On Boomerang Attacks on Quadratic Feistel Ciphers

Xavier Bonnetain and Virginie Lallemand

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

FSE 2024

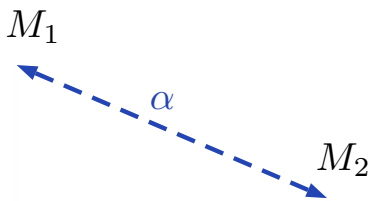
Boomerang Distinguishers

Differential Distinguisher

(α, β) so that $\quad E(M_1 + \alpha) + E(M_1) = \beta \quad$ with high probability

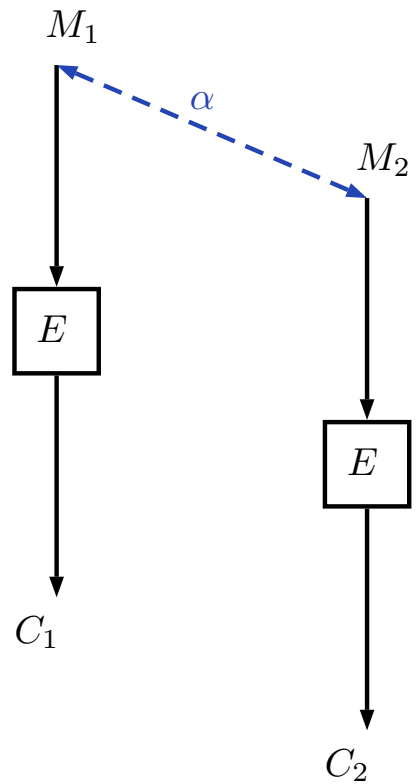
Differential Distinguisher

(α, β) so that $\quad E(M_1 + \alpha) + E(M_1) = \beta \quad$ with high probability



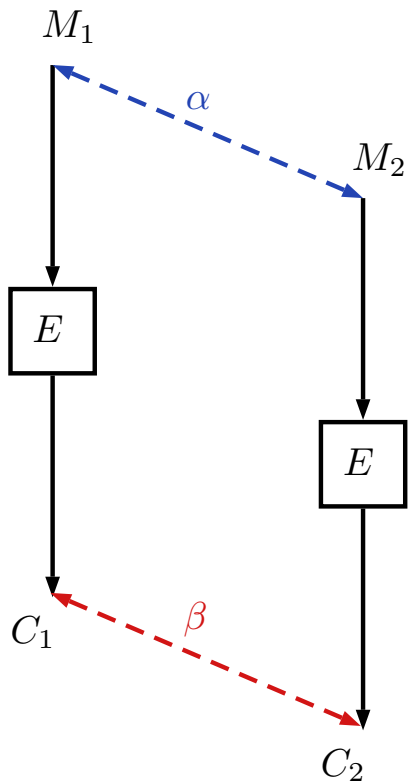
Differential Distinguisher

(α, β) so that $E(M_1 + \alpha) + E(M_1) = \beta$ with high probability



Differential Distinguisher

(α, β) so that $E(M_1 + \alpha) + E(M_1) = \beta$ with high probability

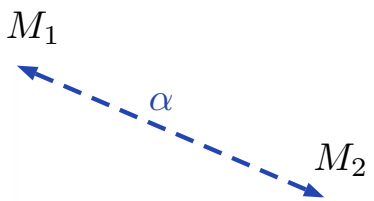


Boomerang Distinguisher

(α, δ) so that $E^{-1}(E(M_1)\oplus\delta)\oplus E^{-1}(E(M_1\oplus\alpha)\oplus\delta) = \alpha$ with high probability

