

On the **Feistel** counterpart of the BCT

Introduction and Analysis of the **FBCT**

Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal and Marine Minier

Université de Lorraine, INRIA, Loria, CNRS - Nancy, France

FSE 2020 | November 9-13, 2020 | your computer screen

In this talk

- The Boomerang switches and the BCT
- Feistel case: introducing the **FBCT**
- Multiple-round case

Basic boomerang distinguisher

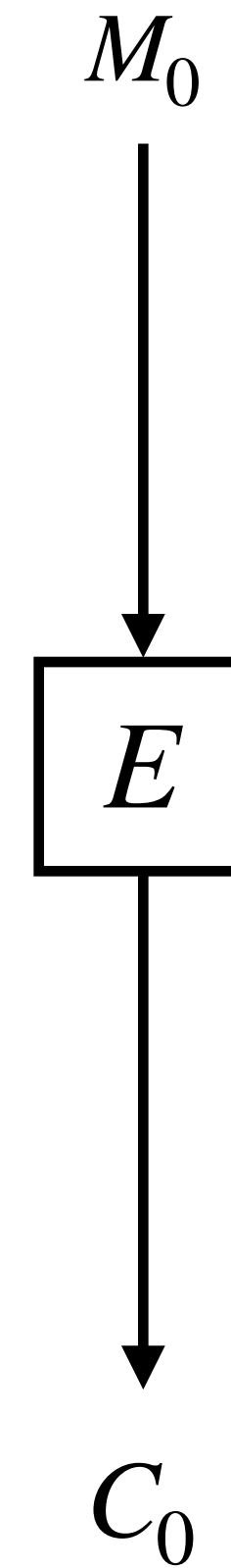
 [The Boomerang Attack](#)
Wagner, *FSE 1999*

Variant of differential cryptanalysis that considers **quartets** of messages.

Basic boomerang distinguisher

[Wagner, FSE '99]

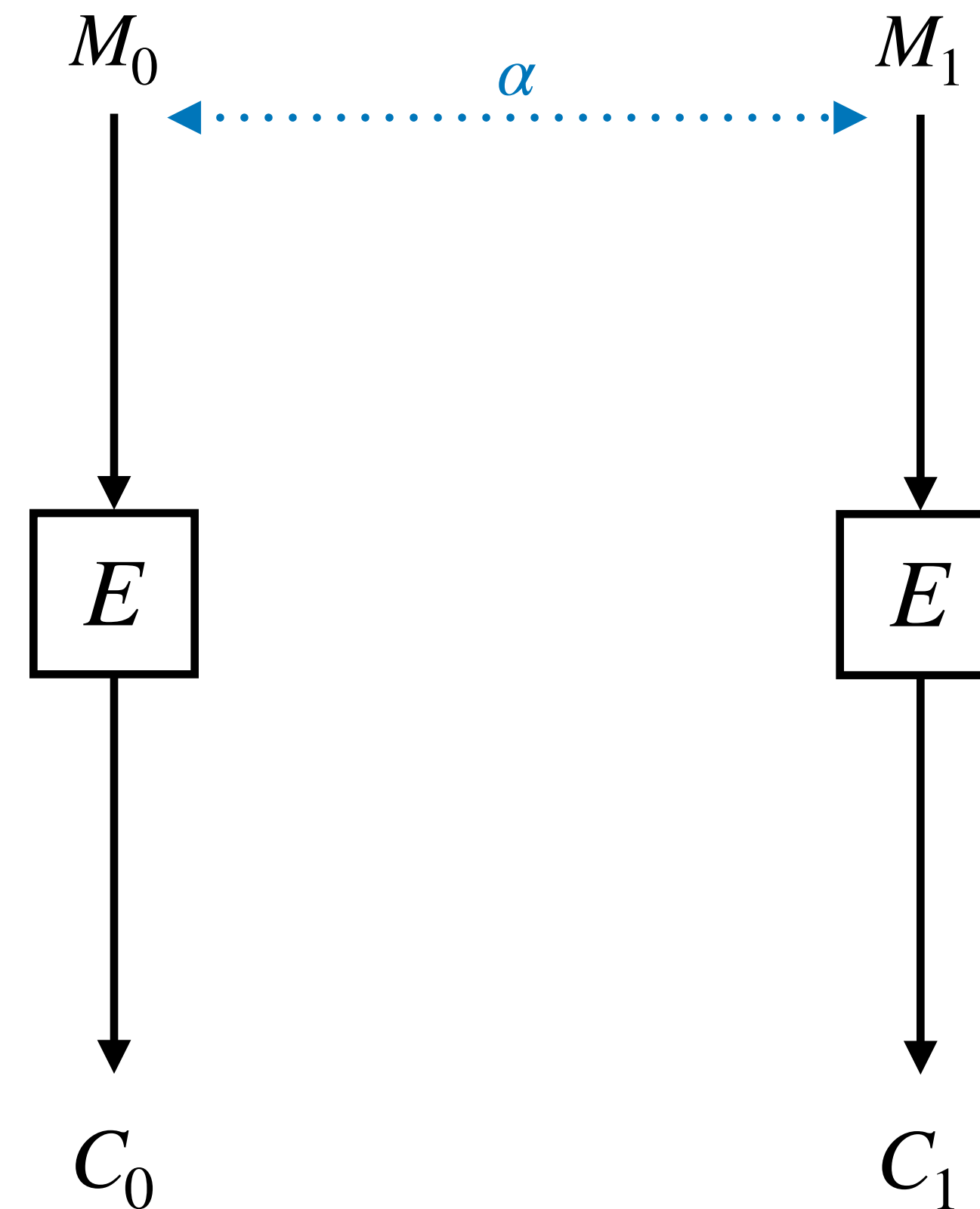
1. Pick M_0 at random, ask for its ciphertext C_0



Basic boomerang distinguisher

[Wagner, FSE '99]

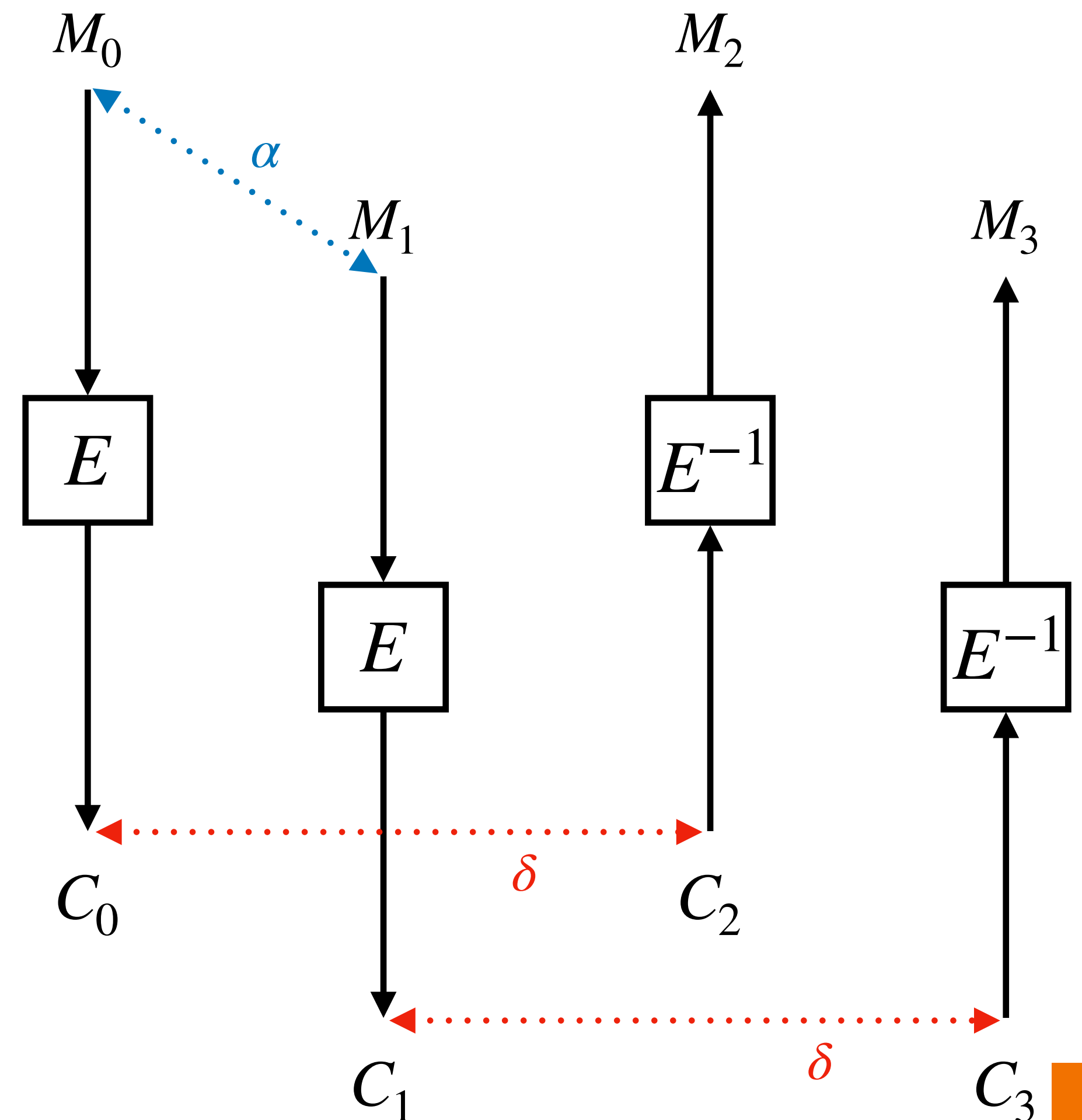
1. Pick M_0 at random, ask for its ciphertext C_0
2. Ask for C_1 , the ciphertext of $M_1 = M_0 \oplus \alpha$



Basic boomerang distinguisher

[Wagner, FSE '99]

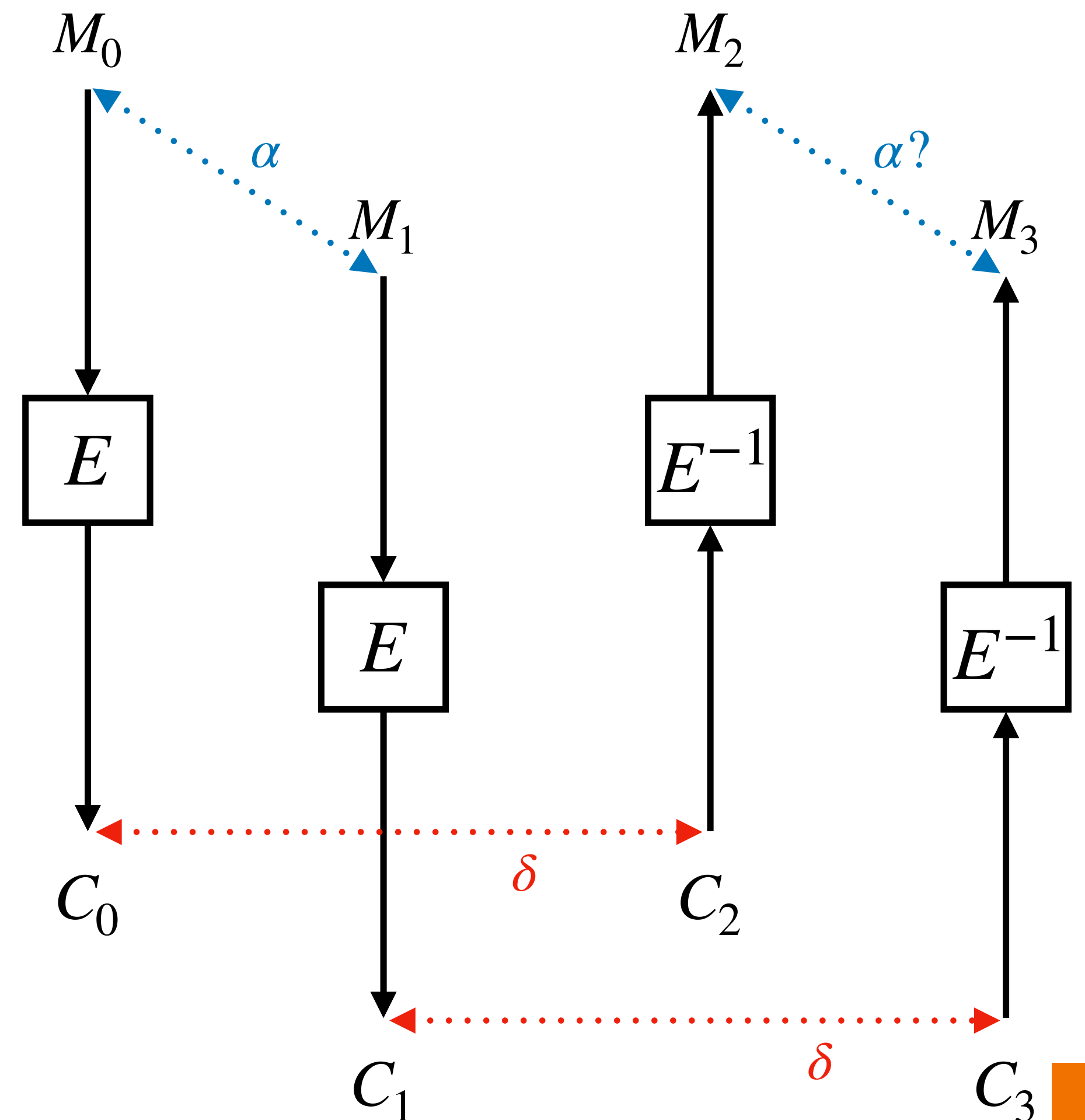
1. Pick M_0 at random, ask for its ciphertext C_0
2. Ask for C_1 , the ciphertext of $M_1 = M_0 \oplus \alpha$
3. Compute $C_2 = C_0 \oplus \delta$, $C_3 = C_1 \oplus \delta$
4. Ask for their decryption (M_2, M_3)



Basic boomerang distinguisher

[Wagner, FSE '99]

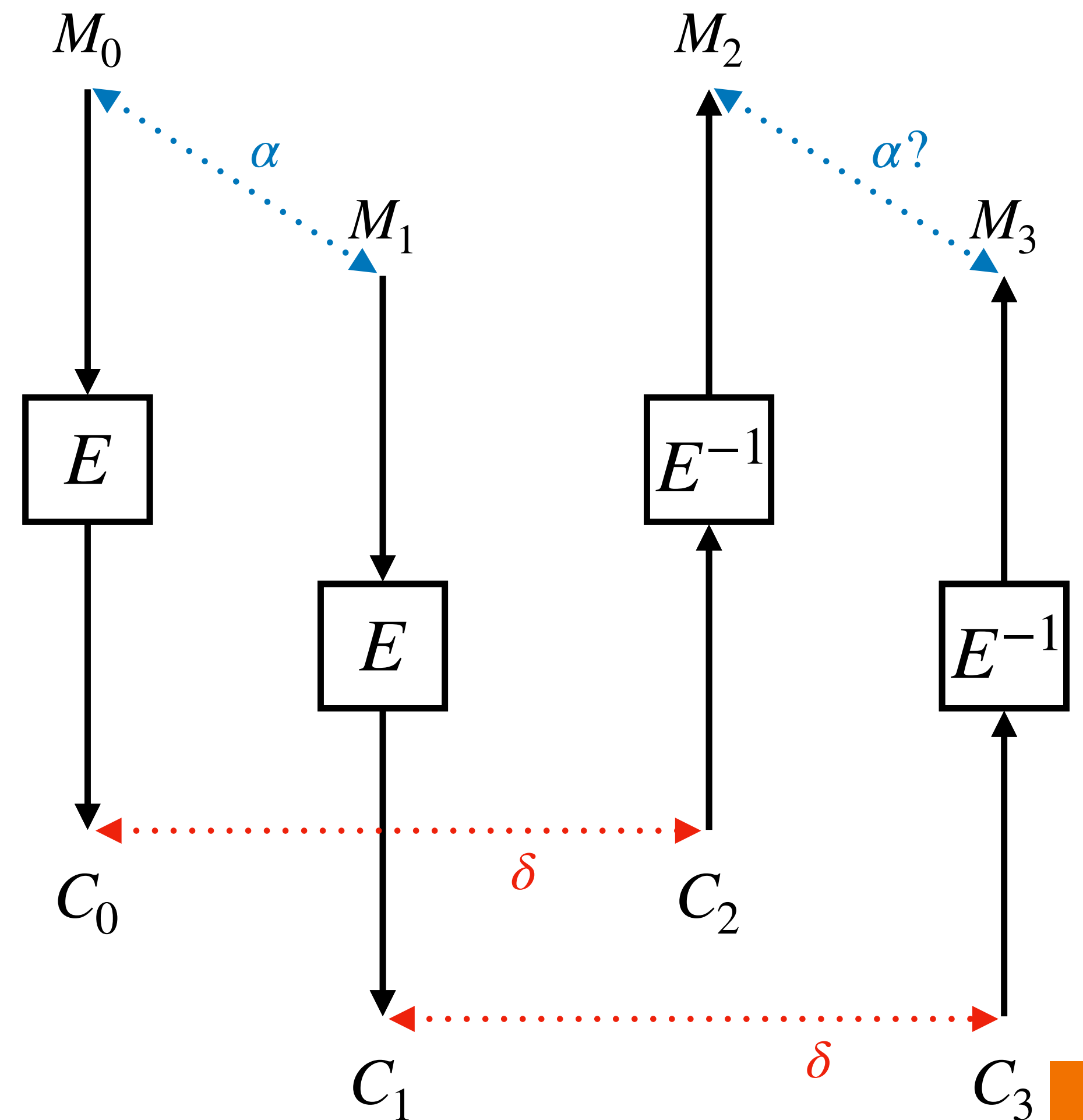
1. Pick M_0 at random, ask for its ciphertext C_0
2. Ask for C_1 , the ciphertext of $M_1 = M_0 \oplus \alpha$
3. Compute $C_2 = C_0 \oplus \delta$, $C_3 = C_1 \oplus \delta$
4. Ask for their decryption (M_2, M_3)
5. Check if $M_2 \oplus M_3 = \alpha$



