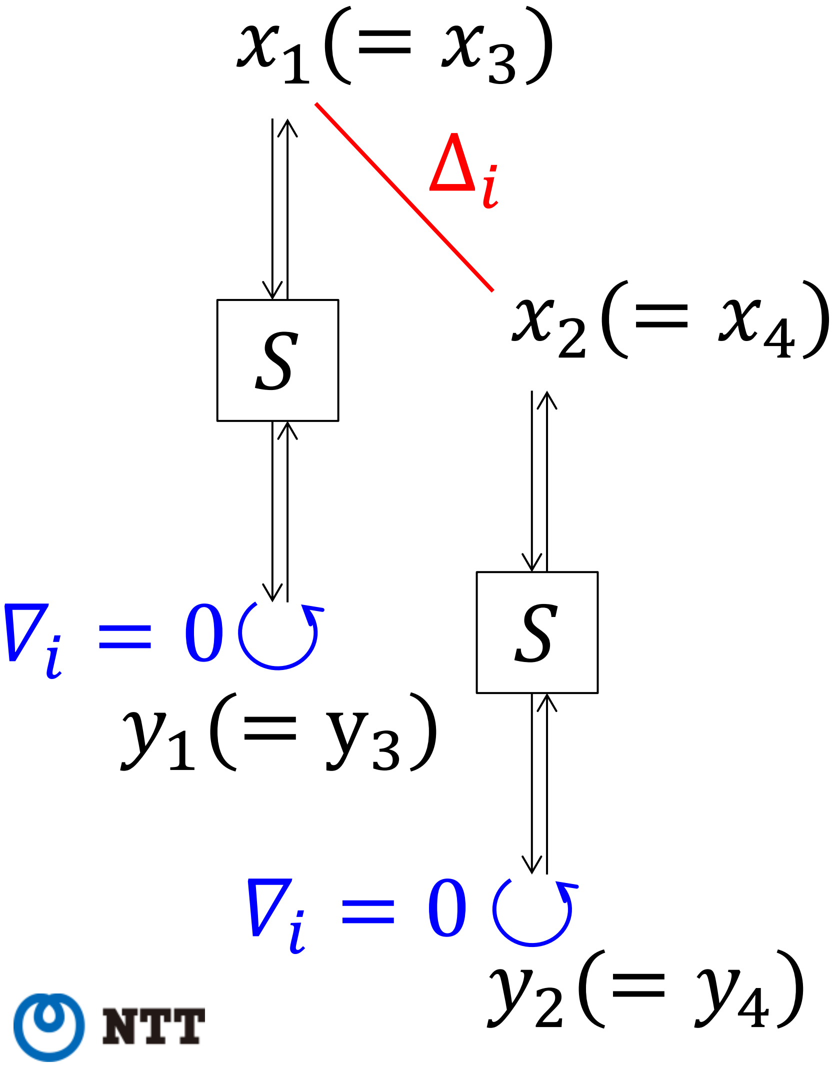


r: prob of being Δ_o

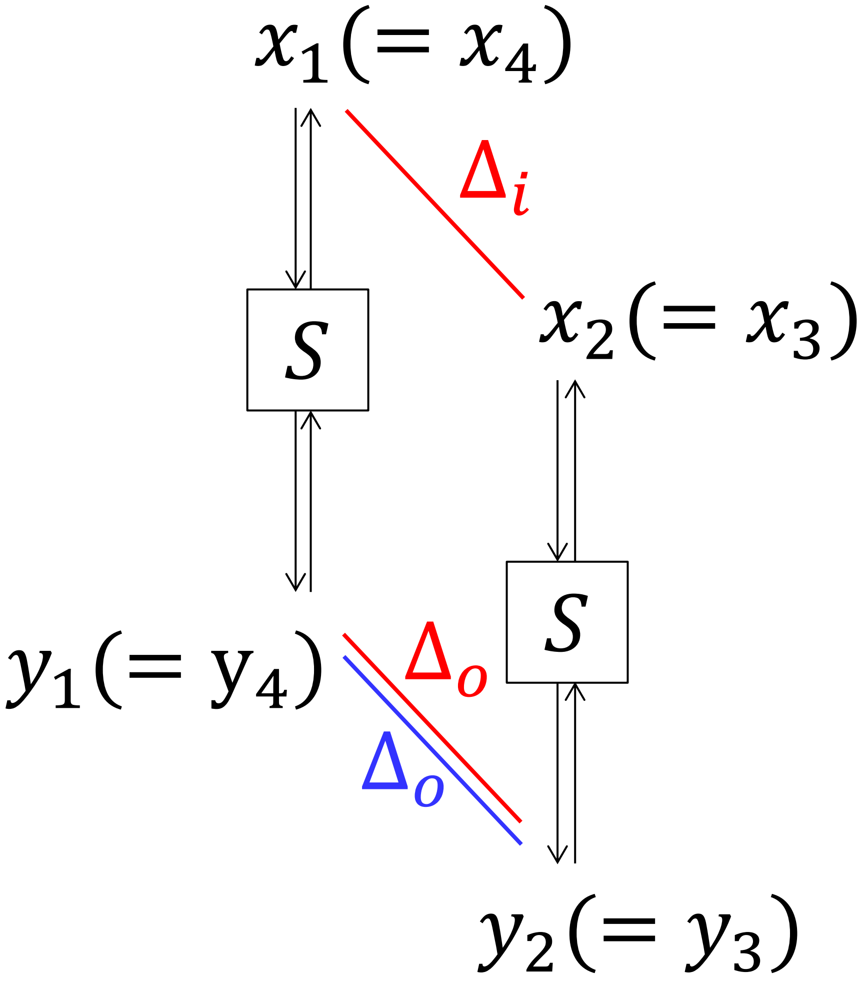
Probability space is only the size of E_m, not its square.