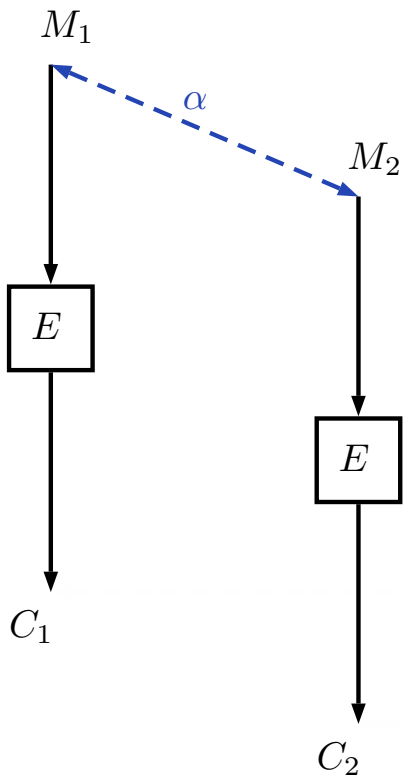
Boomerang Distinguisher

(α, δ) so that $E^{-1}(E(M_1)\oplus\delta)\oplus E^{-1}(E(M_1\oplus\alpha)\oplus\delta) = \alpha$ with high probability



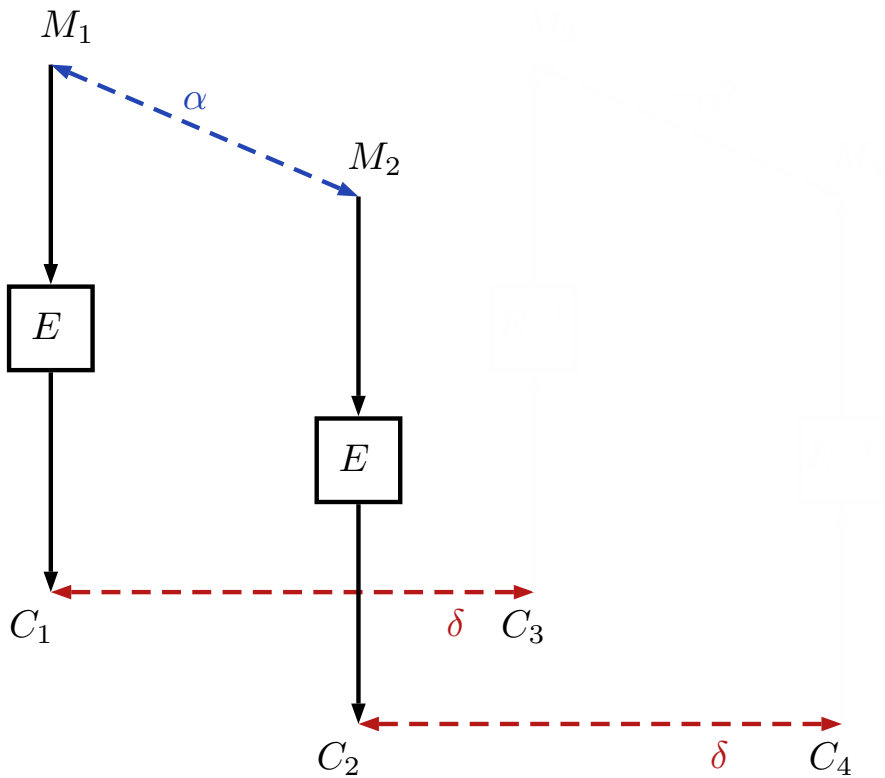
Boomerang Distinguisher

(α, δ) so that $E^{-1}(E(M_1)\oplus\delta)\oplus E^{-1}(E(M_1\oplus\alpha)\oplus\delta) = \alpha$ with high probability