Basic boomerang distinguisher

[Wagner, FSE '99]

Rewrite $E = E_1 \circ E_0$

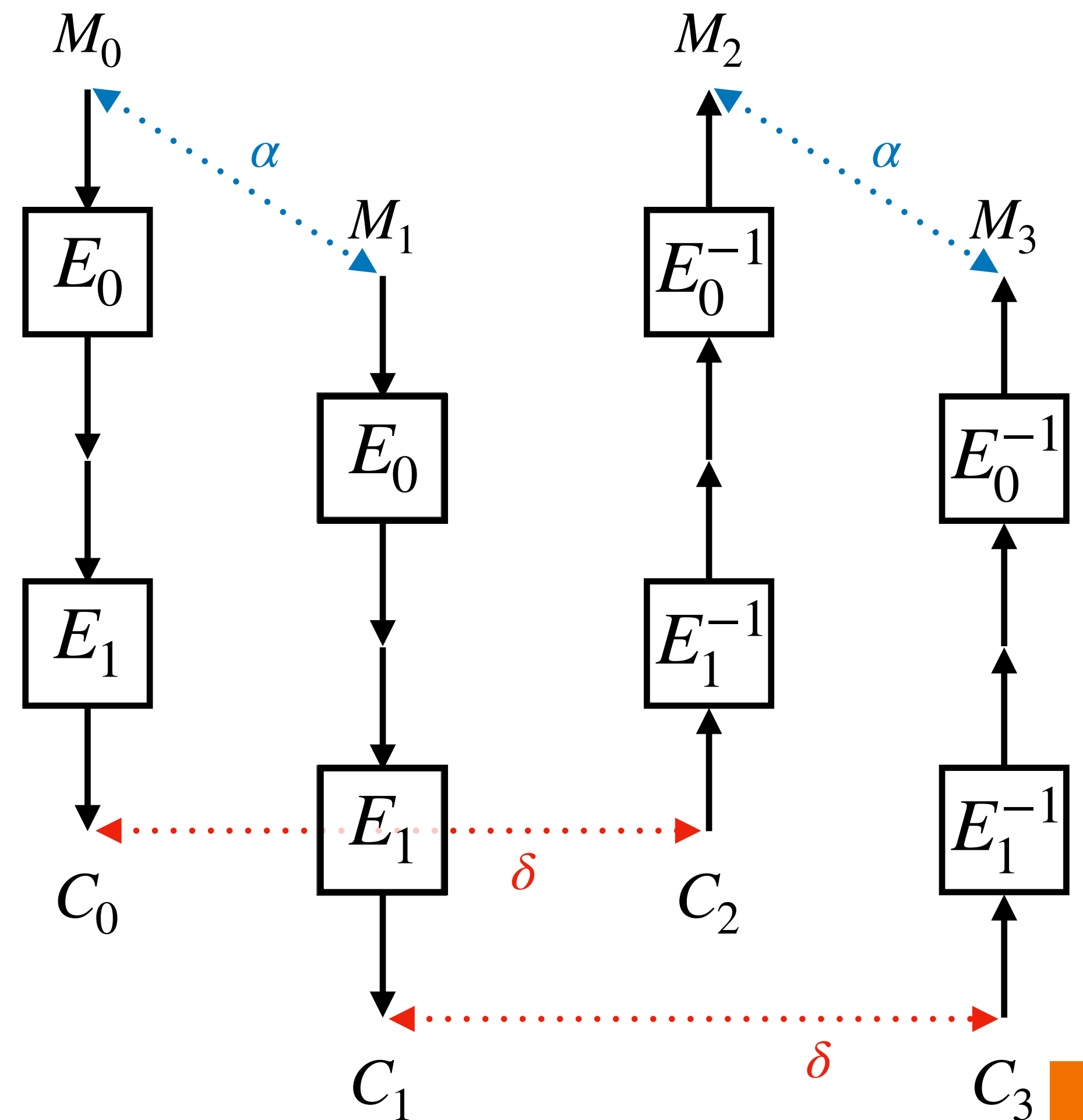


Basic boomerang distinguisher

[Wagner, FSE '99]

Rewrite $E = E_1 \circ E_0$

Find good differentials:



Basic boomerang distinguisher

[Wagner, FSE '99]

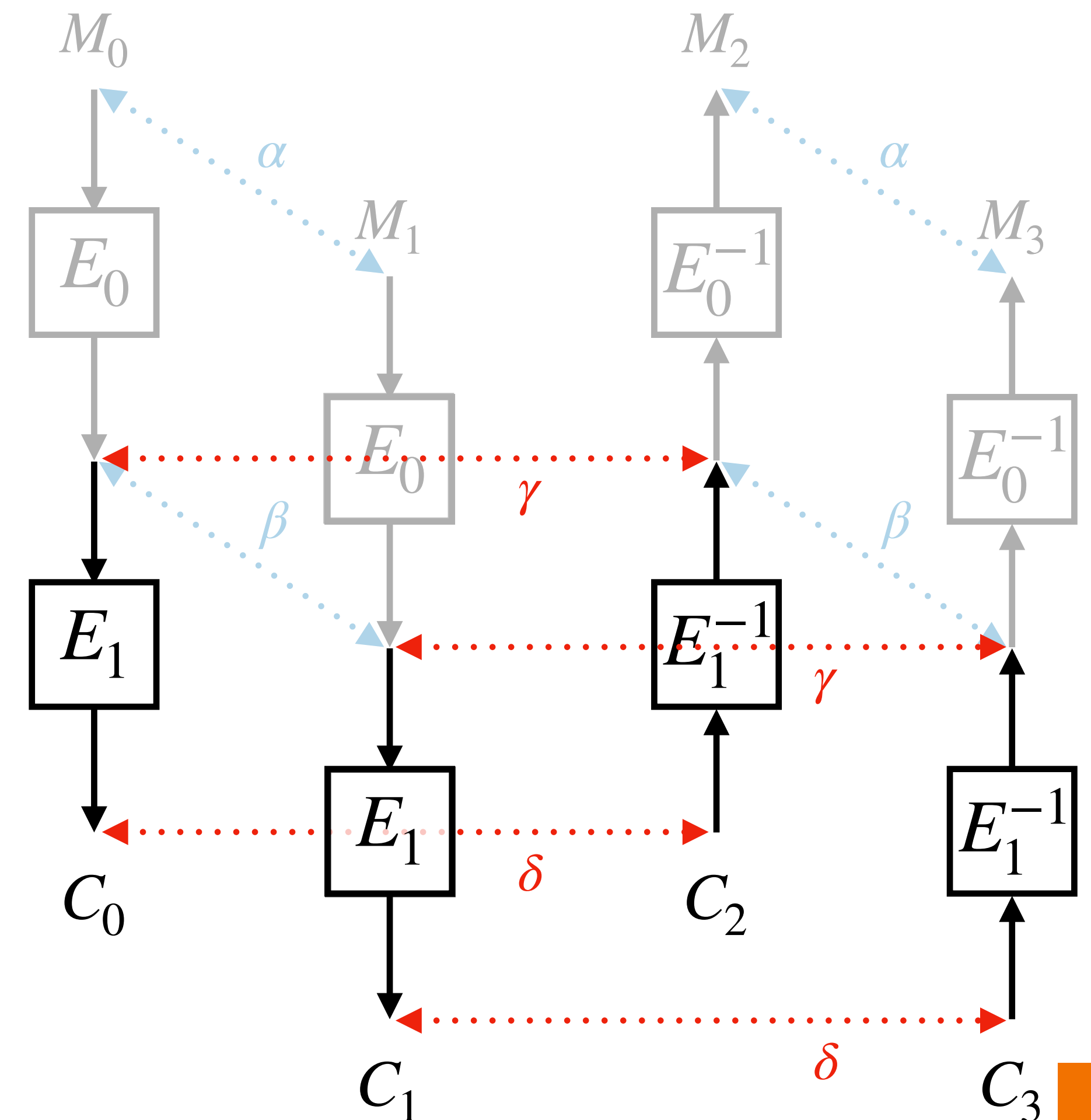
Rewrite $E = E_1 \circ E_0$

Find good differentials:

$$\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$$

$$\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$$

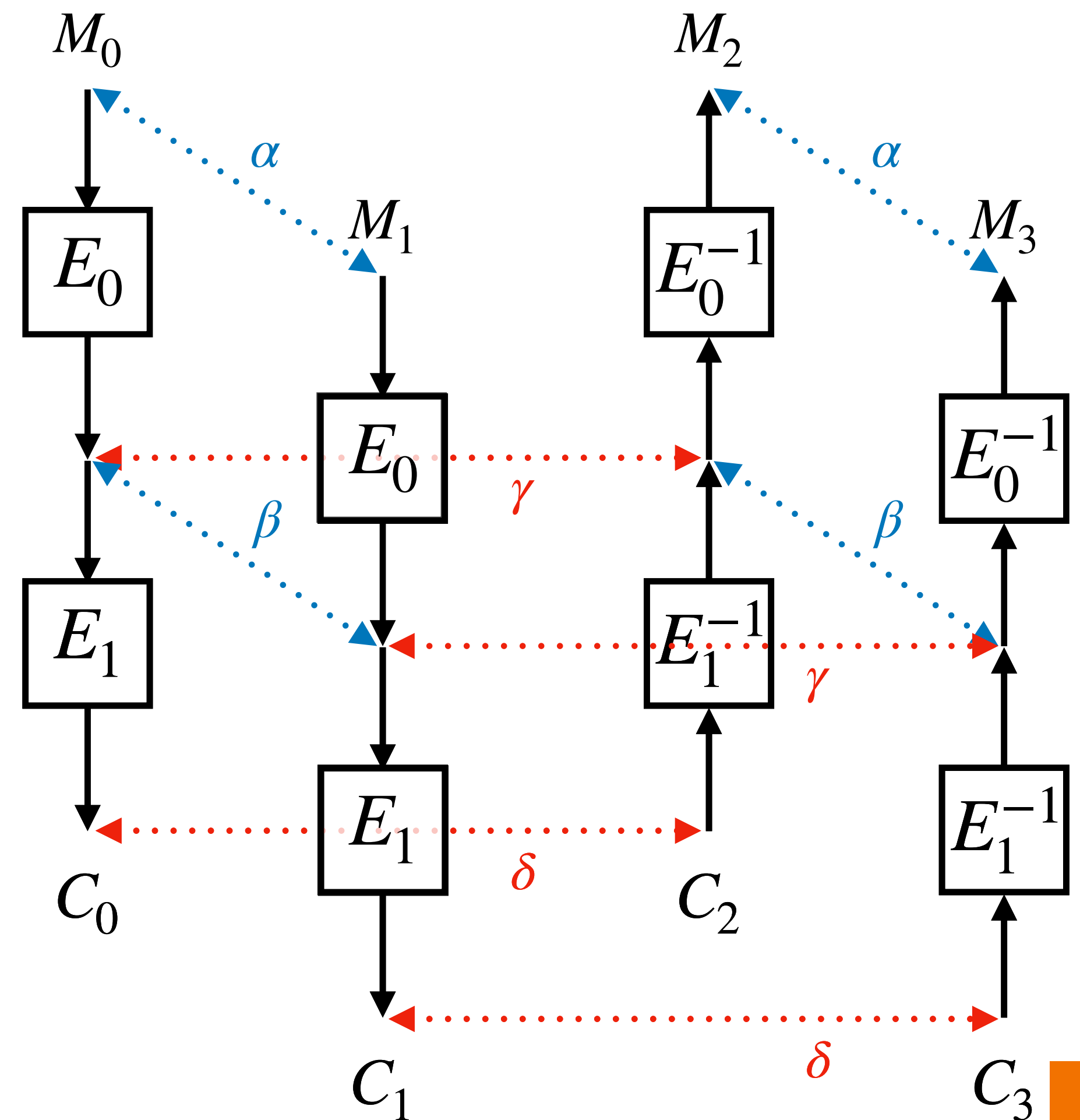
Expected probability of p^2q^2 if the two characteristics are “independant”.



Basic boomerang distinguisher

[Wagner, FSE '99]

Incompatibilities are discovered.



Basic boomerang distinguisher

[Wagner, FSE '99]

Incompatibilities are discovered.

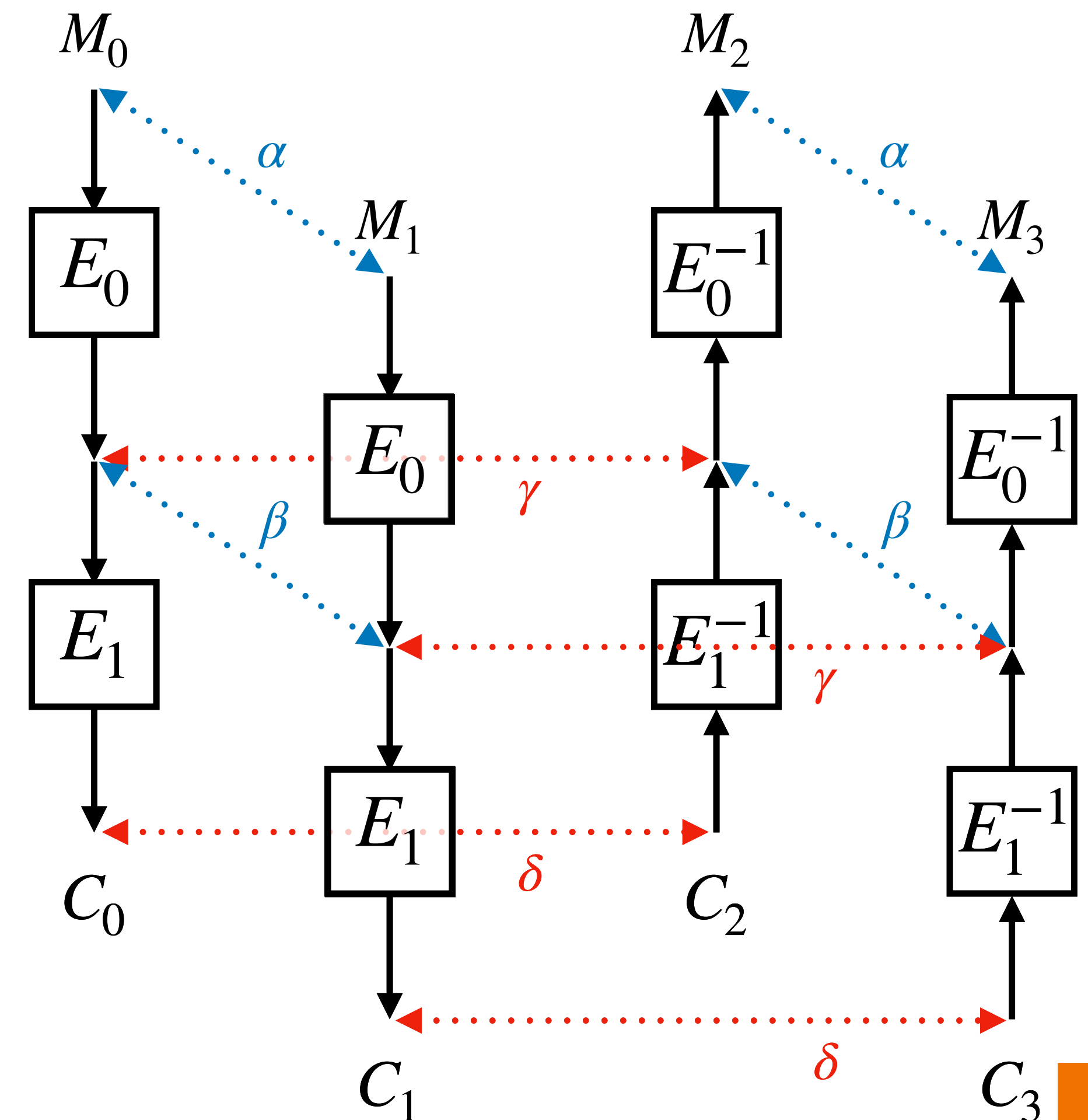
📄 [Related-key Cryptanalysis of the Full AES-192 and AES-256](#)

Biryukov & Khovratovich, *ASIACRYPT 2009*

📄 [The Return of the Cryptographic Boomerang](#)

Murphy, *IEEE Transactions on Information Theory 2011*

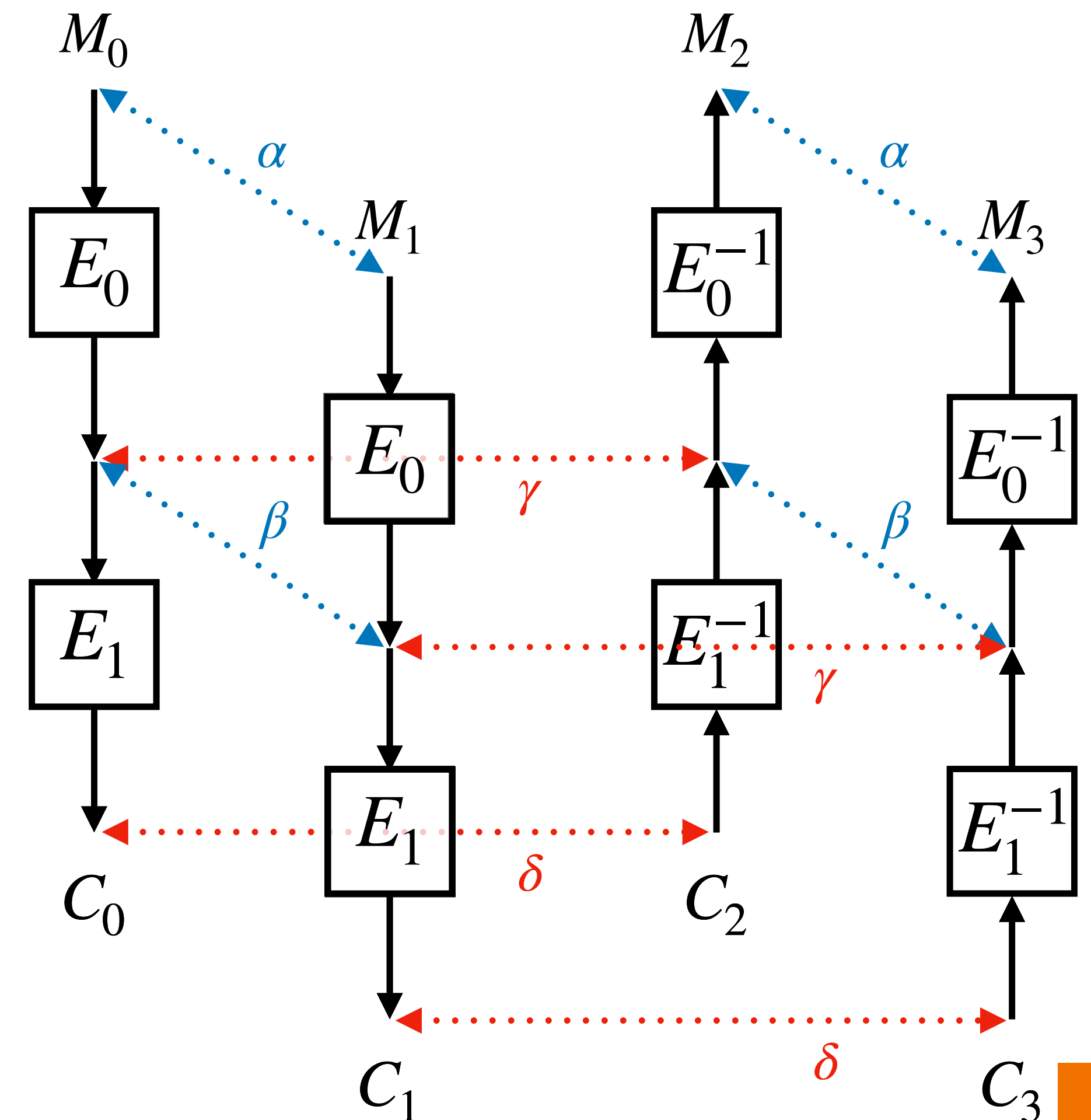
The problems come from interactions at the **junction** of the two trails.