View of Boomerang Switch in Sandwich Attack

Ladder Switch $r = 1$



S-box Switch $r = p$



Our Goal

- r is for a quartet, not for a pair in the standard differential cryptanalysis. How to evaluate it?

- Our focus: E_m is a single S-box layer

- a new form to easily evaluate r for S-box

  Adv. 1: new switching effect (r is surprisingly high)

  Adv. 2: quantitating the strength of S-box against sandwich attack (a new S-box design criterion)

- We reveal several relationships between the standard probability in DDT and r.

DDT: Differential Distribution Table

$$\#\{x \in \{0,1\}^n | S(x) \oplus S(x \oplus \Delta_i) = \Delta_o\}$$

Δ_o

		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	4	0	0	0	4	0	4	0	0	0	4	0	0
	2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
	3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
	4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
	5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
	6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
Δ_i	7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
	8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
	9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
	a	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
	b	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
	c	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
	d	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
	e	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
	f	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

PRESENT
S-box

BCT: Boomerang Connectivity Table

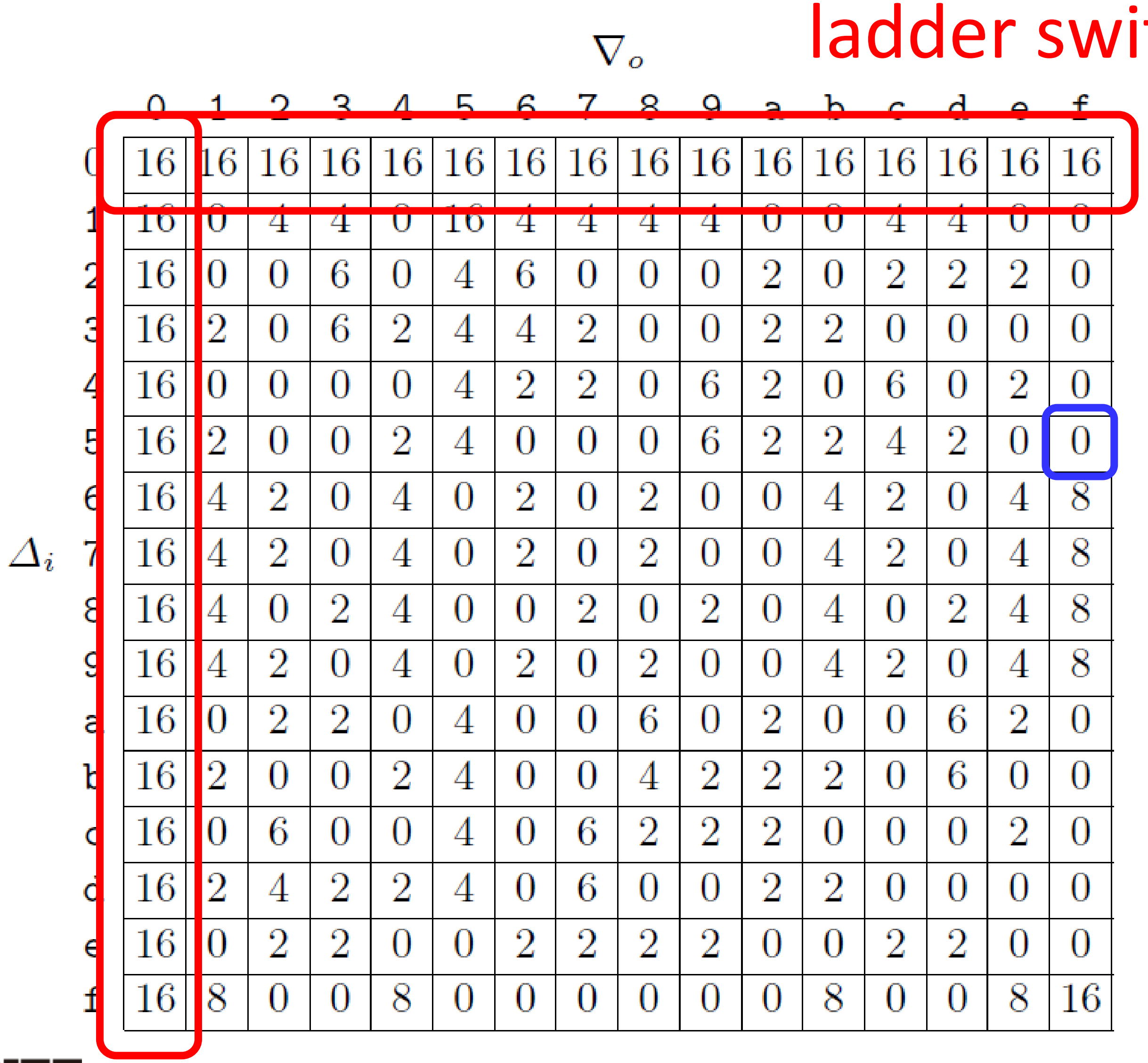
$$\#\{x \in \{0,1\}^n | S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i\}$$