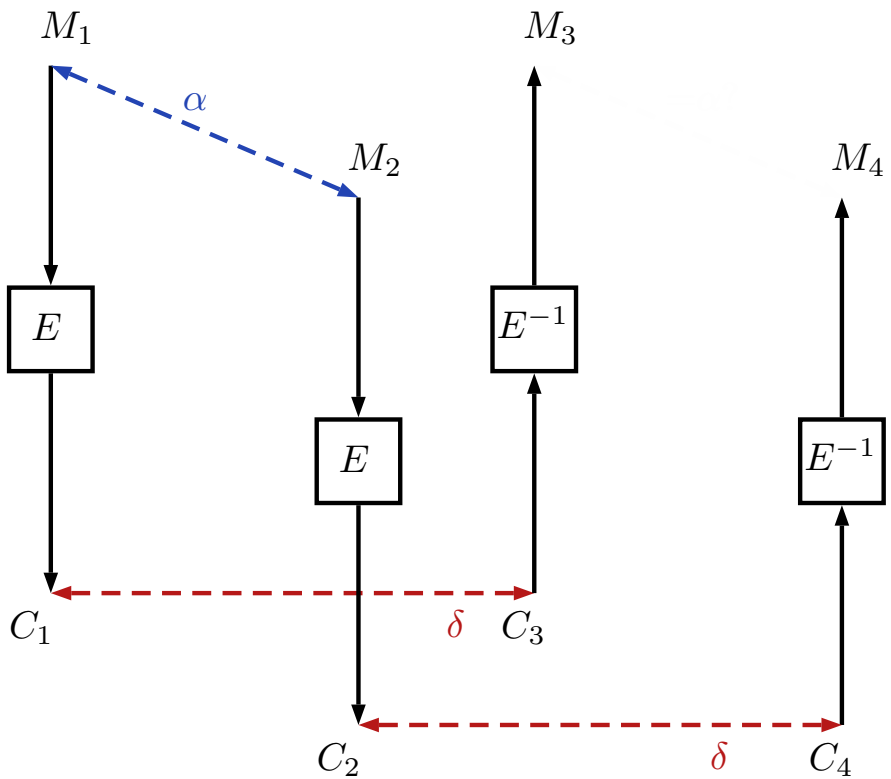
Boomerang Distinguisher

(α, δ) so that $E^{-1}(E(M_1)\oplus\delta)\oplus E^{-1}(E(M_1\oplus\alpha)\oplus\delta) = \alpha$ with high probability



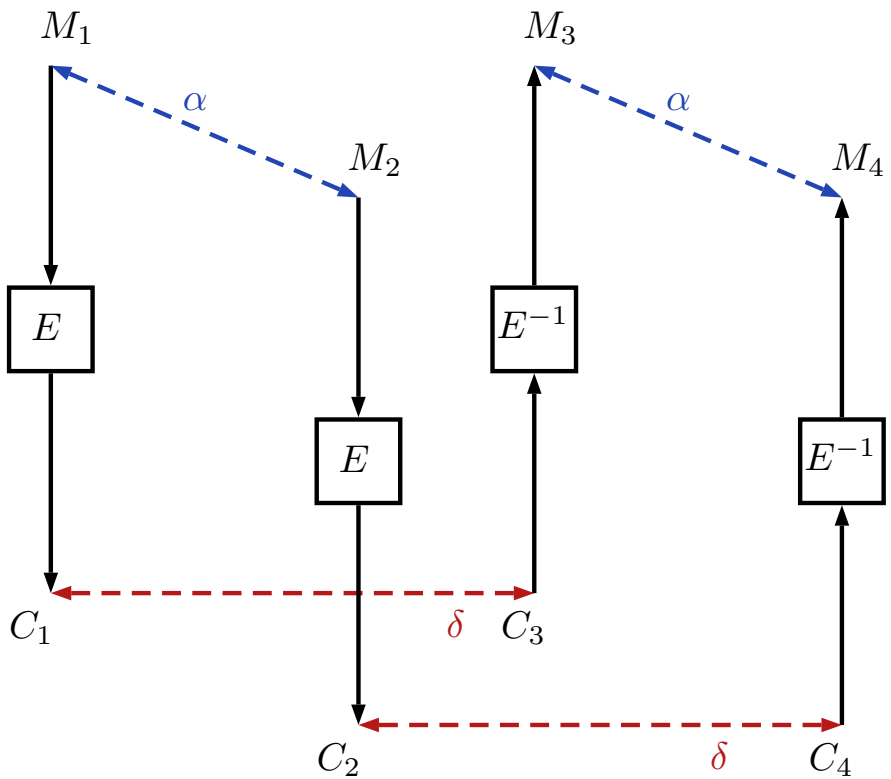
Boomerang Distinguisher

(α, δ) so that $E^{-1}(E(M_1)\oplus\delta)\oplus E^{-1}(E(M_1\oplus\alpha)\oplus\delta) = \alpha$ with high probability