Analysis of the junction

The sandwich attack

 [A Practical-time Related-key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony](#)
Dunkelman, Keller & Shamir, *CRYPTO 2010*



Analysis of the junction

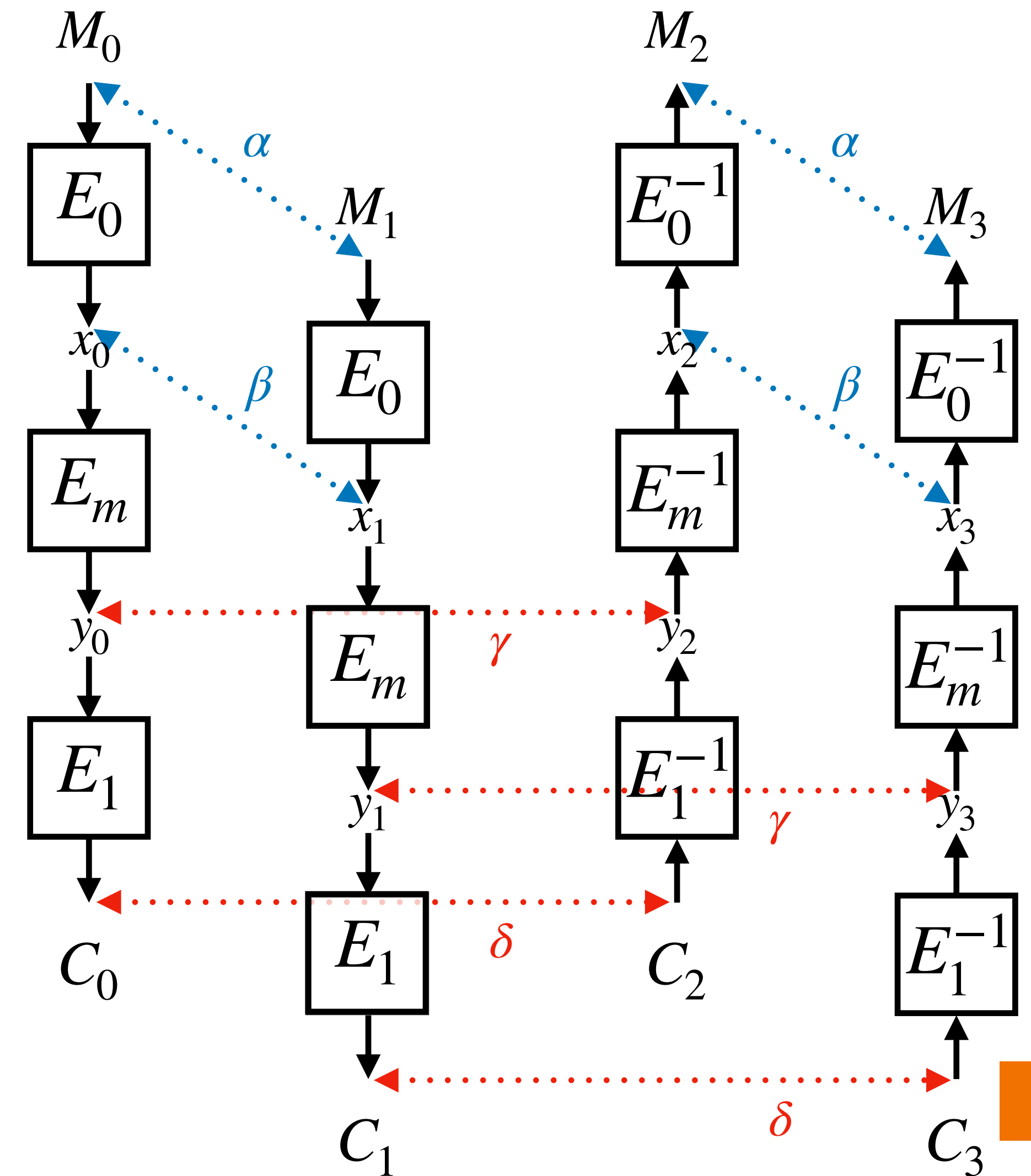
The sandwich attack

 A Practical-time Related-key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony
Dunkelman, Keller & Shamir, *CRYPTO 2010*

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

E_m is 1 round (boomerang switch)

Expected probability of p^2q^2r



The BCT

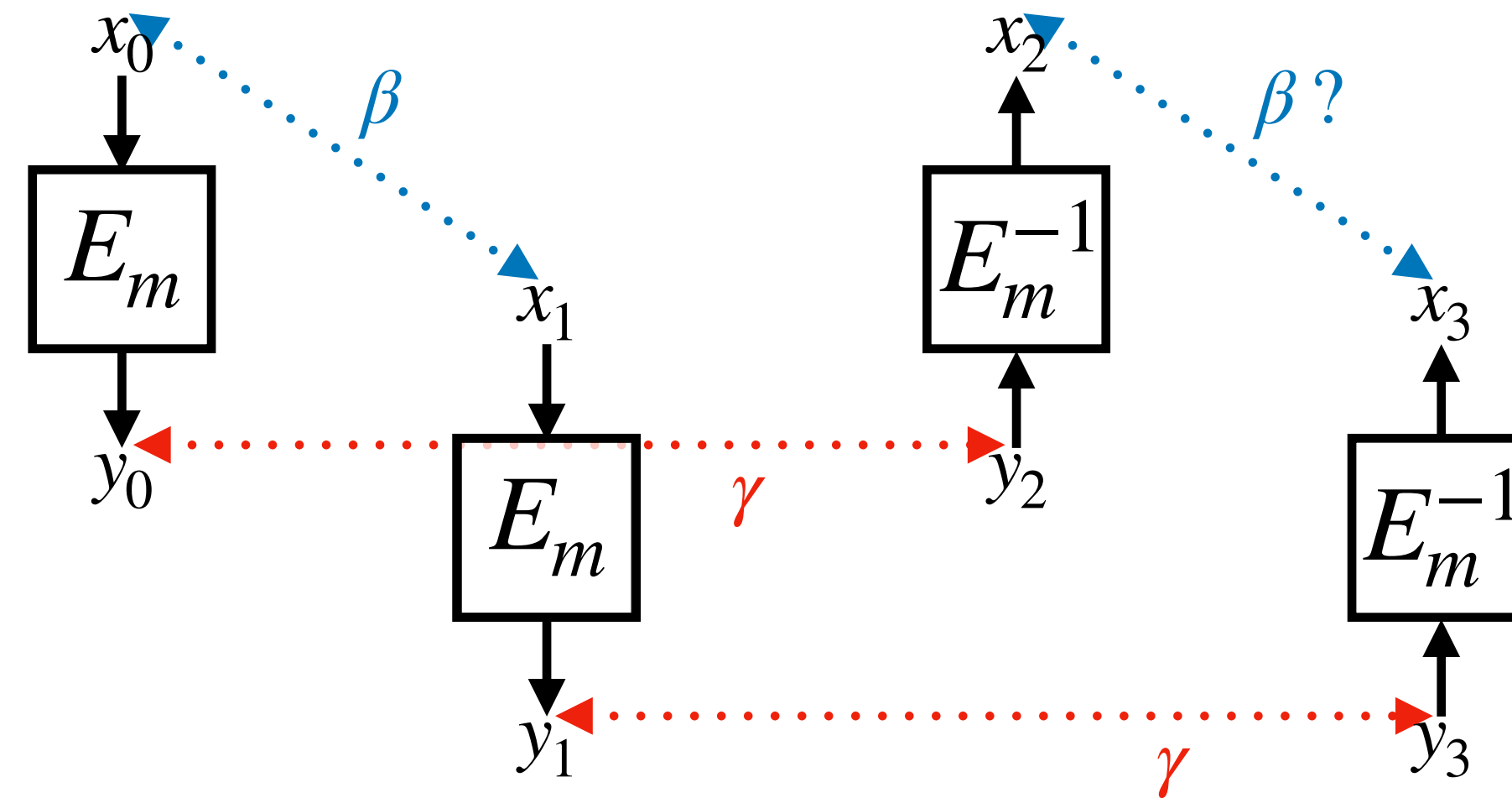
Automated analysis for a 1-round E_m for SPNs

 [Boomerang Connectivity Table: a New Cryptanalysis Tool](#)
Cid, Huang, Peyrin, Sasaki & Song, *EUROCRYPT 2018*

The BCT

Automated analysis for a 1-round E_m for SPNs

 [Boomerang Connectivity Table: a New Cryptanalysis Tool](#)
Cid, Huang, Peyrin, Sasaki & Song, *EUROCRYPT 2018*

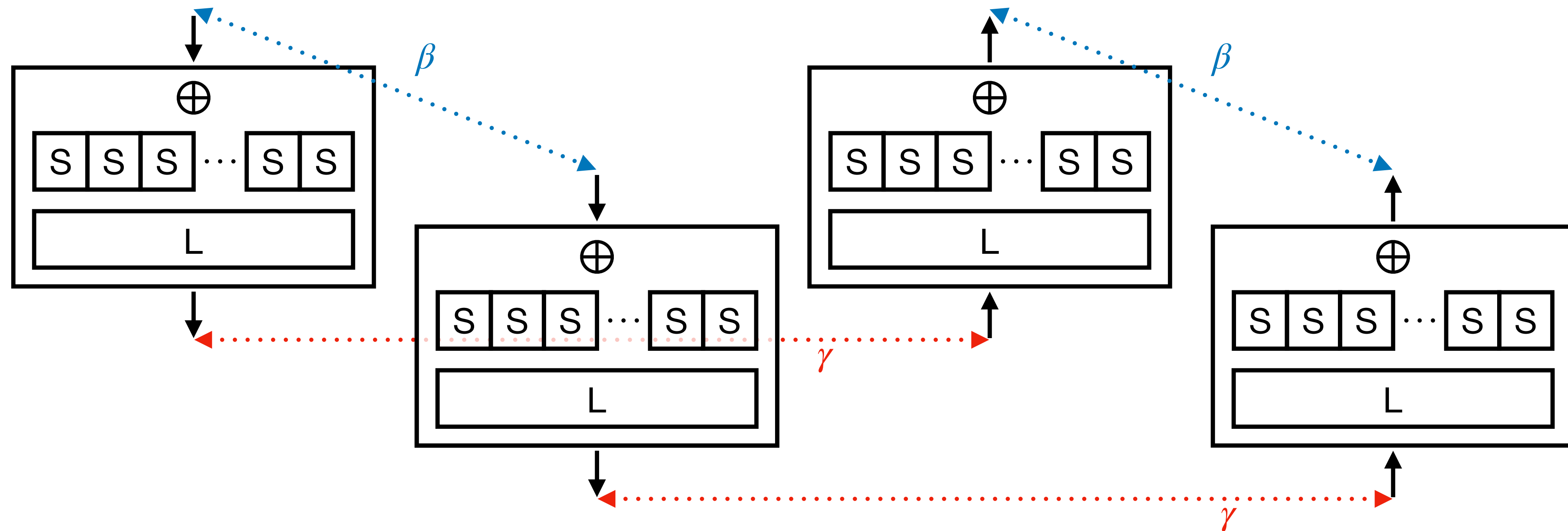


$$E_m^{-1}(E_m(X) \oplus \gamma) \oplus E_m^{-1}(E_m(X \oplus \beta) \oplus \gamma) = \beta$$

The BCT

Automated analysis for a 1-round E_m for SPNs

 [Boomerang Connectivity Table: a New Cryptanalysis Tool](#)
 Cid, Huang, Peyrin, Sasaki & Song, *EUROCRYPT 2018*

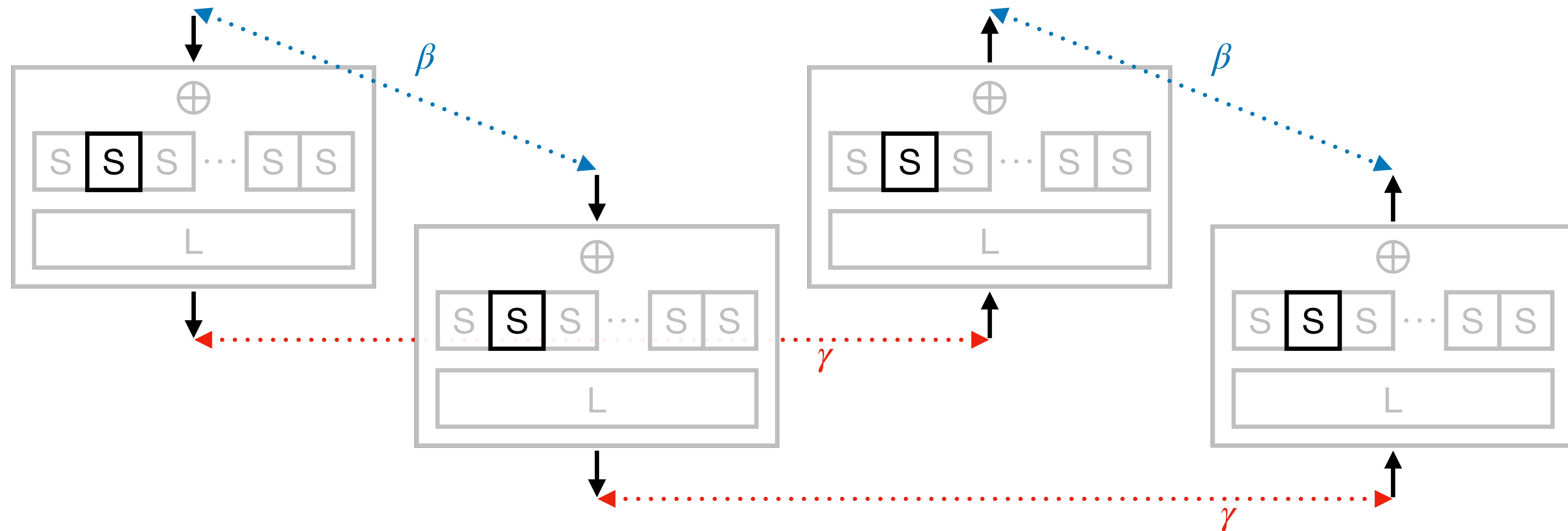


$$E_m^{-1}(E_m(X) \oplus \gamma) \oplus E_m^{-1}(E_m(X \oplus \beta) \oplus \gamma) = \beta$$

The BCT

Automated analysis for a 1-round E_m for SPNs

 [Boomerang Connectivity Table: a New Cryptanalysis Tool](#)
Cid, Huang, Peyrin, Sasaki & Song, *EUROCRYPT 2018*