∇_o

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

PRESENT
S-box

Observations of BCT (1/3)



ladder switch

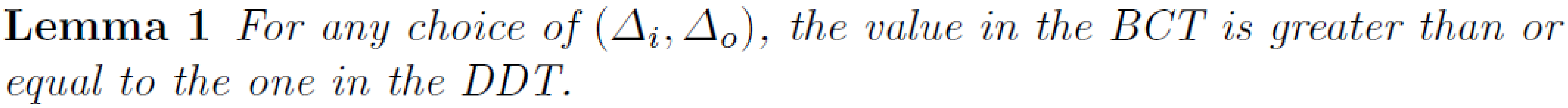
incompatibility [Mur09]

∇_o

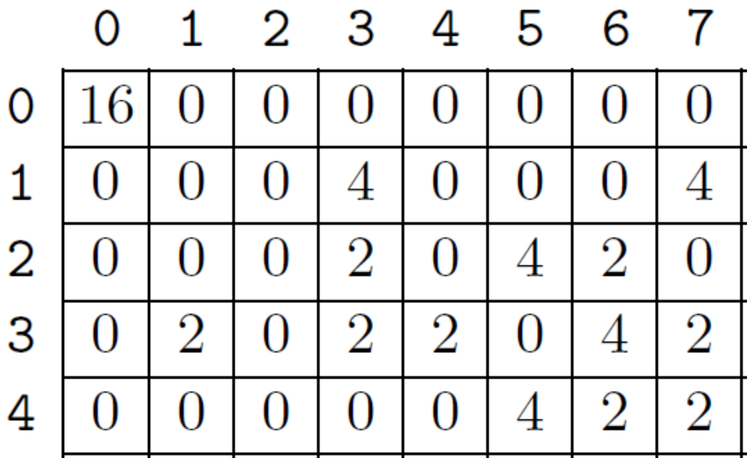
Δ_i	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	0	4	4	0	16	4	4	4	4	0	0	4	4	0	0
2	16	0	0	6	0	4	6	0	0	0	2	0	2	2	2	0
3	16	2	0	6	2	4	4	2	0	0	2	2	0	0	0	0
4	16	0	0	0	0	4	2	2	0	6	2	0	6	0	2	0
5	16	2	0	0	2	4	0	0	0	6	2	2	4	2	0	0
6	16	4	2	0	4	0	2	0	2	0	0	4	2	0	4	8
7	16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

Observations of BCT (2/3)

S-box Switch: $\text{"}\Pr[\Delta \xrightarrow{S} \nabla] = \boldsymbol{p}\text{"} \Rightarrow \text{"}\boldsymbol{r} = \boldsymbol{p}\text{"}$

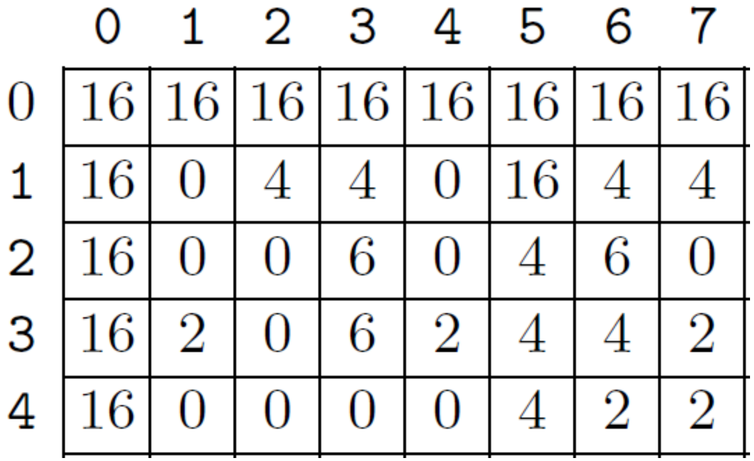


Lemma 1 *For any choice of (Δ_i, Δ_o), the value in the BCT is greater than or equal to the one in the DDT.*



	0	1	2	3	4	5	6	7
0	16	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4
2	0	0	0	2	0	4	2	0
3	0	2	0	2	2	0	4	2
4	0	0	0	0	0	4	2	2

DDT



	0	1	2	3	4	5	6	7
0	16	16	16	16	16	16	16	16
1	16	0	4	4	0	16	4	4
2	16	0	0	6	0	4	6	0
3	16	2	0	6	2	4	4	2
4	16	0	0	0	0	4	2	2

BCT

S-box switch is the equal case of Lem. 1

Observations of BCT (3/3)

Values in BCT can be bigger than DDT.