Boomerang Distinguisher

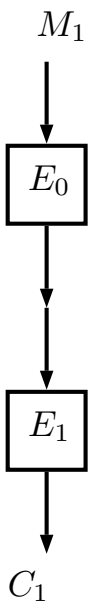
(α, δ) so that $E^{-1}(E(M_1)\oplus\delta)\oplus E^{-1}(E(M_1\oplus\alpha)\oplus\delta) = \alpha$ with high probability



Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

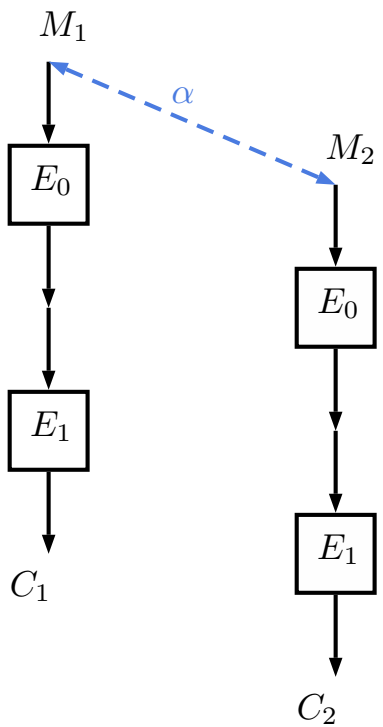
Probability:



Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

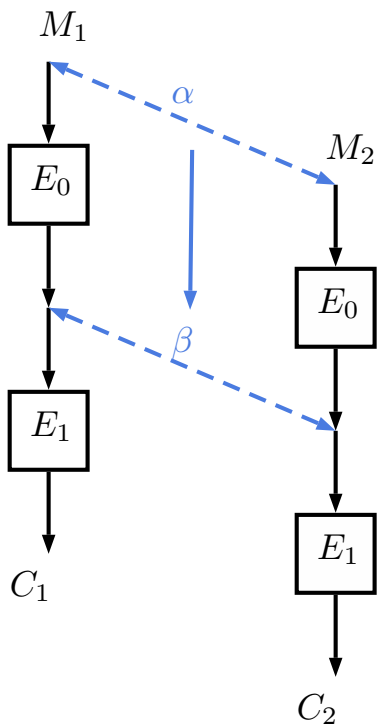


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

p

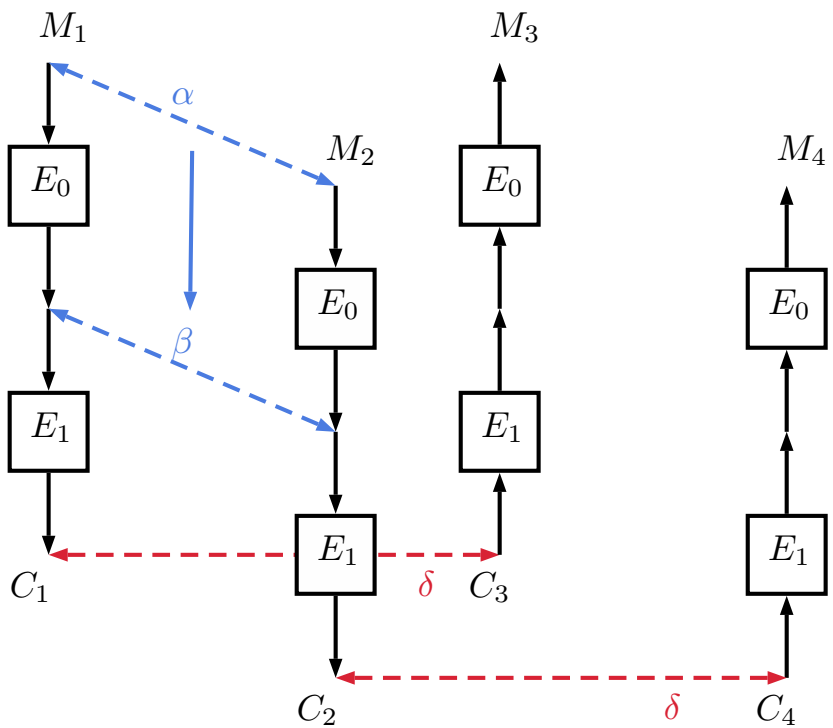


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

p

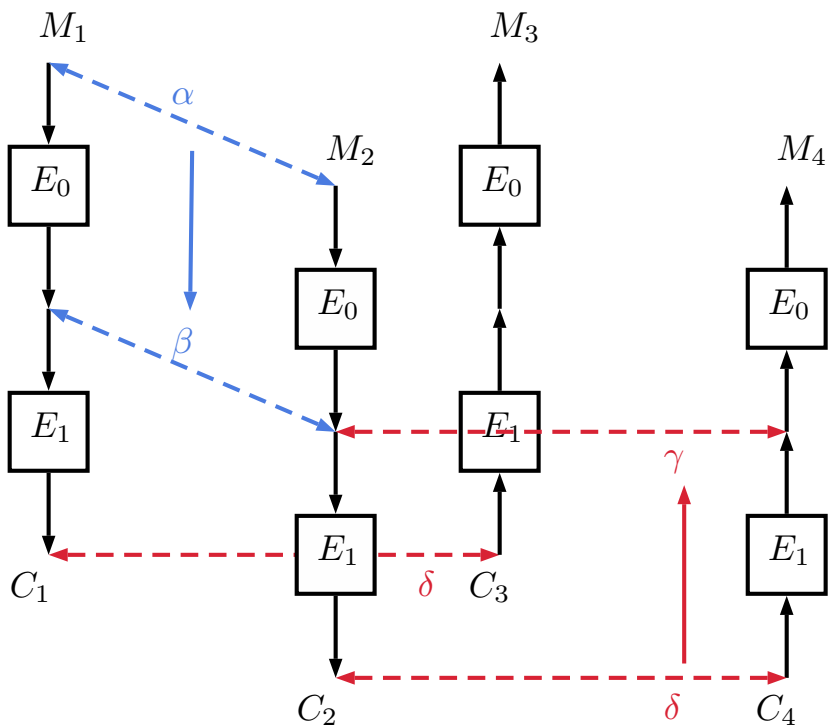


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