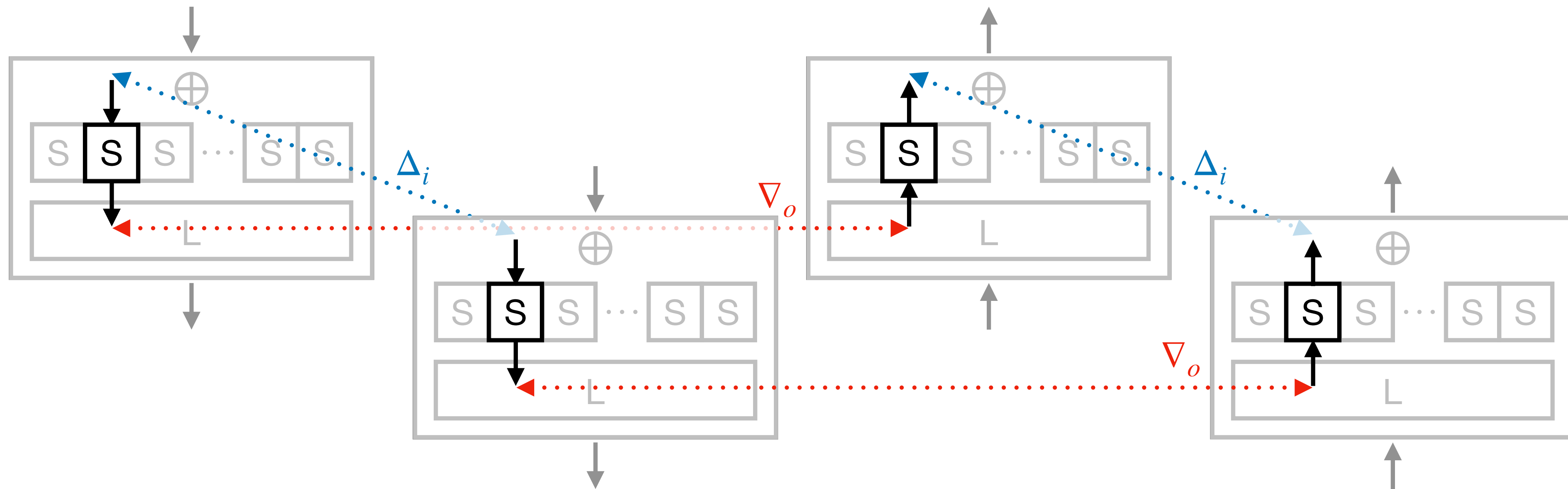


$$E_m^{-1}(E_m(X) \oplus \gamma) \oplus E_m^{-1}(E_m(X \oplus \beta) \oplus \gamma) = \beta$$

The BCT

Automated analysis for a 1-round E_m for SPNs

 [Boomerang Connectivity Table: a New Cryptanalysis Tool](#)
 Cid, Huang, Peyrin, Sasaki & Song, *EUROCRYPT 2018*

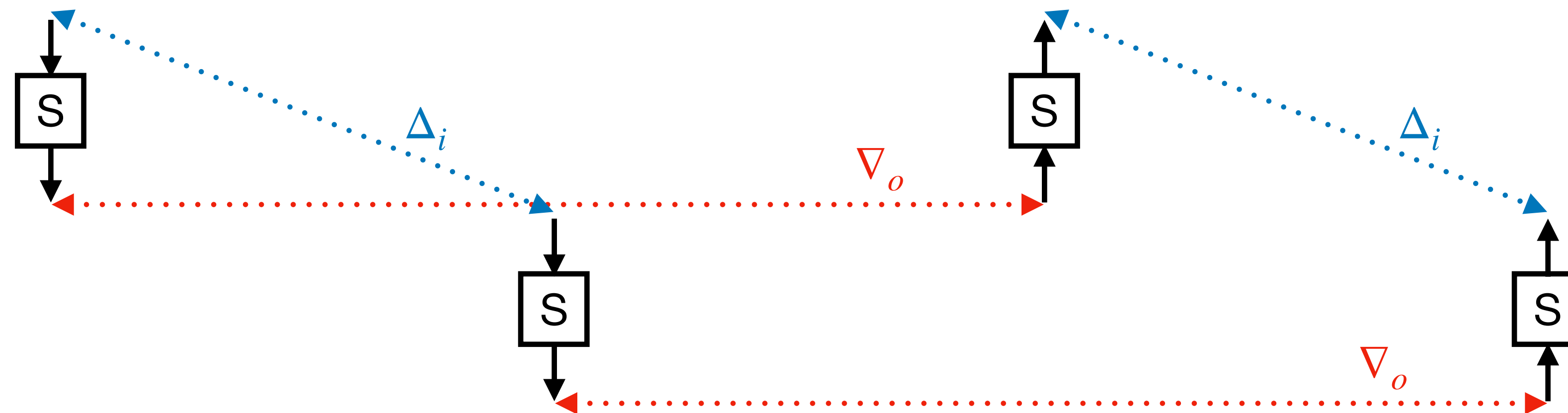


$$SE_m^{-1}(SE_m(x) \oplus \gamma) \oplus SE_m^{-1}(SE_m(x \oplus \Delta_i) \oplus \gamma) = \Delta_i$$

The BCT

Automated analysis for a 1-round E_m for SPNs

 [Boomerang Connectivity Table: a New Cryptanalysis Tool](#)
Cid, Huang, Peyrin, Sasaki & Song, *EUROCRYPT 2018*



Probability over 1 round = product of the probabilities over each S-box

$$S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o) = \Delta_i$$

The BCT

$$\text{BCT}(\Delta_i, \nabla_o) = \#\{x \mid S^{-1}(S(x) \oplus \nabla_o) \oplus S^{-1}(S(x \oplus \Delta_i) \oplus \nabla_o)\} = \Delta_i\}$$

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

The BCT

The BCT detects cases where the boomerang **won't come back**.

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

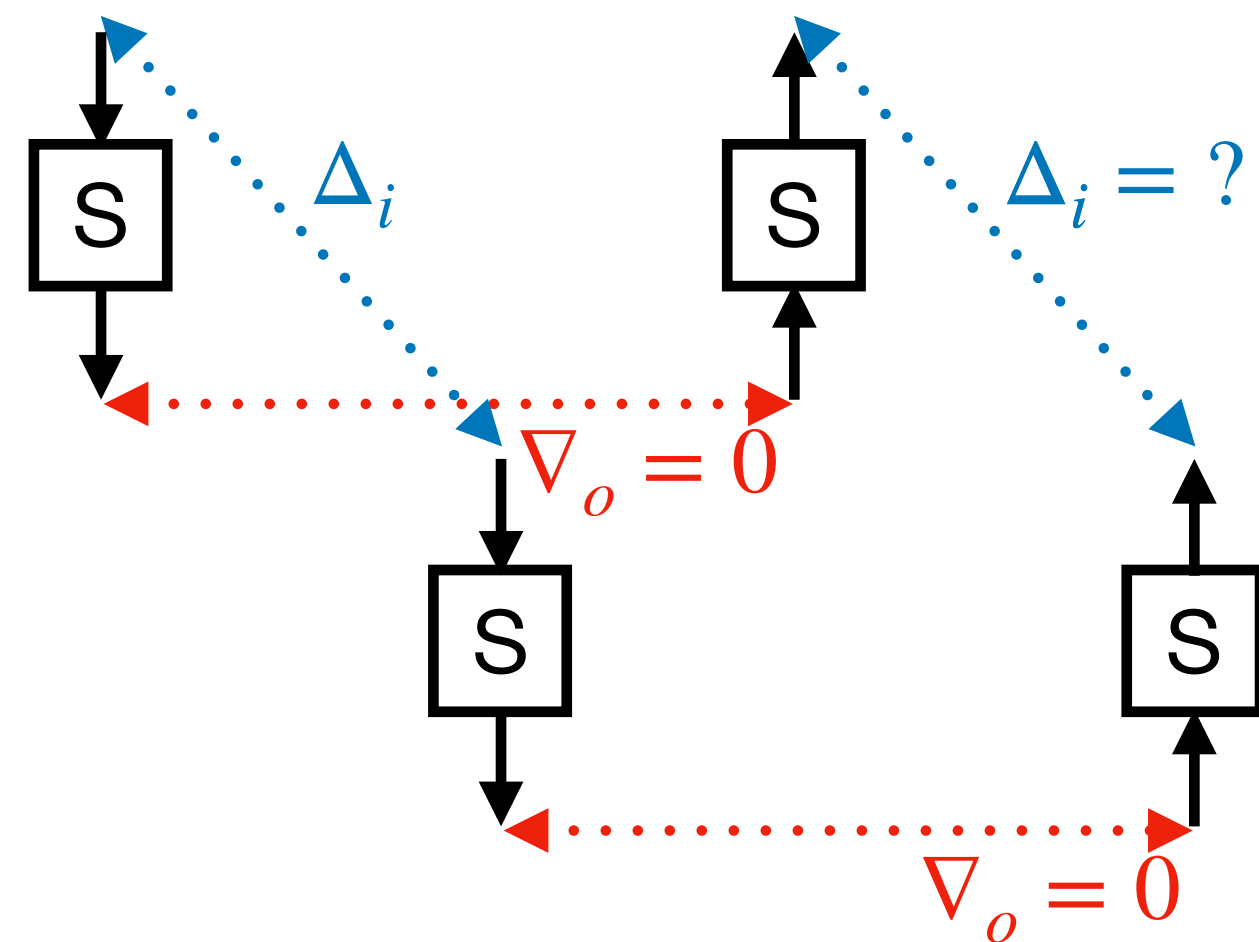
The BCT

The BCT detects the **ladder switch**.

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

The BCT

The BCT detects the **ladder switch**.

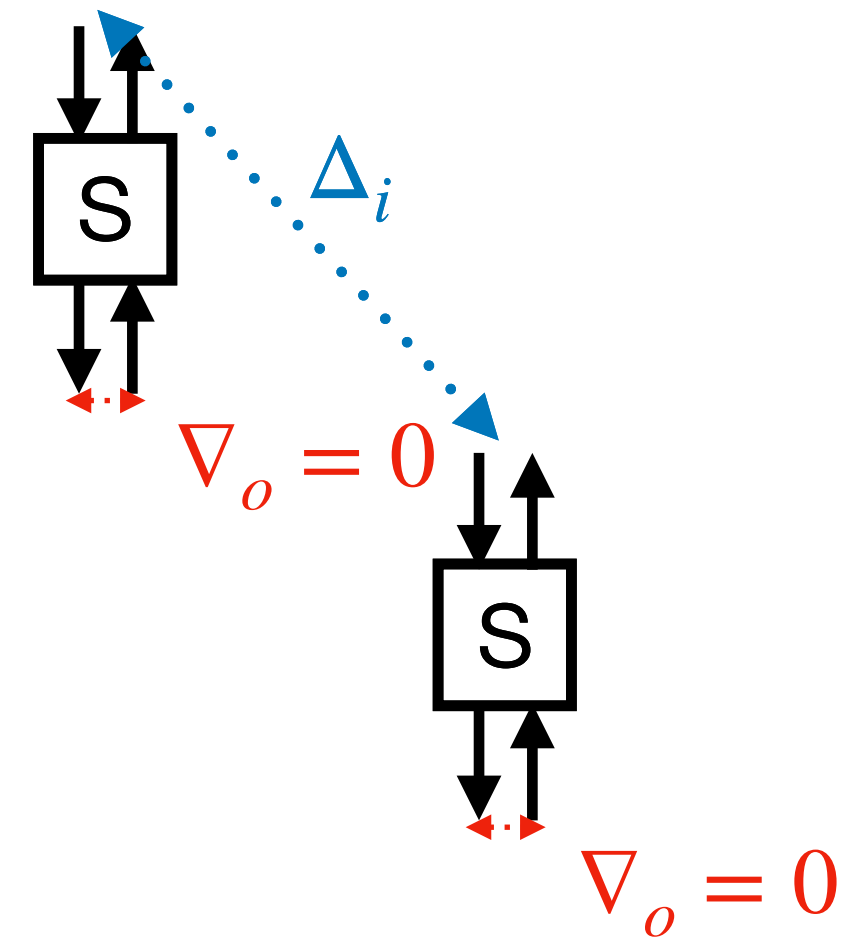


Ladder Switch: when one given S-box is active in E_0 and is not active in E_1 (and conversely), the transition comes for free.

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

The BCT

The BCT detects the **ladder switch**.



Ladder Switch: when one given S-box is active in E_0 and is not active in E_1 (and conversely), the transition comes for free.

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

The BCT

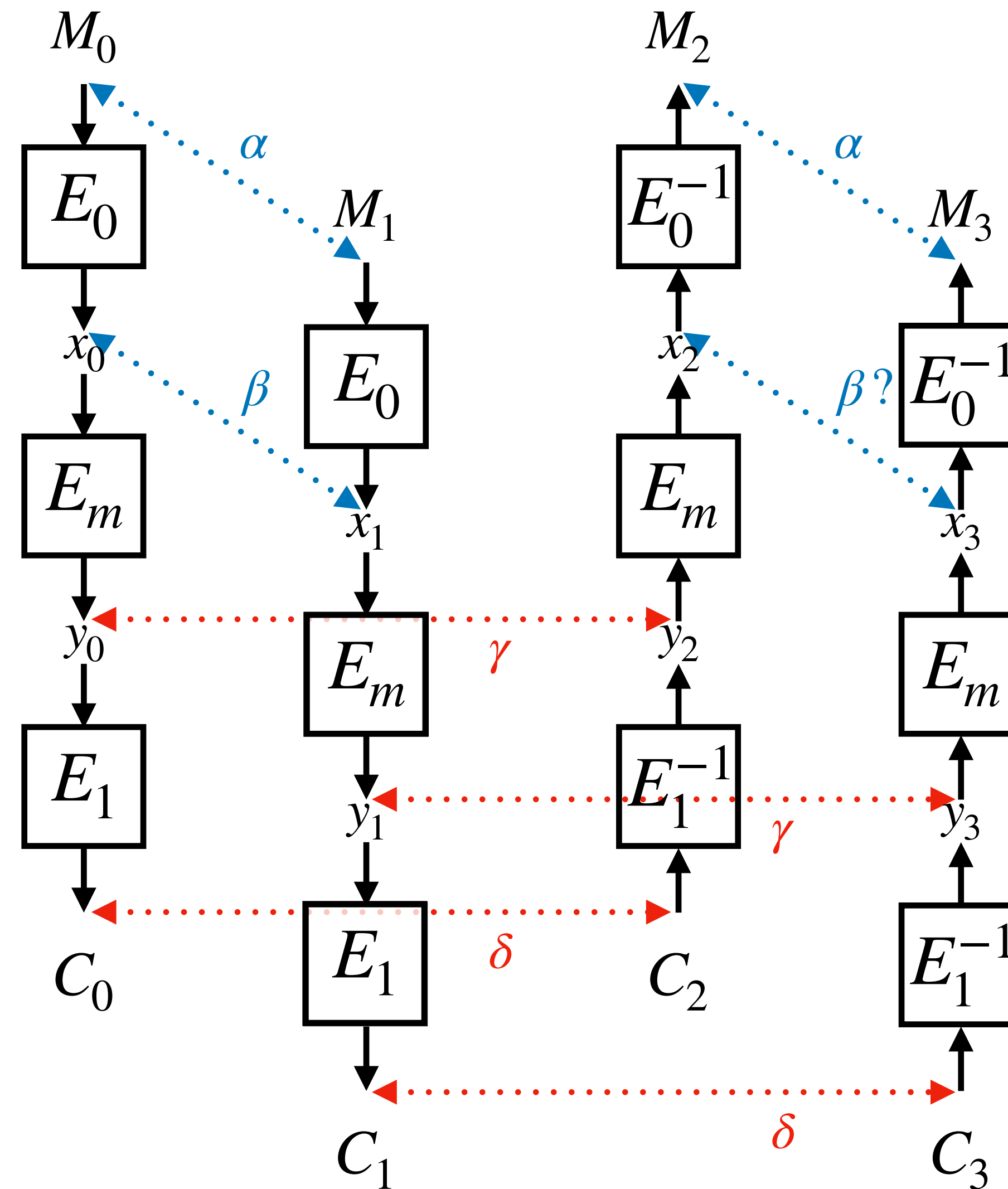
Recap

- Reduces the problem of computing the boomerang switch over 1 round of SPN to the one of computing it over each S-box of its nonlinear layer
- Easily gives incompatibility, Ladder switch (+ S-box switch)
- Gives a new criteria for S-boxes

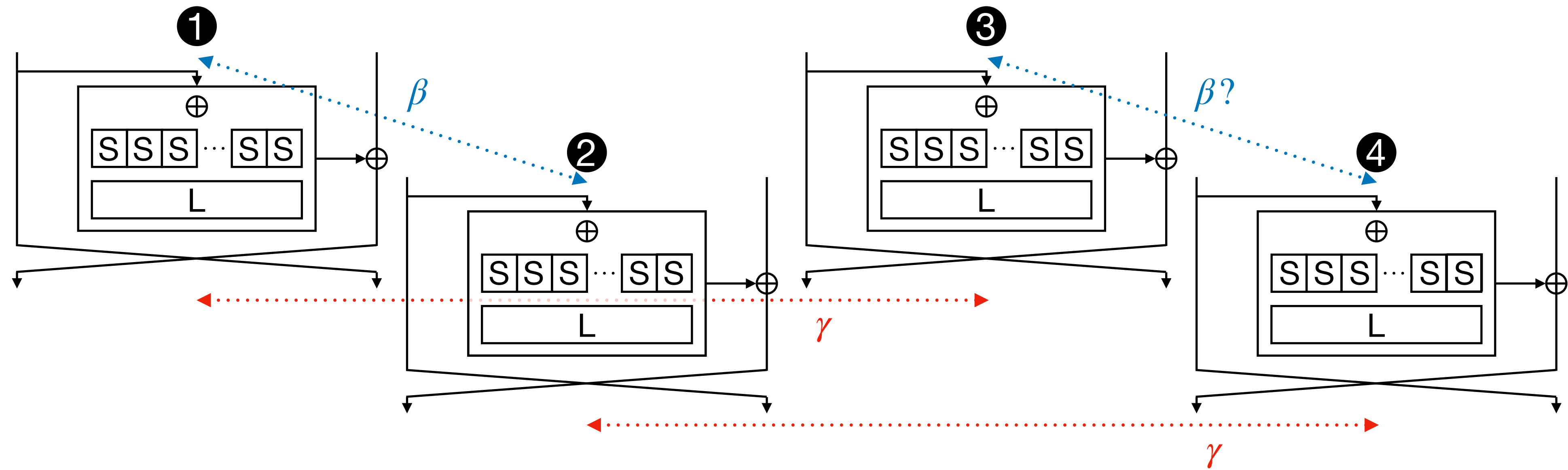
What about Feistel ciphers ?