	0	1	2	3	4	5	6	7
0	16	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4
2	0	0	0	2	0	4	2	0
3	0	2	0	2	2	0	4	2
4	0	0	0	0	0	4	2	2

DDT

	0	1	2	3	4	5	6	7
0	16	16	16	16	16	16	16	16
1	16	0	4	4	0	16	4	4
2	16	0	0	6	0	4	6	0
3	16	2	0	6	2	4	4	2
4	16	0	0	0	0	4	2	2

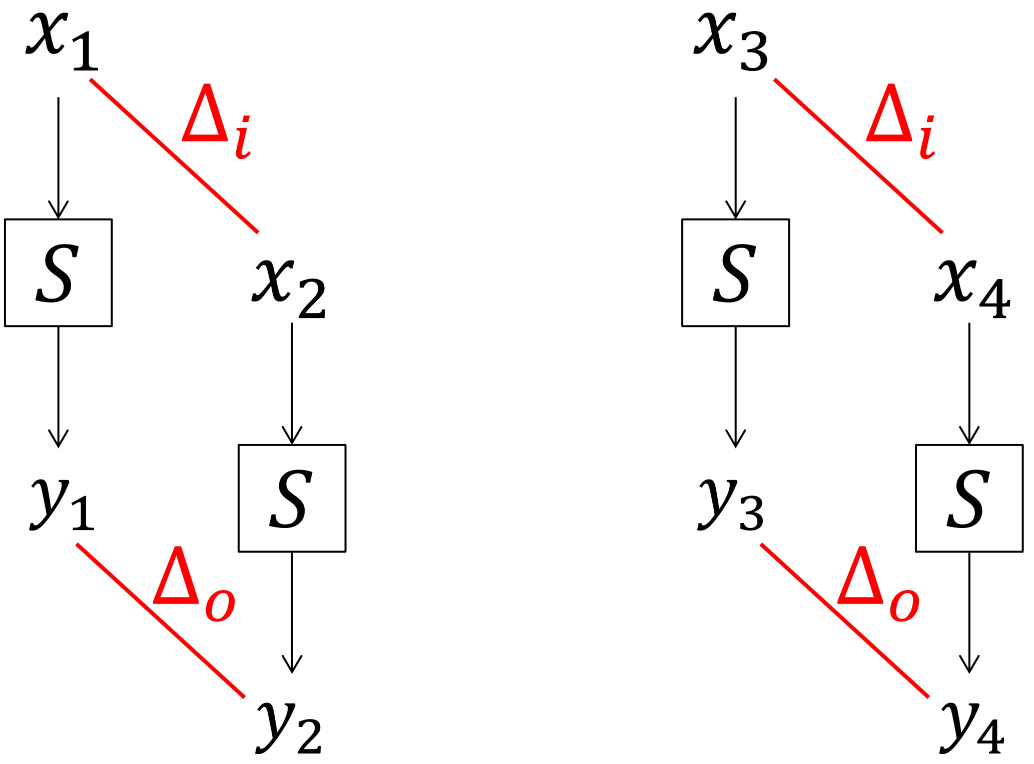
BCT

Comparison of DDT and BCT for AES S-box

Value	256	6	4	2	0
DDT	1	-	255	32130	33150
BCT	511	510	255	31620	32640

Generalized Switching Effect

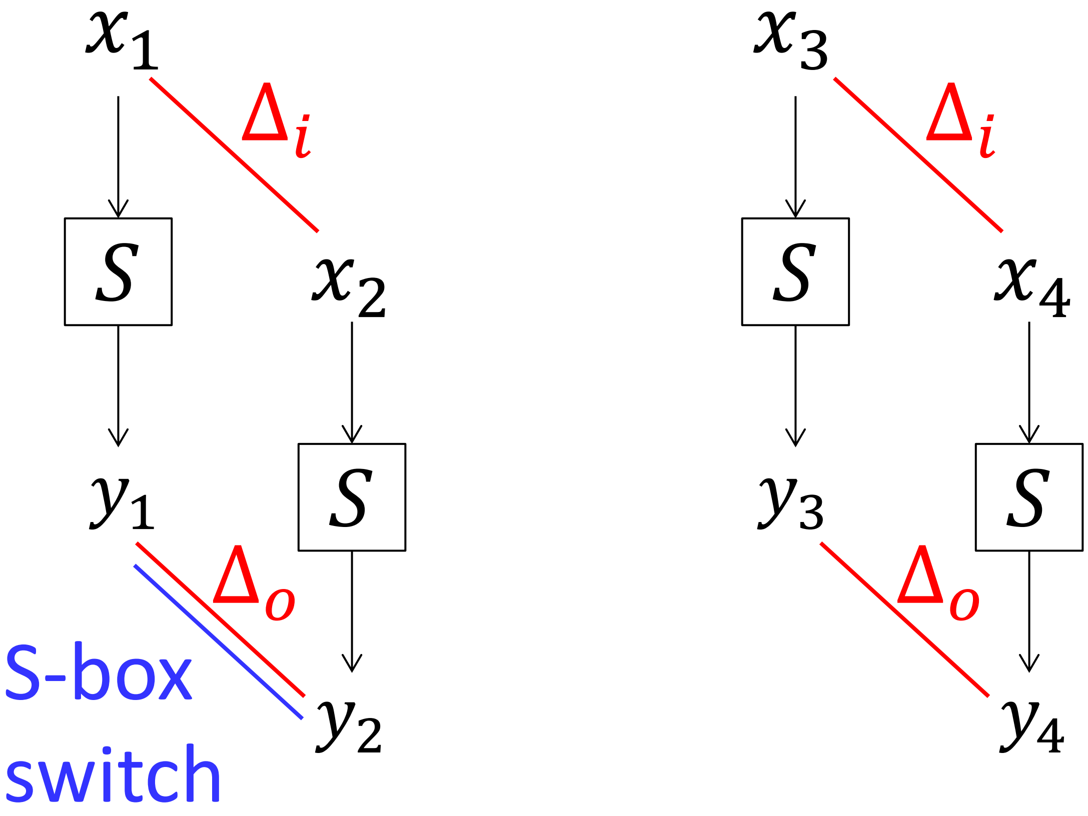
- Focus on (Δ_i, Δ_o) whose DDT entry is 4.
- 2 pairs satisfying those diff propagation



How can we define ∇ s.t. a quartet is formed?

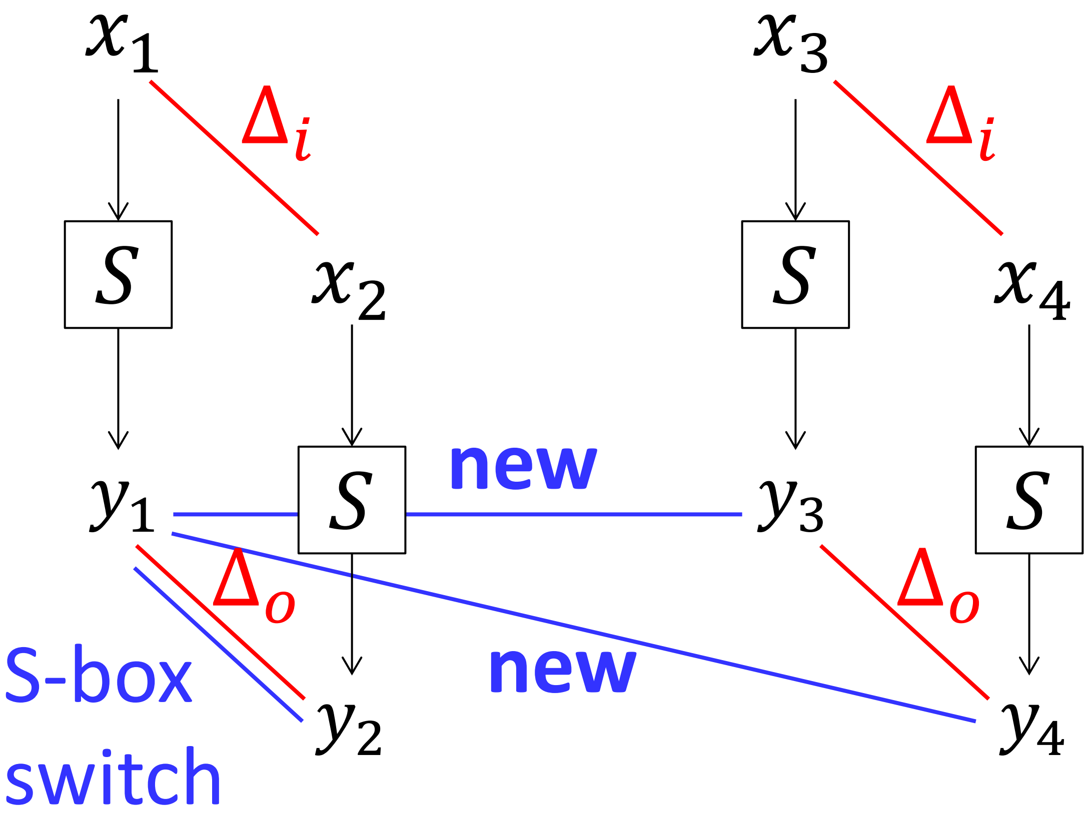
Generalized Switching Effect

- 3 ways to define ∇, one is known as S-box switch



Generalized Switching Effect

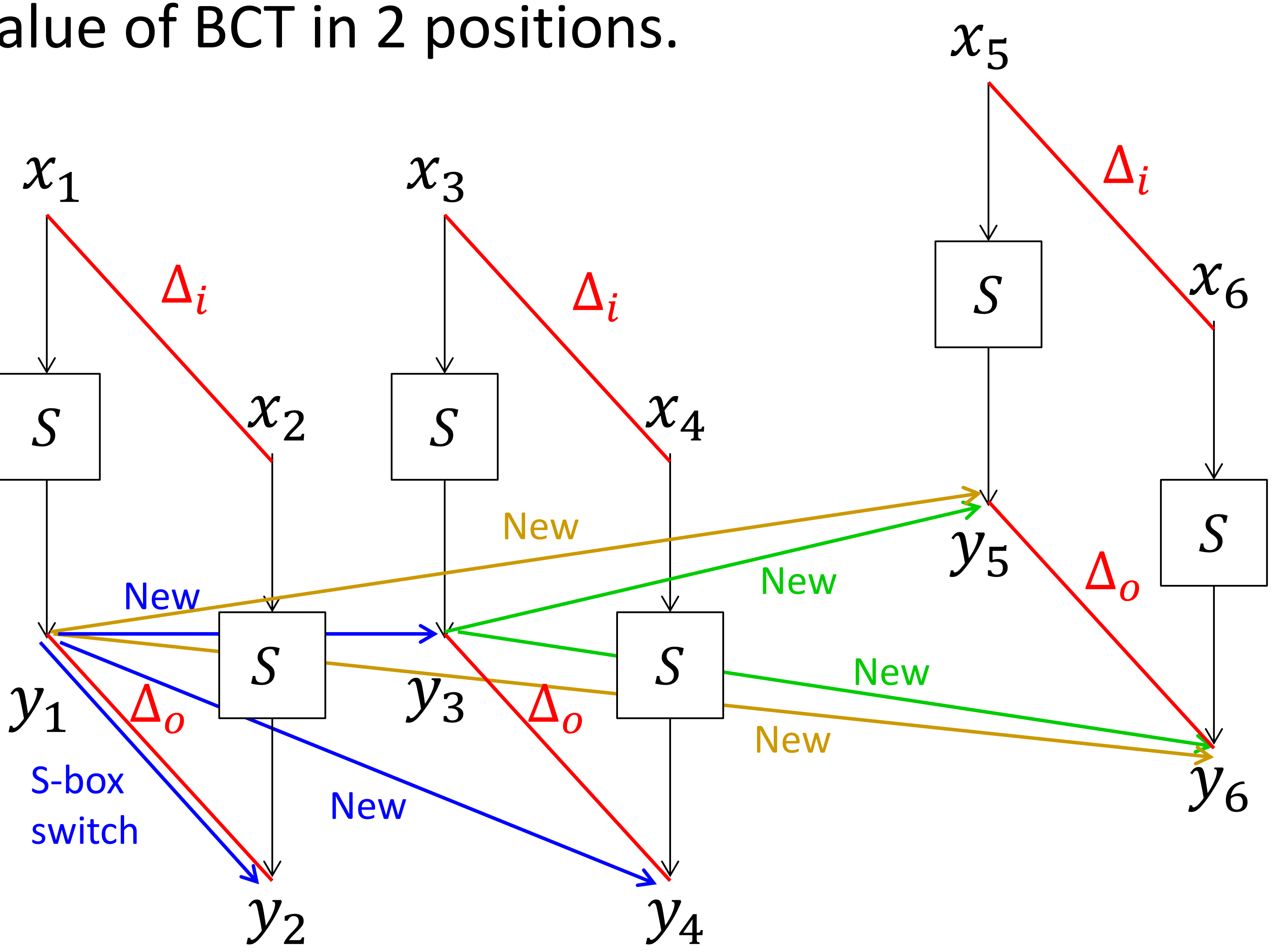
- 3 ways to define ∇, one is known as S-box switch



Lemma 2 *For any fixed Δ_i, for each entry with '4' in the DDT, the value of two positions in the BCT will increase by 4.*

Generalized Switch for 6-uniform DDT

We can make 3 distinct quartets. Each increases the value of BCT in 2 positions.