The Feistel Boomerang Connectivity Table

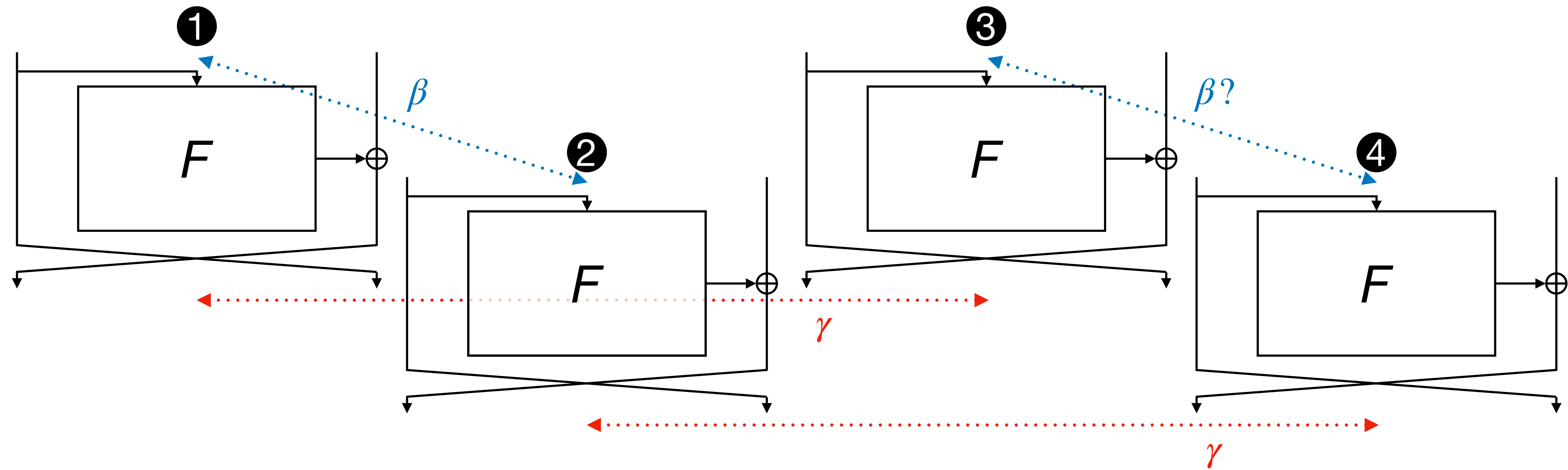
The Feistel counterpart of the BCT



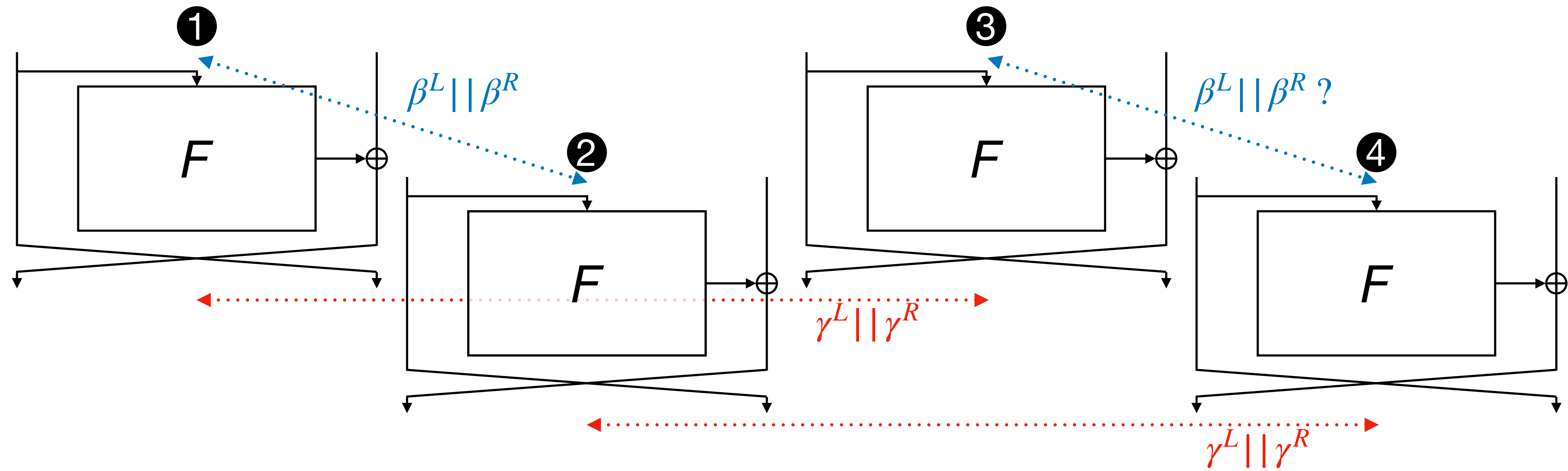
The FBCT



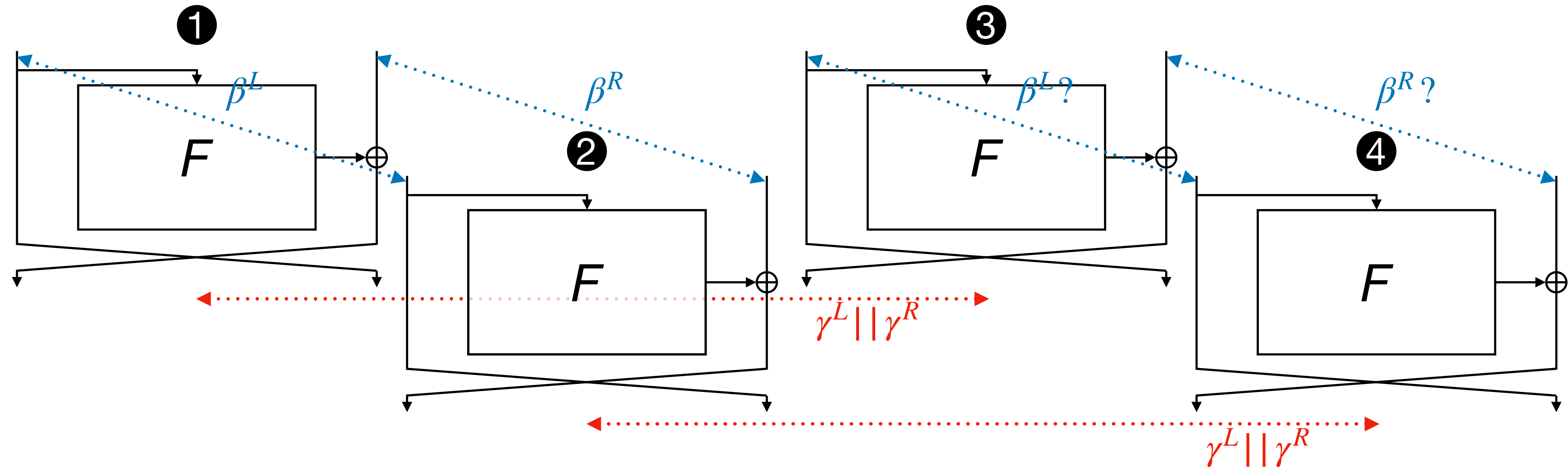
The FBCT



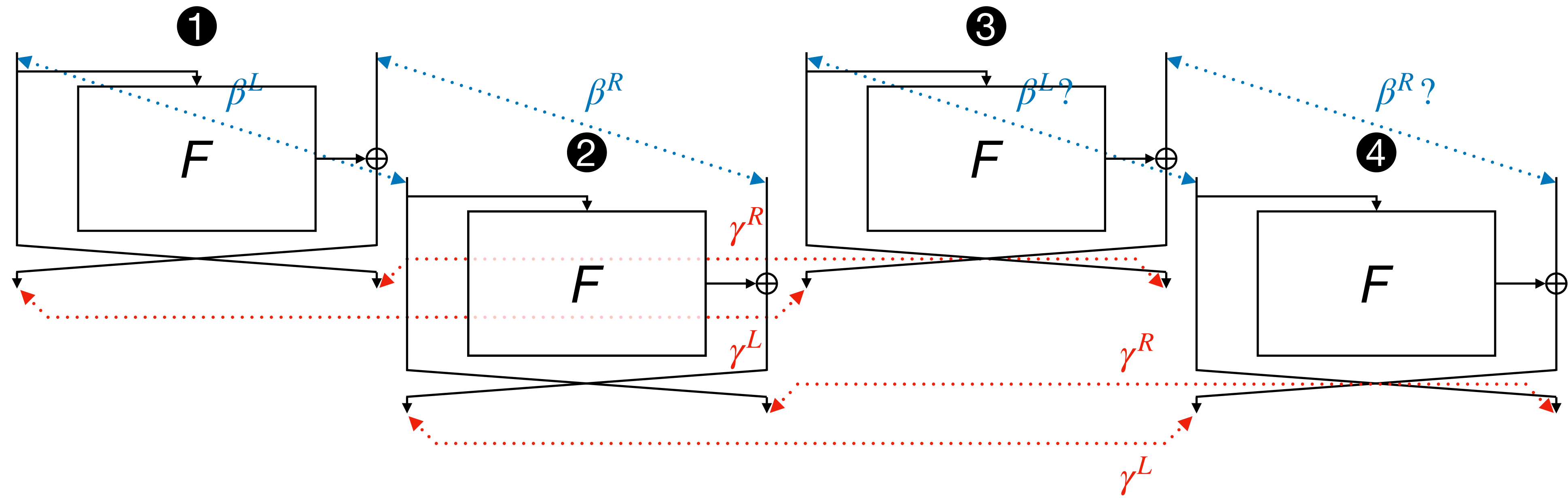
The FBCT



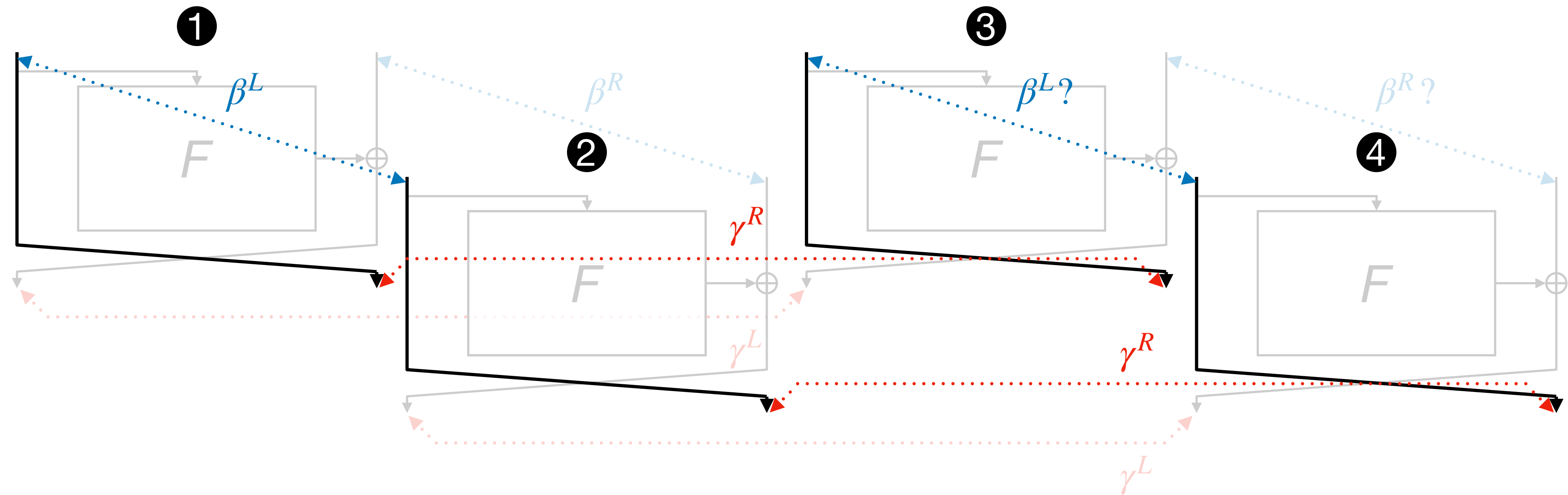
The FBCT



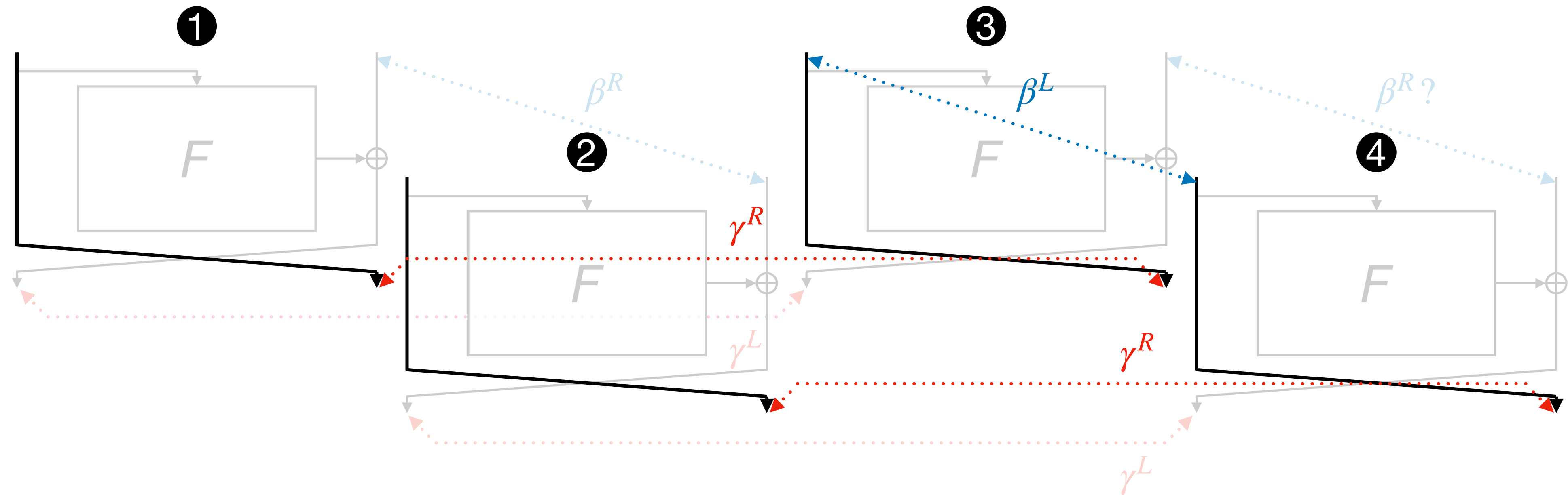
The FBCT



The FBCT (left part)

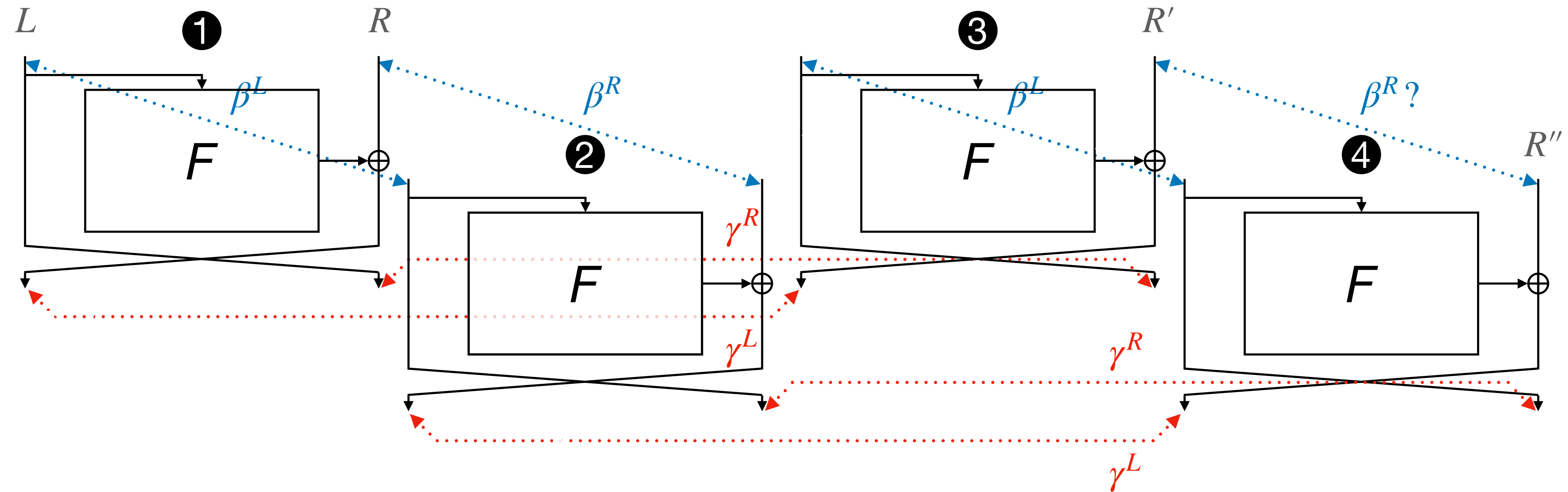


The FBCT (left part)



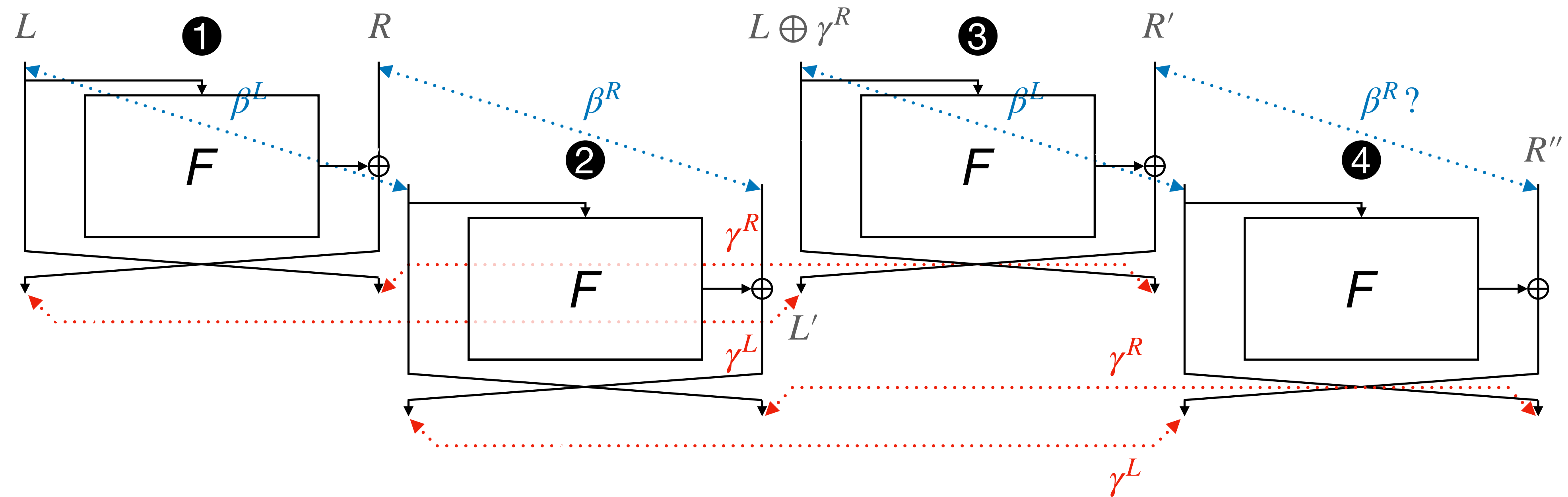
The left part of the difference comes for free.

The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

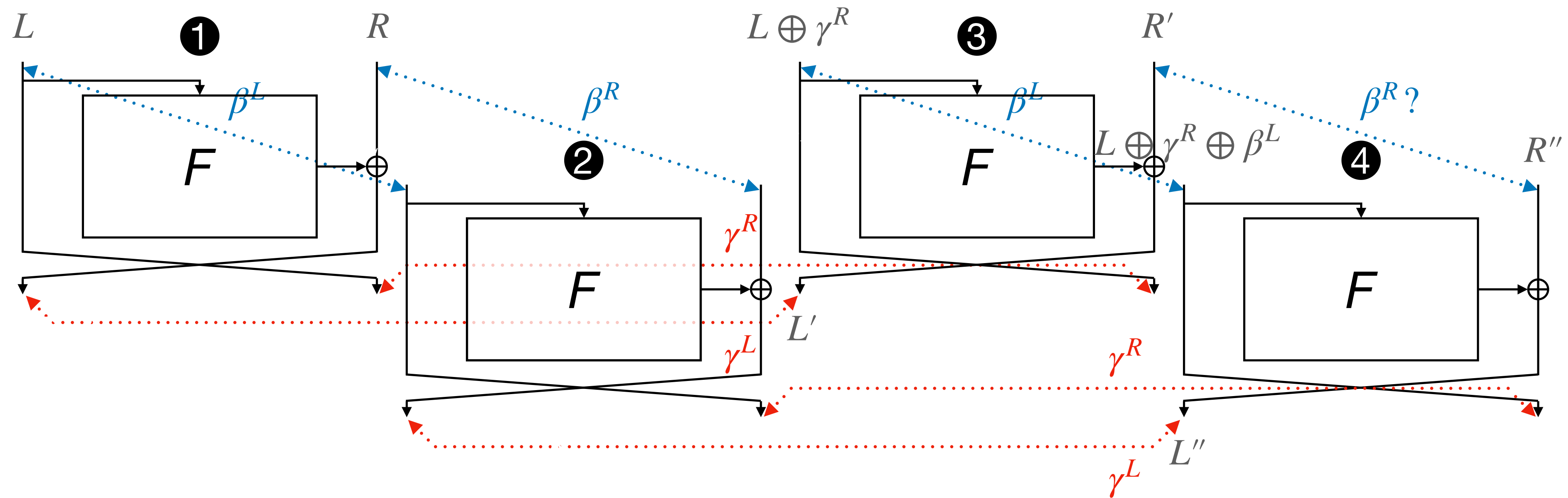
The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

$$R' \oplus R'' = F(L \oplus \gamma^R) \oplus L' \oplus R''$$

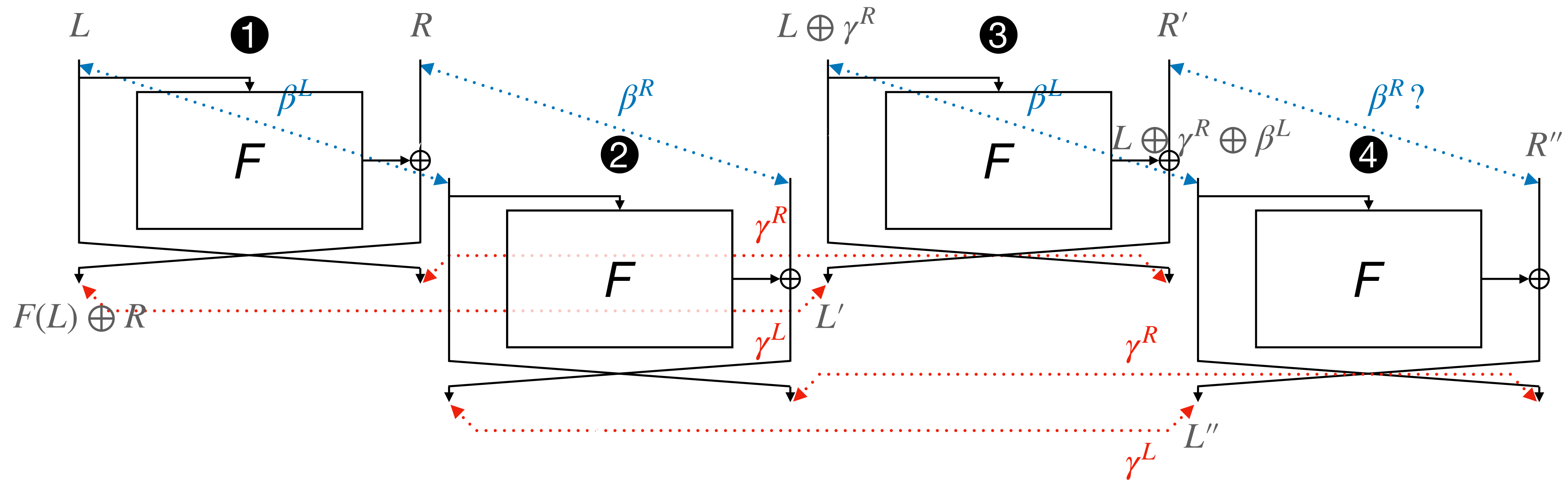
The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

$$R' \oplus R'' = F(L \oplus \gamma^R) \oplus L' \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus L''$$

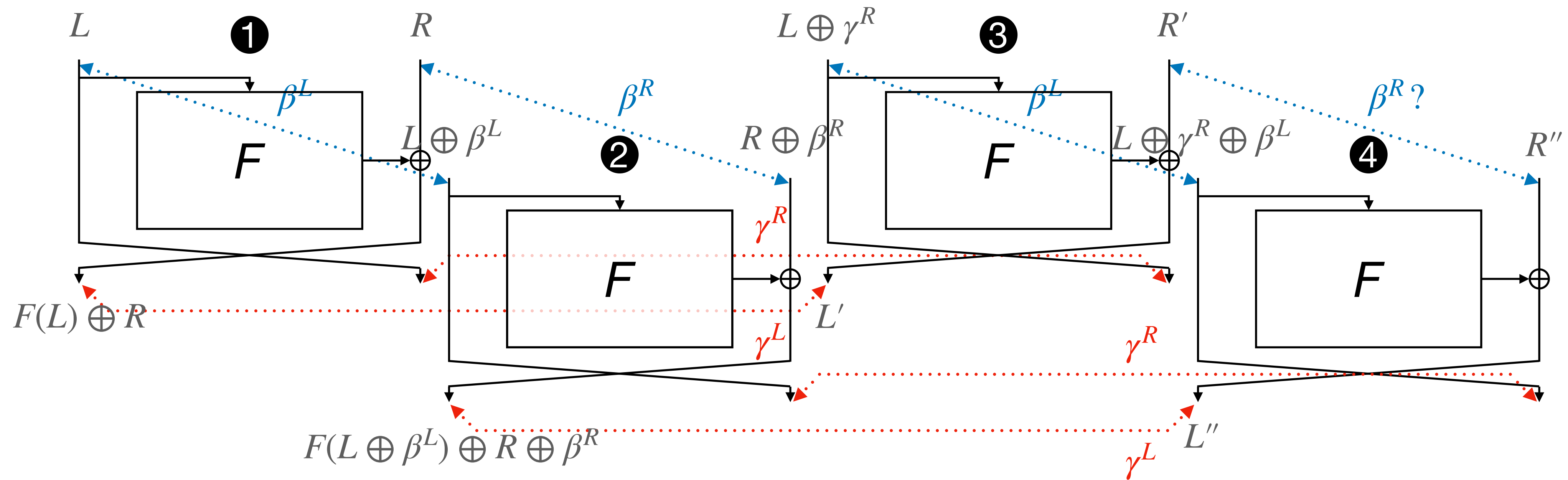
The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

$$R' \oplus R'' = F(L \oplus \gamma^R) \oplus F(L) \oplus R \oplus \gamma^L \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus L''$$

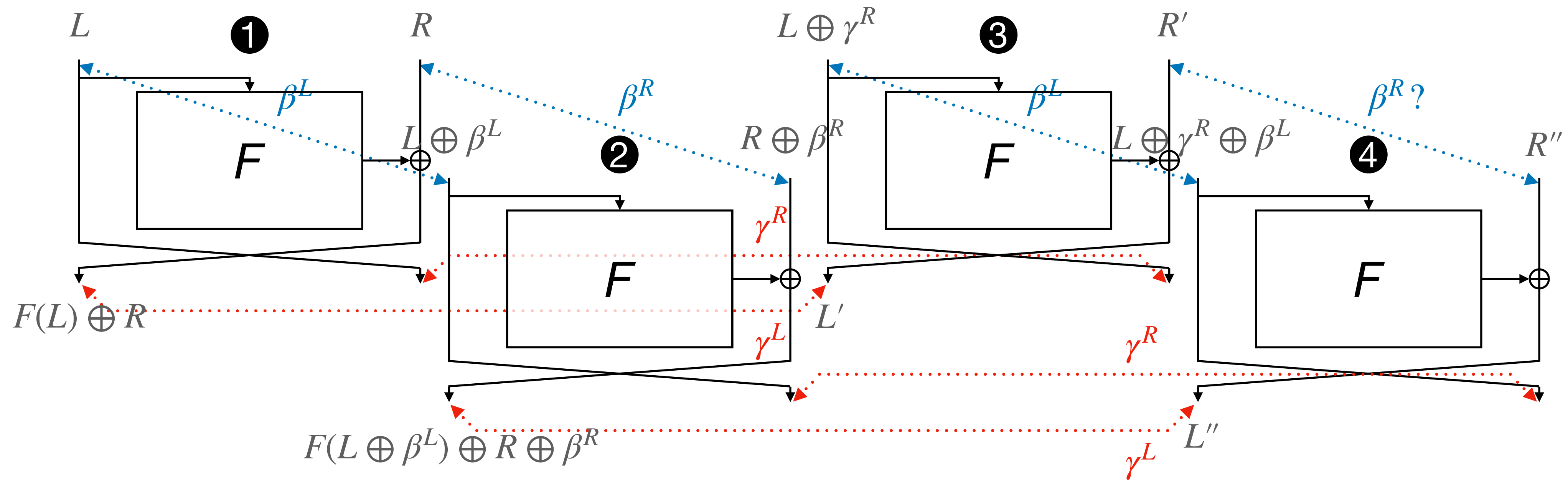
The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

$$R' \oplus R'' = F(L \oplus \gamma^R) \oplus \cancel{F(L) \oplus R \oplus \gamma^L} \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus F(L \oplus \beta^L) \oplus \cancel{R \oplus \beta^R} \oplus \cancel{\gamma^L}$$

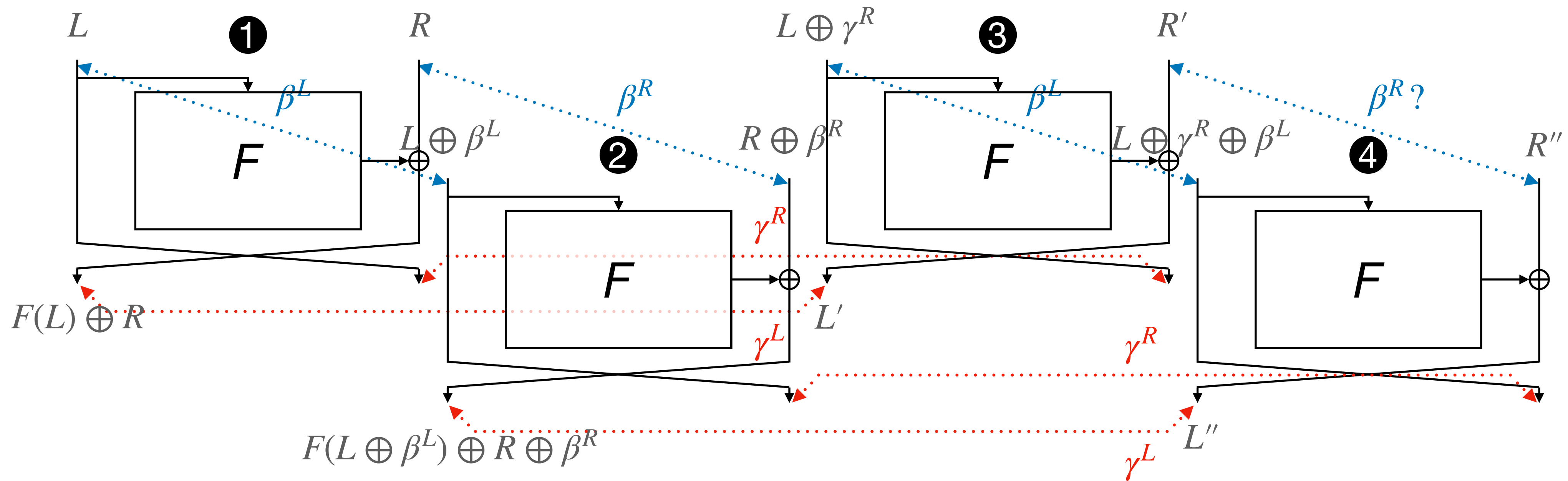
The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

$$R' \oplus R'' = F(L \oplus \gamma^R) \oplus F(L) \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus F(L \oplus \beta^L) \oplus \beta^R$$

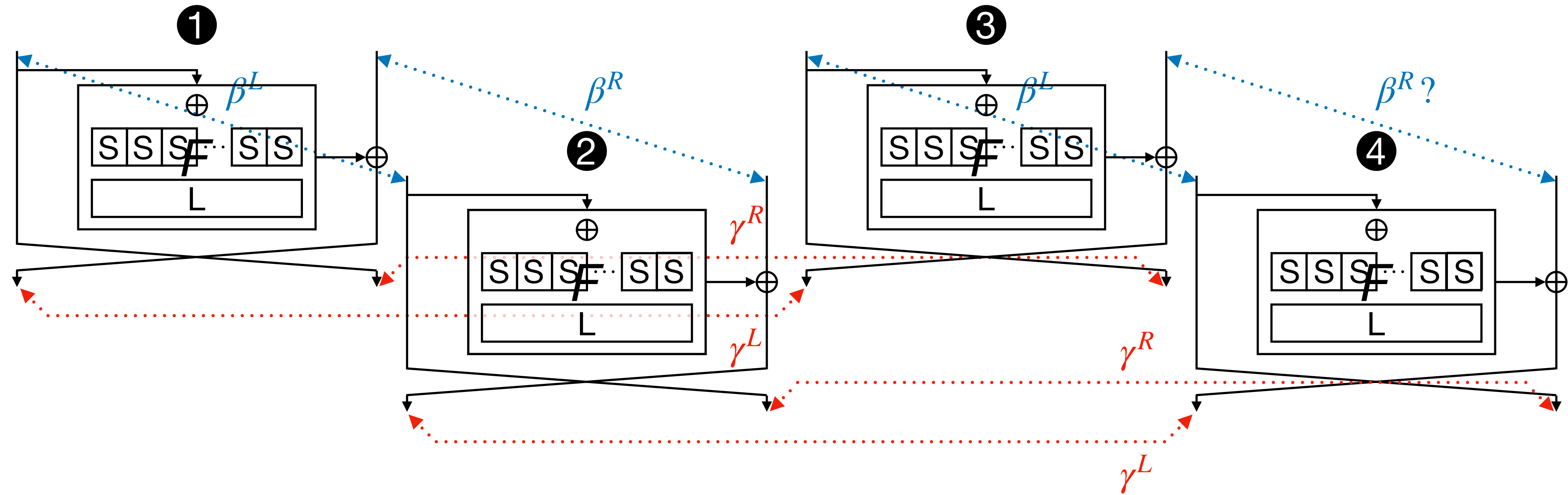
The FBCT (right part)