Applications so far

Related-tweakey boomerang distinguisher on 8-round Deoxys-384:

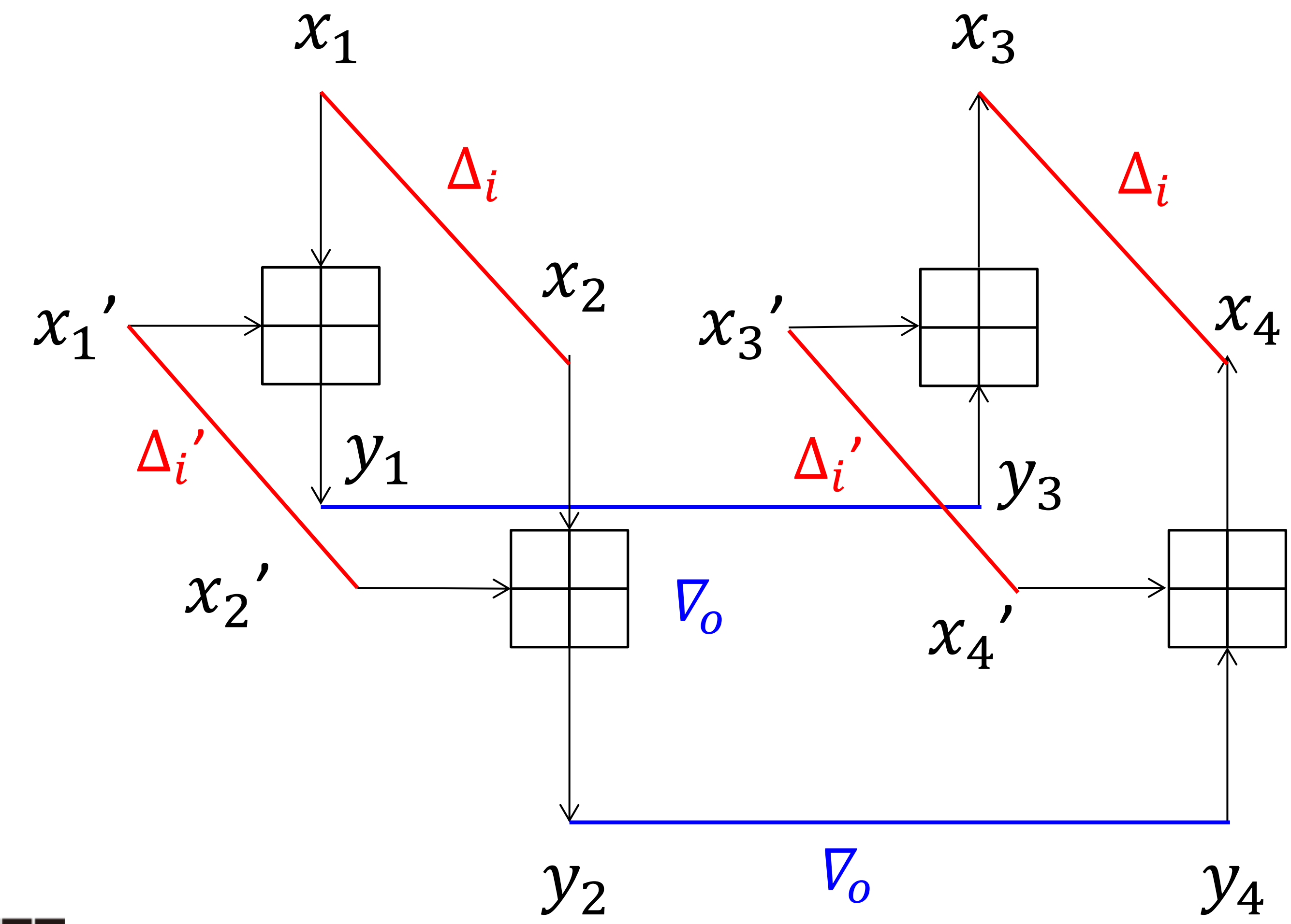
- Prev: 2^{-6} (single S-box switch)
- New: $2^{-5.4}$ (single generalized switch)
- 9R and 10R distinguishers are also improved.