We want that $R' \oplus R'' = \beta^R$

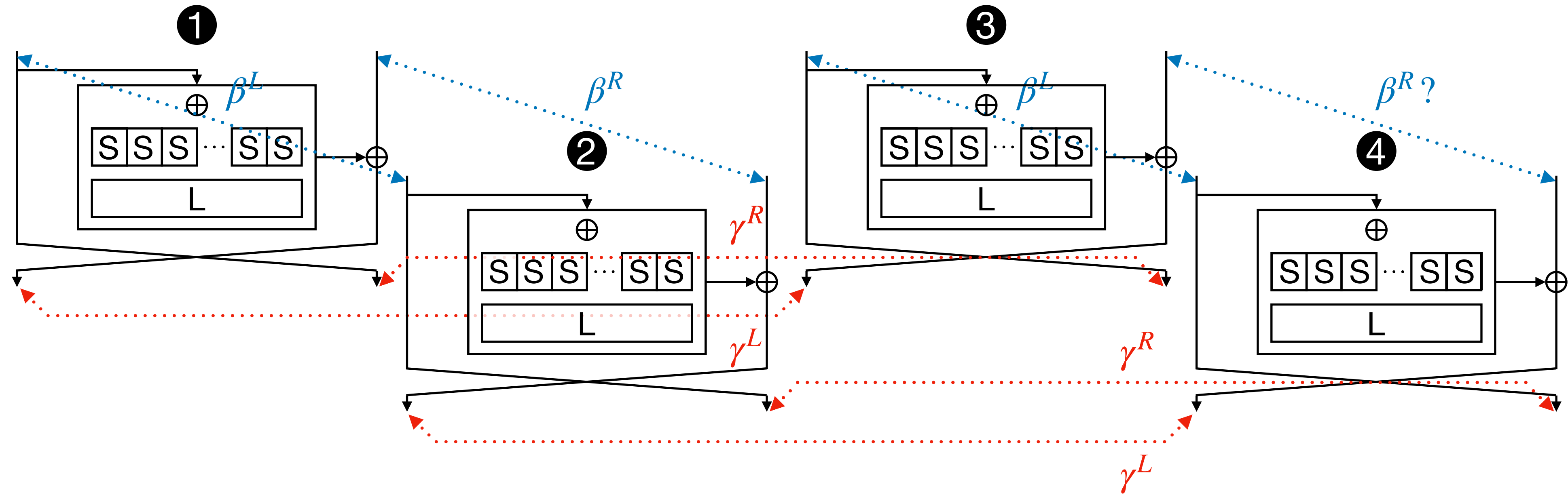
$$R' \oplus R'' = \underbrace{F(L \oplus \gamma^R) \oplus F(L) \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus F(L \oplus \beta^L)}_0 \oplus \beta^R$$

The FBCT (right part)



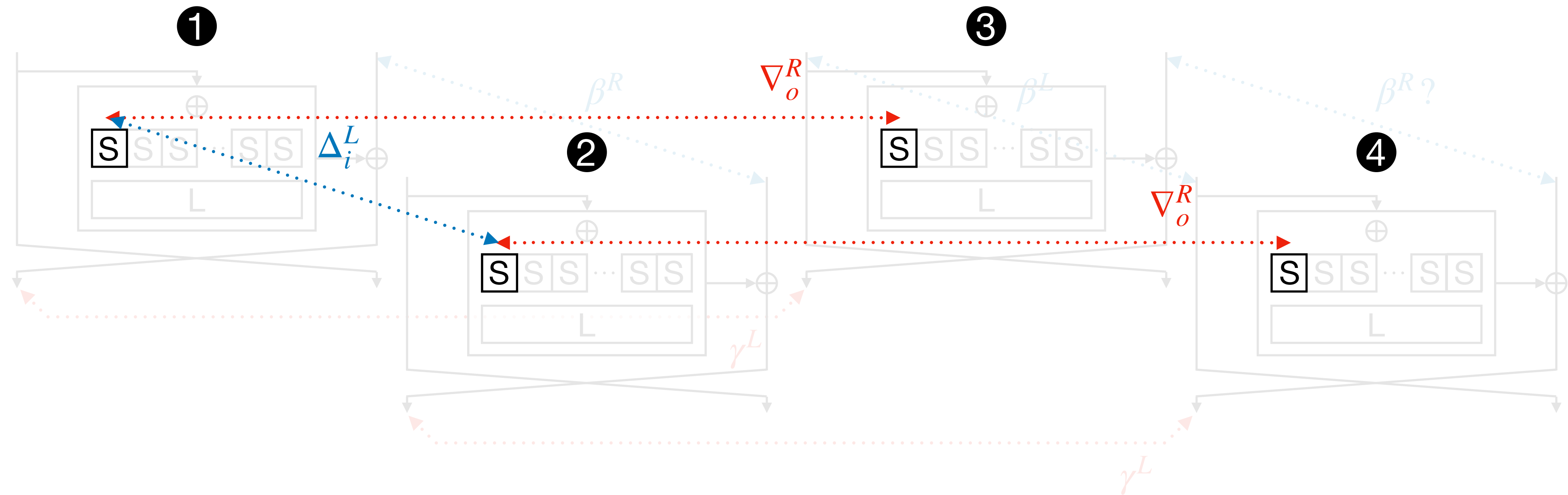
$$F(L \oplus \gamma^R) \oplus F(L) \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus F(L \oplus \beta^L) = 0$$

The FBCT (right part)



$$F(L \oplus \gamma^R) \oplus F(L) \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus F(L \oplus \beta^L) = 0$$

The FBCT (right part)



$$F(L \oplus \gamma^R) \oplus F(L) \oplus F(L \oplus \gamma^R \oplus \beta^L) \oplus F(L \oplus \beta^L) = 0$$

$$S(x \oplus \nabla_o^R) \oplus S(x) \oplus S(x \oplus \nabla_o^R \oplus \Delta_i^L) \oplus S(x \oplus \Delta_i^L) = 0$$

second derivative canceling out

Properties of the FBCT

$$\text{FBCT}_S(\Delta_i, \nabla_o) = \#\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0\}$$

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

Properties of the FBCT

$$\text{FBCT}_S(\Delta_i, \nabla_o) = \#\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0\}$$

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

Symmetry: $\text{FBCT}(\Delta_i, \nabla_o) = \text{FBCT}(\nabla_o, \Delta_i)$

Diagonal: $\text{FBCT}(\Delta_i, \Delta_i) = 2^n$

Multiplicity: $\text{FBCT}(\Delta_i, \nabla_o) \equiv 0 \pmod{4}$

Equalities: $\text{FBCT}(\Delta_i, \nabla_o) = \text{FBCT}(\Delta_i, \Delta_i \oplus \nabla_o)$

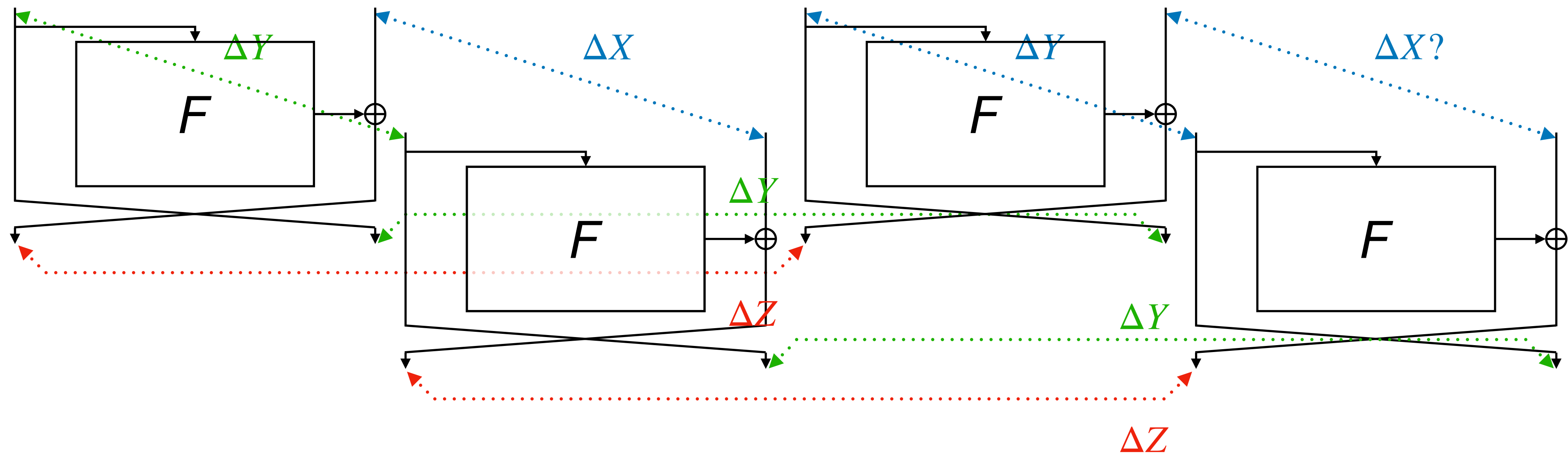
The Feistel switch

"Surprisingly, a Feistel round with an **arbitrary function** (e.g., an S-box) can be passed for **free** [...] Suppose the internal state (X, Y) is transformed to $(Z = X \oplus f(Y), Y)$ at the end of E_0 . Suppose also that the E_0 difference before this transformation is $(\Delta X, \Delta Y)$, and that the E_1 difference after this transformation is $(\Delta Z, \Delta Y)$ [...] **the decryption phase of the boomerang creates the difference ΔX in X at the end of E_0 “for free”.**"

 [Related-key Cryptanalysis of the Full AES-192 and AES-256](#)
Biryukov & Khovratovich, *ASIACRYPT 2009*

The Feistel switch

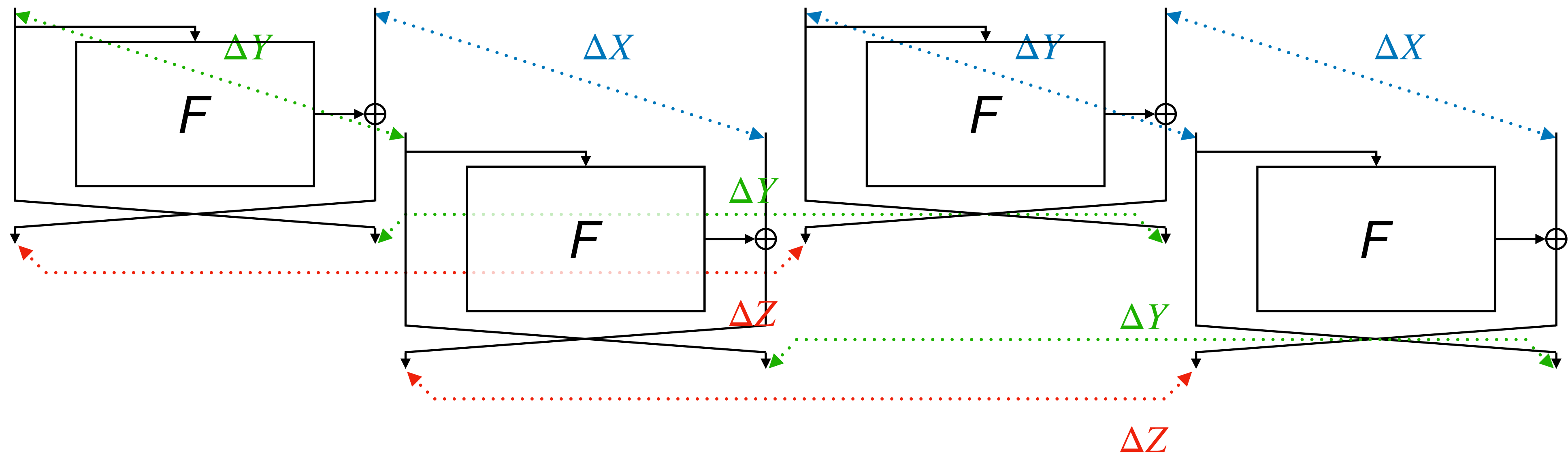
"Surprisingly, a Feistel round with an **arbitrary function** (e.g., an S-box) can be passed for **free** [...] Suppose the internal state (X, Y) is transformed to $(Z = X \oplus f(Y), Y)$ at the end of E_0 . Suppose also that the E_0 difference before this transformation is $(\Delta X, \Delta Y)$, and that the E_1 difference after this transformation is $(\Delta Z, \Delta Y)$ [...] **the decryption phase of the boomerang creates the difference ΔX in X at the end of E_0 "for free".**"



$$F(x \oplus \gamma^R) \oplus F(x) \oplus F(x \oplus \gamma^R \oplus \beta^L) \oplus F(x \oplus \beta^L) = 0$$

The Feistel switch

"Surprisingly, a Feistel round with an **arbitrary function** (e.g., an S-box) can be passed for **free** [...] Suppose the internal state (X, Y) is transformed to $(Z = X \oplus f(Y), Y)$ at the end of E_0 . Suppose also that the E_0 difference before this transformation is $(\Delta X, \Delta Y)$, and that the E_1 difference after this transformation is $(\Delta Z, \Delta Y)$ [...] **the decryption phase of the boomerang creates the difference ΔX in X at the end of E_0 "for free".**"



$$F(x \oplus \gamma^R) \oplus F(x) \oplus F(x \oplus \gamma^R \oplus \beta^L) \oplus F(x \oplus \beta^L) = 0, \text{ with } \gamma^R = \beta^L = \Delta Y$$

The Feistel switch

"Surprisingly, a Feistel round with an **arbitrary function** (e.g., an S-box) can be passed for **free** [...] Suppose the internal state (X, Y) is transformed to $(Z = X \oplus f(Y), Y)$ at the end of E_0 . Suppose also that the E_0 difference before this transformation is $(\Delta X, \Delta Y)$, and that the E_1 difference after this transformation is $(\Delta Z, \Delta Y)$ [...] **the decryption phase of the boomerang creates the difference ΔX in X at the end of E_0 "for free".**"

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

Properties of the FBCT

Theorem

S is APN if and only if its FBCT verifies $\text{FBCT}(\Delta_i, \nabla_o) = 0 \quad \forall 1 \leq \Delta_i \neq \nabla_o \leq 2^n - 1$

Properties of the FBCT

Theorem

S is APN if and only if its FBCT verifies $\text{FBCT}(\Delta_i, \nabla_o) = 0 \forall 1 \leq \Delta_i \neq \nabla_o \leq 2^n - 1$

e.g. $S = [1, 3, 6, 5, 2, 4, 7, 0]$

8	0	0	0	0	0	0	0
0	0	2	2	0	0	2	2
0	0	0	0	2	2	2	2
0	0	2	2	2	2	0	0
0	2	0	2	0	2	0	2
0	2	2	0	0	2	2	0
0	2	0	2	2	0	2	0
0	2	0	0	2	0	0	2

DDT

8	8	8	8	8	8	8	8
8	8	0	0	0	0	0	0
8	0	8	0	0	0	0	0
8	0	0	8	0	0	0	0
8	0	0	0	8	0	0	0
8	0	0	0	0	8	0	0
8	0	0	0	0	0	8	0
8	0	0	0	0	0	0	8

FBCT

8	8	8	8	8	8	8	8
8	0	2	2	0	0	2	2
8	0	0	0	2	2	2	2
8	0	2	2	2	2	0	0
8	2	0	2	0	2	0	2
8	2	2	0	0	2	2	0
8	2	0	2	2	0	2	0
8	2	0	0	2	0	0	2

BCT

Comparing the BCT and the FBCT

Boomerang uniformity for the **SPN** case:

$$\max_{\Delta_i \neq 0, \nabla_o \neq 0} BCT(\Delta_i, \nabla_o)$$

 [On the Boomerang Uniformity of Cryptographic Sboxes](#)
Boura & Canteaut, *ToSC 2018*

Comparing the BCT and the FBCT

Boomerang uniformity for the **SPN** case:

$$\max_{\Delta_i \neq 0, \nabla_o \neq 0} BCT(\Delta_i, \nabla_o)$$

Boomerang uniformity for the **Feistel** case:

$$\max_{\Delta_i \neq 0, \nabla_o \neq 0, \Delta_i \neq \nabla_o} FBCT(\Delta_i, \nabla_o)$$

Comparing the BCT and the FBCT

Boomerang uniformity for the **SPN** case:

$$\max_{\Delta_i \neq 0, \nabla_o \neq 0} BCT(\Delta_i, \nabla_o)$$

Boomerang uniformity for the **Feistel** case:

$$\max_{\Delta_i \neq 0, \nabla_o \neq 0, \Delta_i \neq \nabla_o} FBCT(\Delta_i, \nabla_o)$$

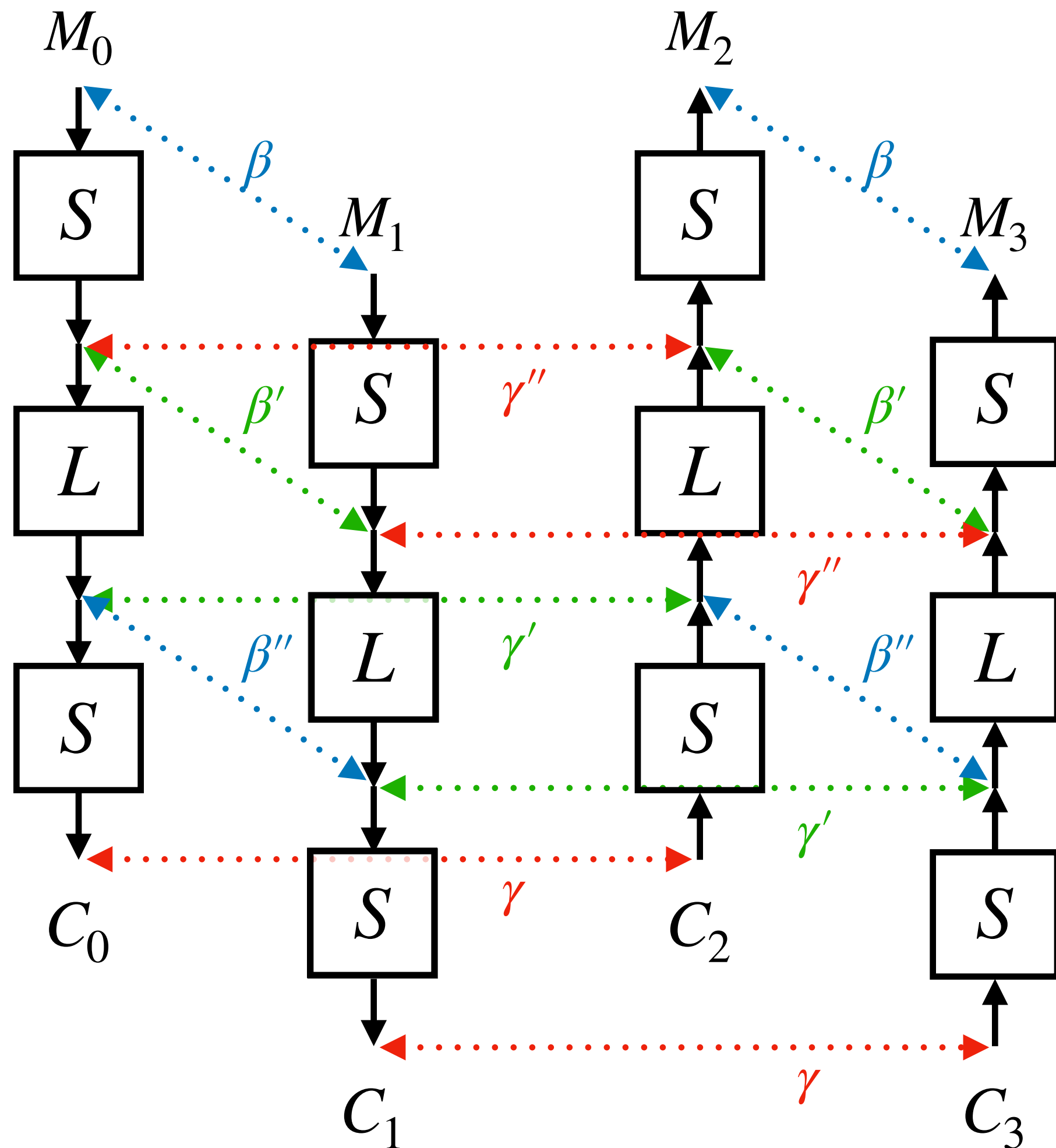
Boomerang uniformity preserved under	BCT	FBCT
Affine equivalence	✓	✓
Extended-affine equivalence	✗	✓
CCZ equivalence	✗	✗
Inversion (if S is invertible)	✓	✗

A good S-box for an SPN is a good S-box for a Feistel regarding many usual criteria (**differential, linear, algebraic degree**)

But its behavior can be different regarding boomerang switches if we use it in an SPN or a Feistel.