Related-tweakey rectangle attacks on SKINNY

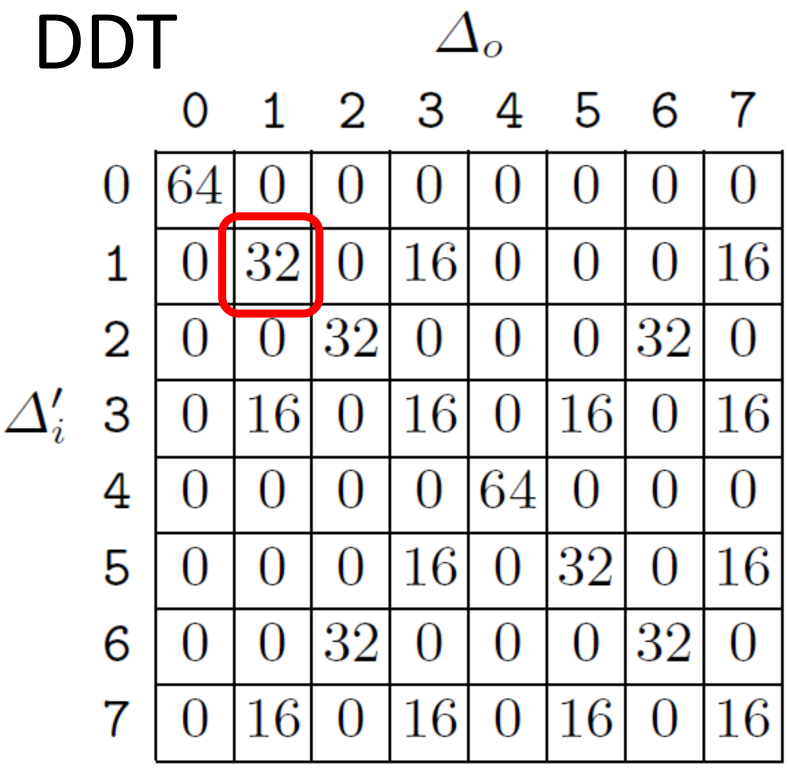
- Prev: prob was experimentally evaluated
- New: theoretical analysis of the probability

Extension to ARX Construction

Similar analysis can be applied to modular addition.

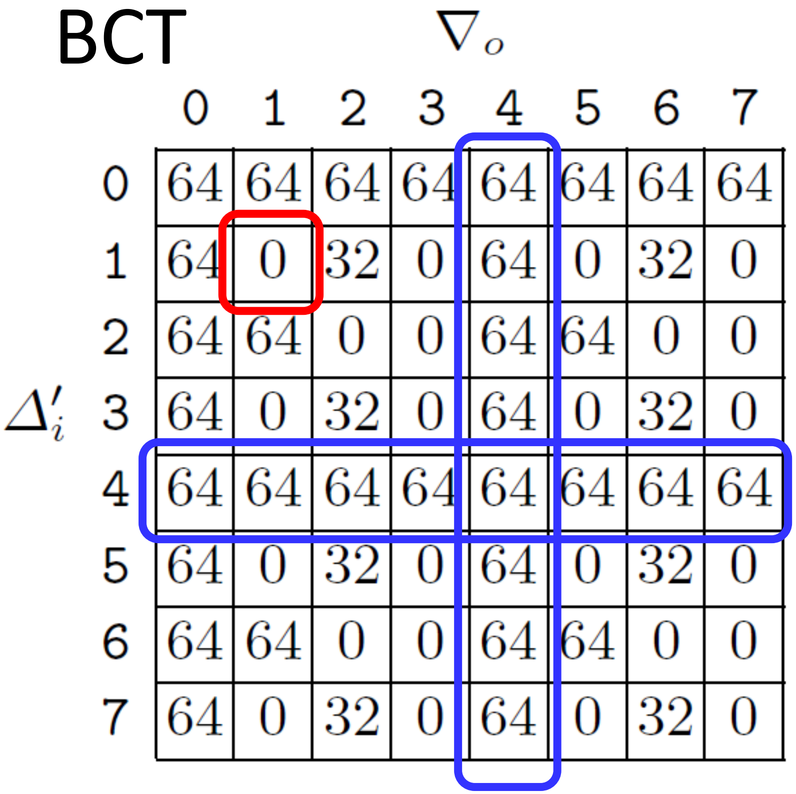


Case Study: 3-bit Addition ($\Delta_i = 0$)



DDT

		Δ_o							
		0	1	2	3	4	5	6	7
	0	64	0	0	0	0	0	0	0
	1	0	32	0	16	0	0	0	16
	2	0	0	32	0	0	0	32	0
Δ'_i	3	0	16	0	16	0	16	0	16
	4	0	0	0	0	64	0	0	0
	5	0	0	0	16	0	32	0	16
	6	0	0	32	0	0	0	32	0
	7	0	16	0	16	0	16	0	16



BCT

		∇_o							
		0	1	2	3	4	5	6	7
	0	64	64	64	64	64	64	64	64
	1	64	0	32	0	64	0	32	0
	2	64	64	0	0	64	64	0	0
Δ'_i	3	64	0	32	0	64	0	32	0
	4	64	64	64	64	64	64	64	64
	5	64	0	32	0	64	0	32	0
	6	64	64	0	0	64	64	0	0
	7	64	0	32	0	64	0	32	0

- BCT < DDT (S-box switch does not work)
- MSB switch

Concluding Remarks

BCT: precomp table of $\boldsymbol{r}$ in the sandwich attack

Adv. 1: new switching effect ($\boldsymbol{r}$ is surprisingly high)

Adv. 2: quantitating the strength of S-box against sandwich attack (S-box design criteria)

Problems to investigate

- improving previous boomerang attacks
- extending E_m (more than single S-layer)
- comprehensive study for modular addition

Thank you for your attention!!