Boomerang switches over more rounds

Two-round case



 [Boomerang Switch in Multiple Rounds](#)

Wang & Peyrin, *ToSC 2019*

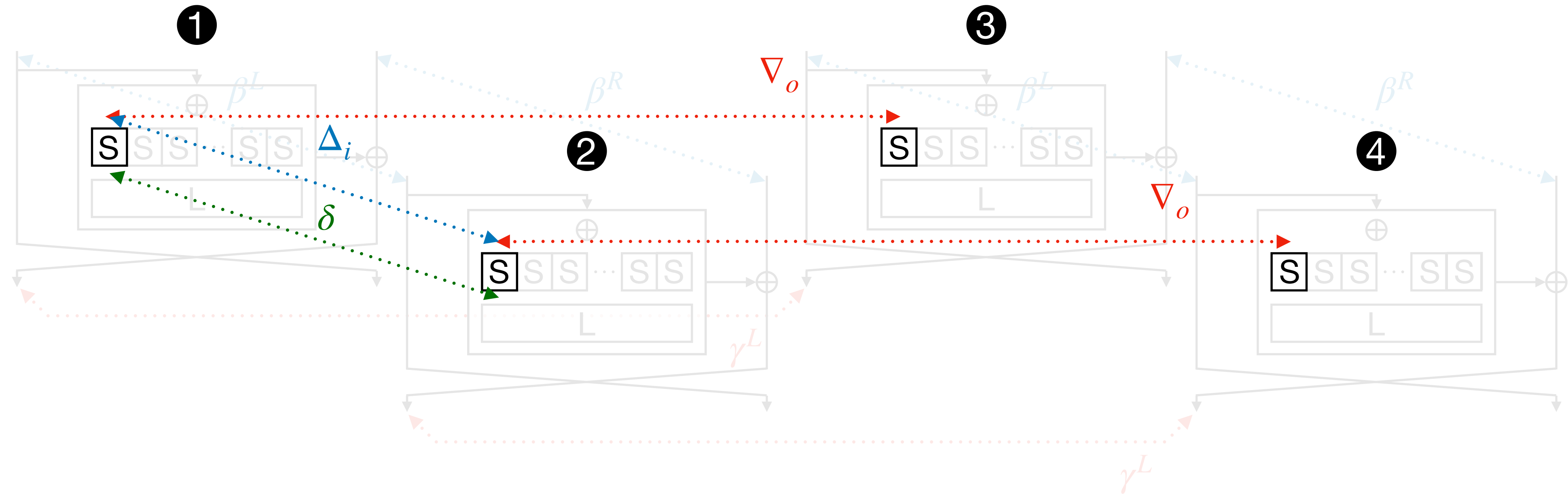
 [Boomerang Connectivity Table Revisited. Application to SKINNY and AES](#)

Song, Qin & Hu, *ToSC 2019*

$$BDT(\beta, \beta', \gamma'') = \#\{x \mid S^{-1}(S(x) \oplus \gamma'') \oplus S^{-1}(S(x \oplus \beta) \oplus \gamma'') = \beta, \\ S(x) \oplus S(x \oplus \beta) = \beta'\}$$

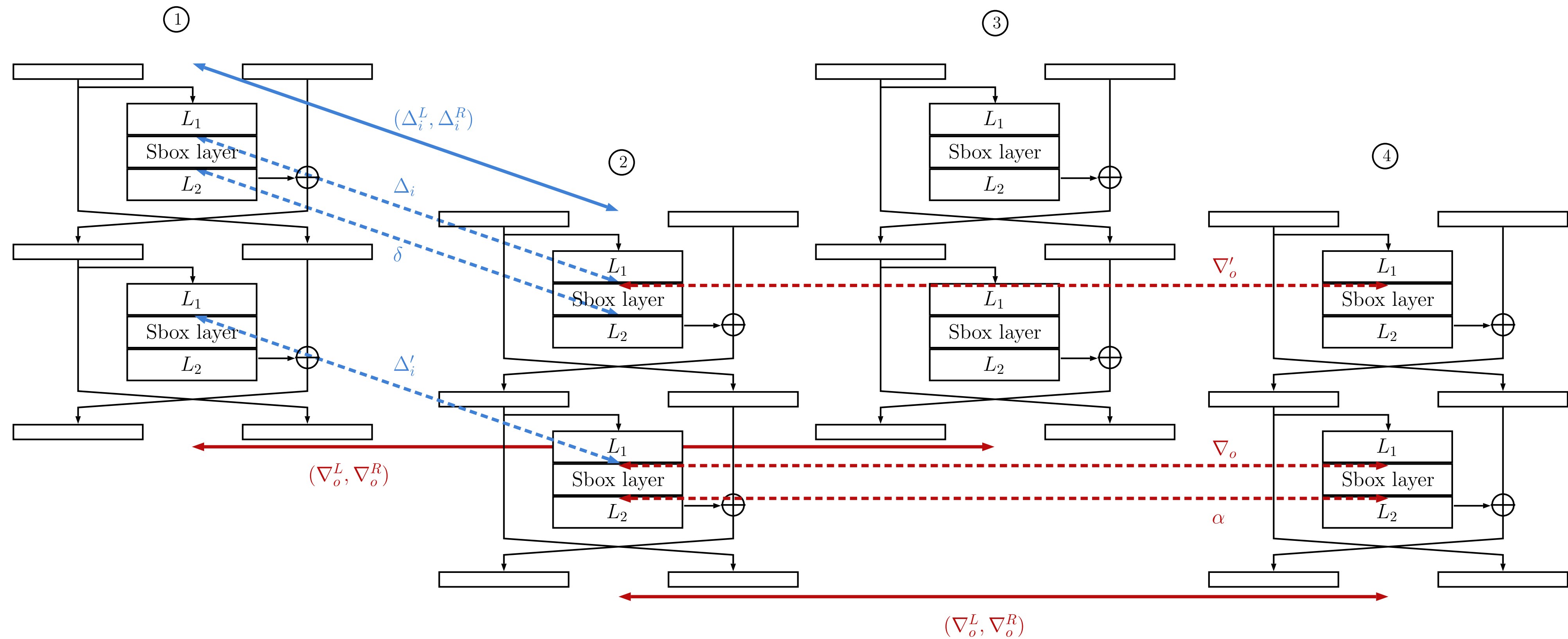
$$BDT'(\gamma, \gamma', \beta'') = \#\{x \mid S(S^{-1}(x) \oplus \beta'') \oplus S(S^{-1}(x \oplus \gamma) \oplus \beta'') = \gamma, \\ S^{-1}(x) \oplus S^{-1}(x \oplus \gamma) = \gamma'\}$$

Two-round case



$$FBDT(\Delta_i, \delta, \nabla_o) = \#\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0 \\ \text{and } S(x) \oplus S(x \oplus \Delta_i) = \delta\}$$

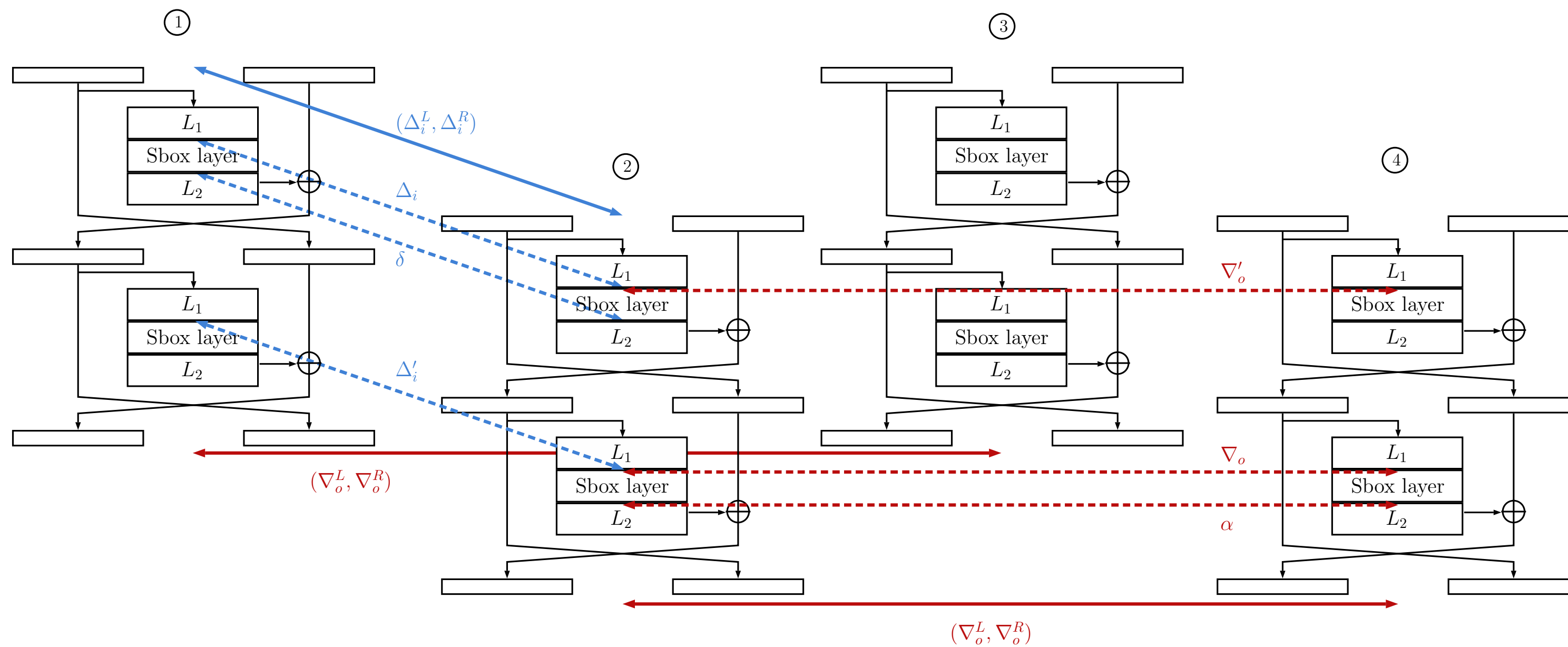
Two-round case



$$FBDT(\Delta_i, \delta, \nabla_o) = \#\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0$$

$$\text{and } S(x) \oplus S(x \oplus \Delta_i) = \delta\}$$

Two-round case

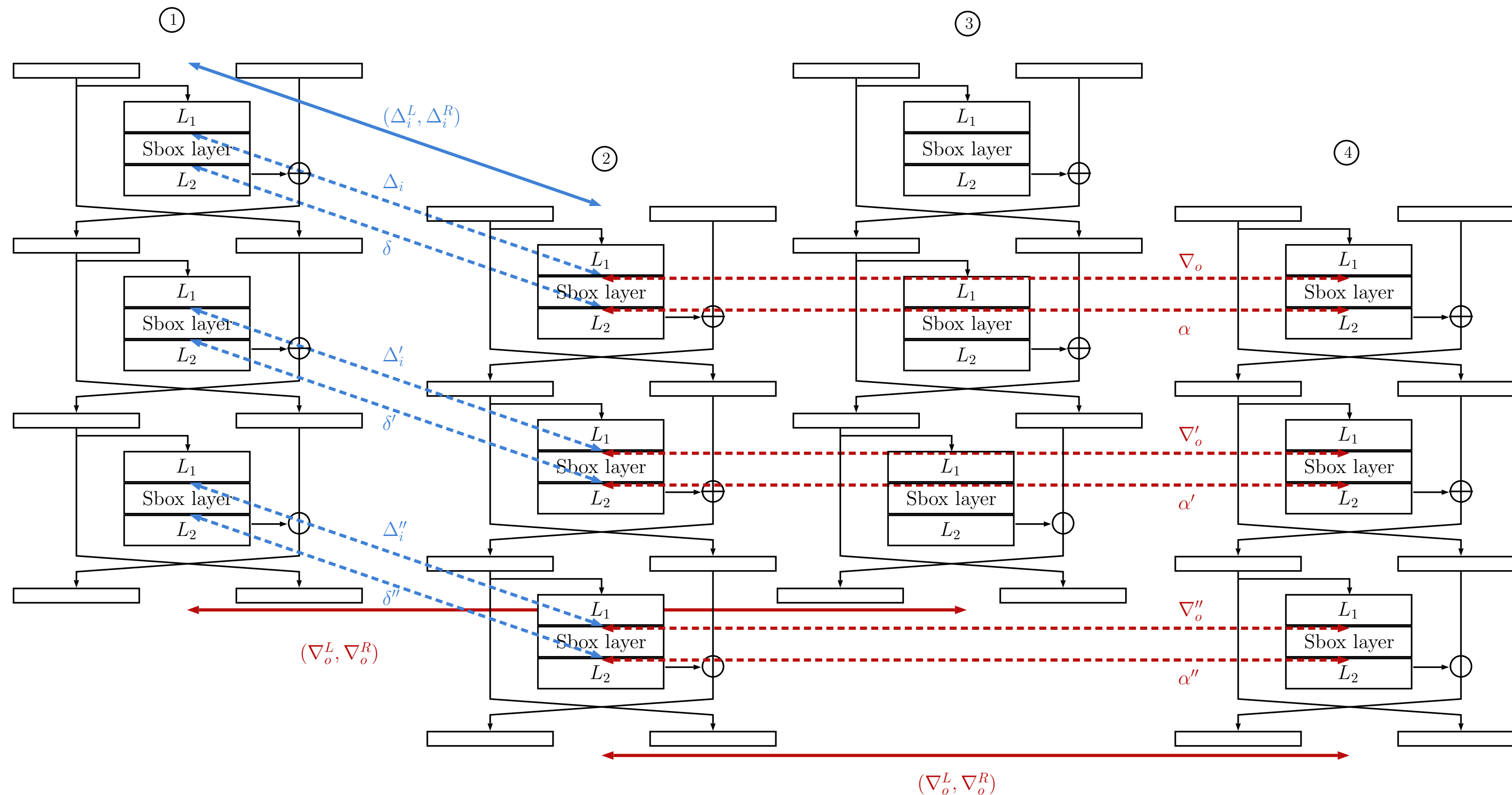


$$2^{-2tn} \times \sum_{0 \leq \delta, \alpha < 2^n} FBDT(\Delta_i, \delta, \nabla_o') \times FBDT(\nabla_o, \alpha, \Delta_i')$$

$$FBDT(\Delta_i, \delta, \nabla_o) = \#\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0$$

and $S(x) \oplus S(x \oplus \Delta_i) = \delta\}$

Switches over 3 rounds and more...



FBET table:

$$\#\{x \in \mathbb{F}_2^n \mid S(x) \oplus S(x \oplus \Delta_i) \oplus S(x \oplus \nabla_o) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = 0,$$

$$S(x) \oplus S(x \oplus \Delta_i) = \delta,$$

$$S(x \oplus \Delta_i) \oplus S(x \oplus \Delta_i \oplus \nabla_o) = \alpha\}$$

Conclusion

- Introduction of the **FBCT**, a new tool that:
 - easily evaluates the probability of a 1-round boomerang switch
 - gives a new criterion when choosing an S-box for a Feistel cipher
- Proposal of a **generic formula** for a switch over many rounds:
 - evaluation is computationally expensive if E_m covers many rounds with many active S-boxes
 - might be preferable to evaluate it experimentally

Thank you for your attention.