$p \times q$

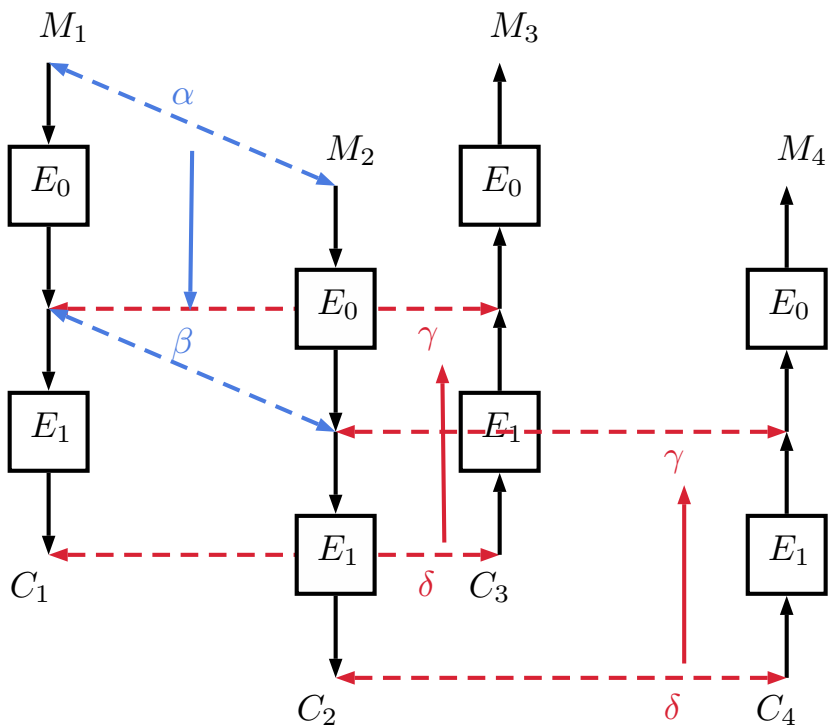


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

$p \times q \times q$

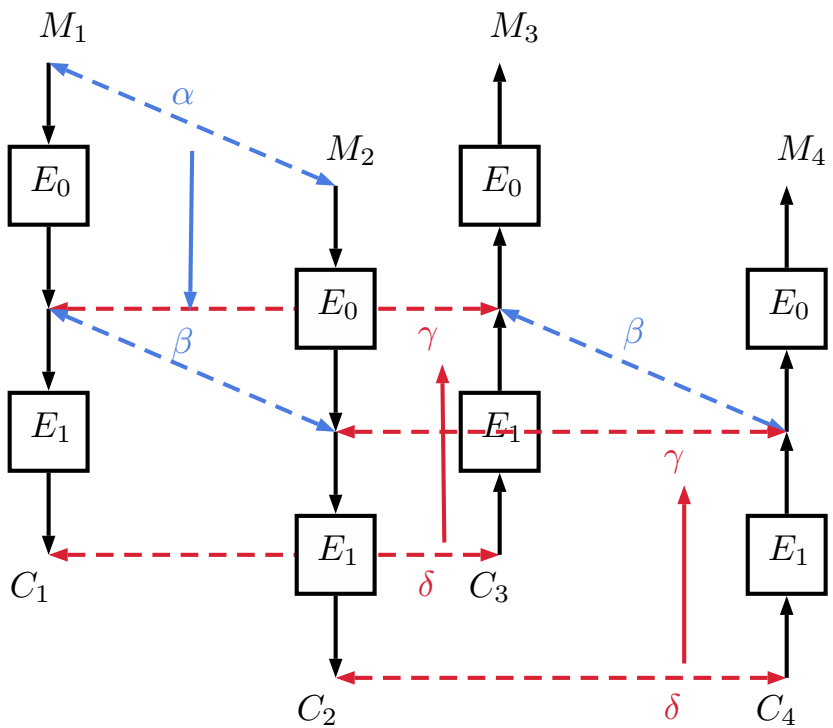


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

$p \times q \times q$

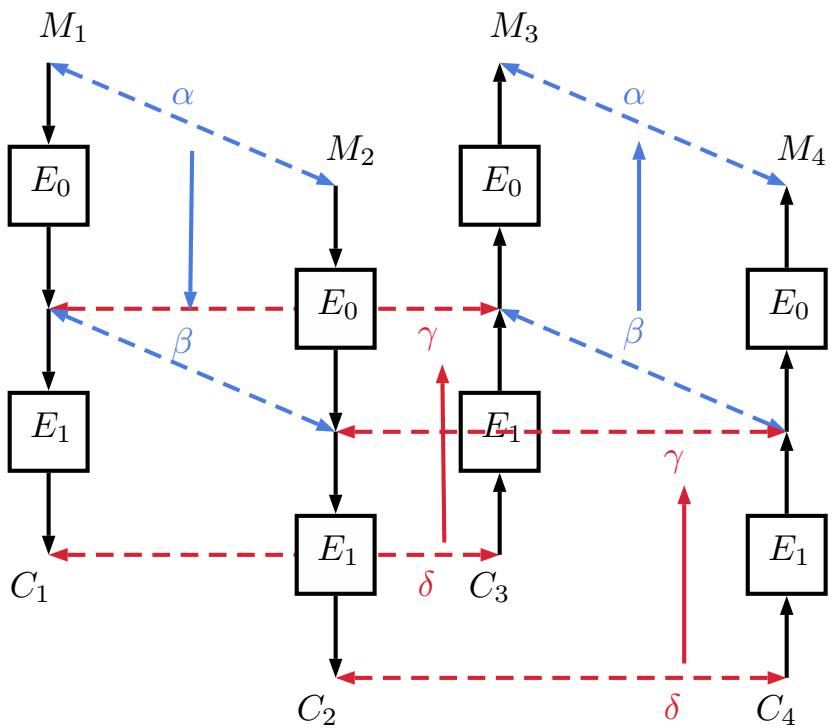


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

Probability:

$p \times q \times q \times p$

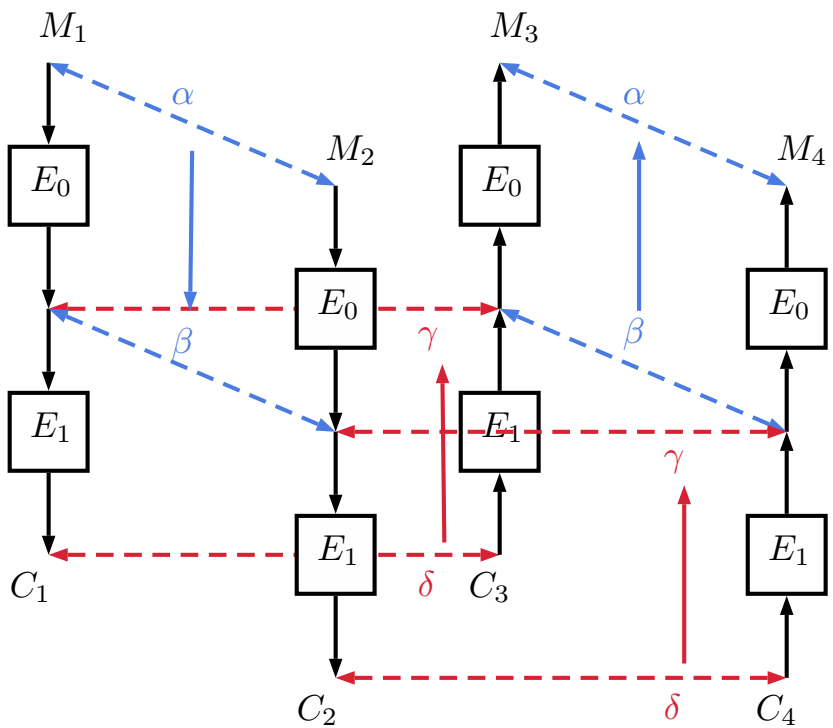


Building a Boomerang Distinguisher

- Rewrite $E = E_1 \circ E_0$
- Find good differentials:
  - $\mathbb{P}(\alpha \longrightarrow_{E_0} \beta) = p$
  - $\mathbb{P}(\gamma \longrightarrow_{E_1} \delta) = q$

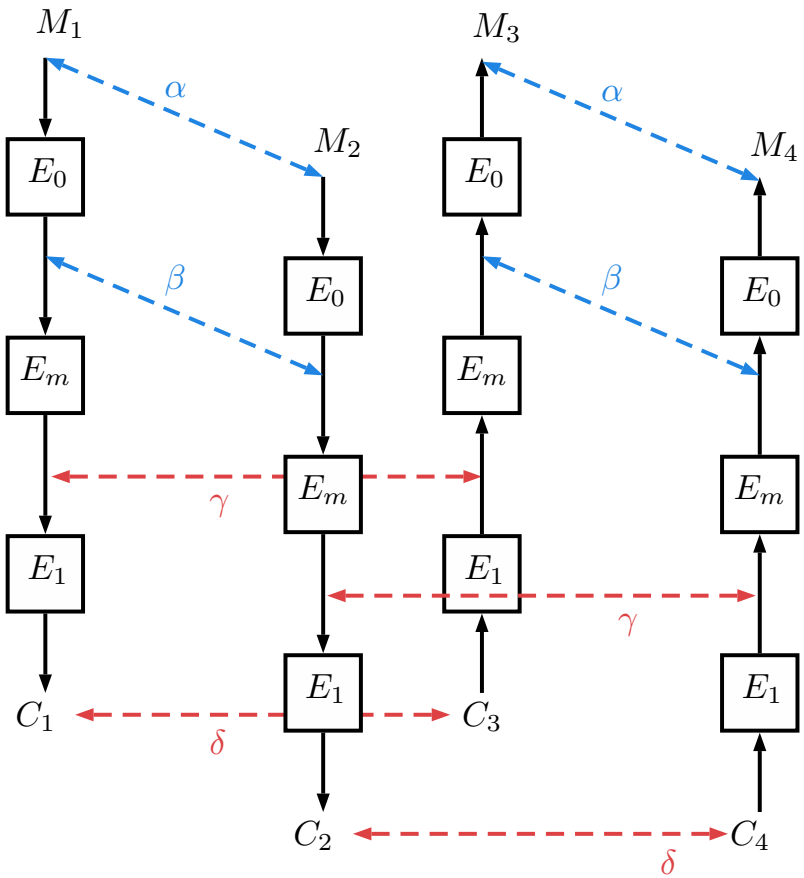
Probability:

$p \times q \times q \times p$



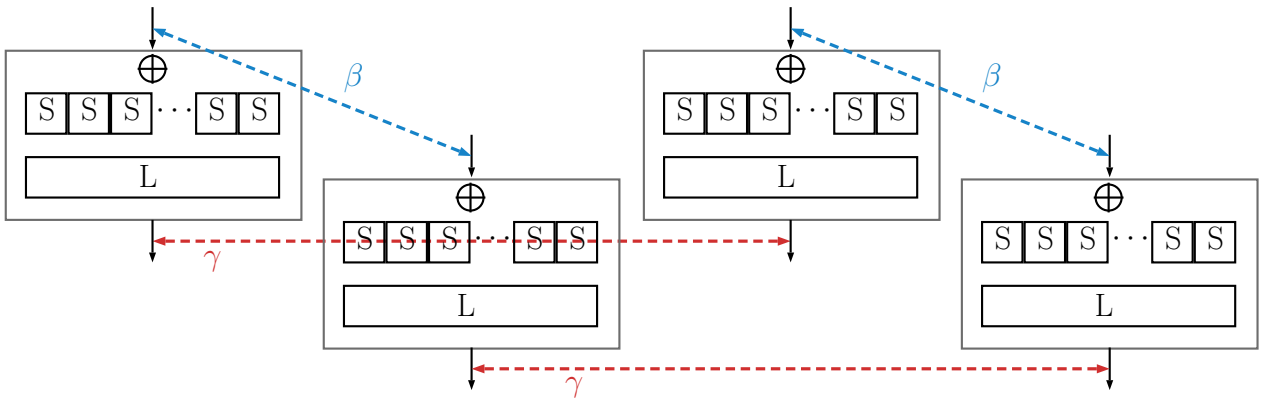
Expected probability of p^2q^2 if all the events are **independent**

Careful Handling of the Middle: the Sandwich Framework



- $E = E_1 \circ E_m \circ E_0$
- estimated probability $p^2 \times r \times q^2$
- $r = Pr[E_m^{-1}(E_m(x_1) \oplus \gamma) \oplus E_m^{-1}(E_m(x_1 \oplus \beta) \oplus \gamma) = \beta]$

BCT approach



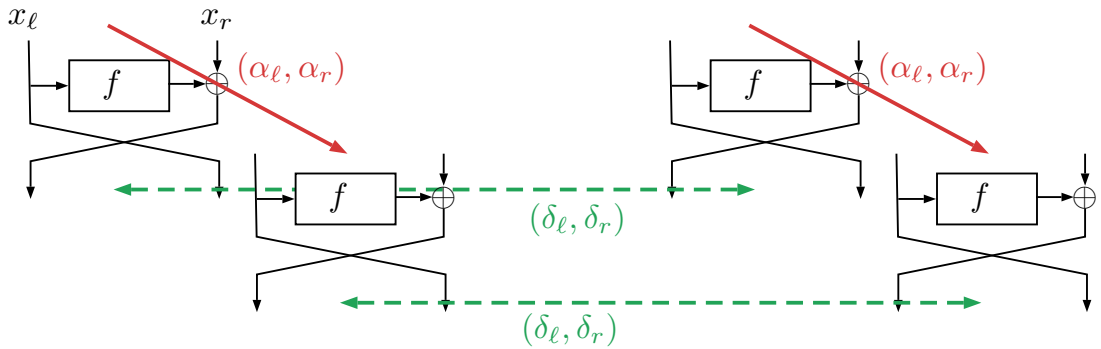
Systematic approach to compute boomerang probabilities for 1 round of SPN. Reduces to analyzing the Sbox.

Many variations:

- More rounds
- Different kind of cipher

Quadratic Feistel Boomerangs

Generic 1-round Boomerang on a Feistel cipher

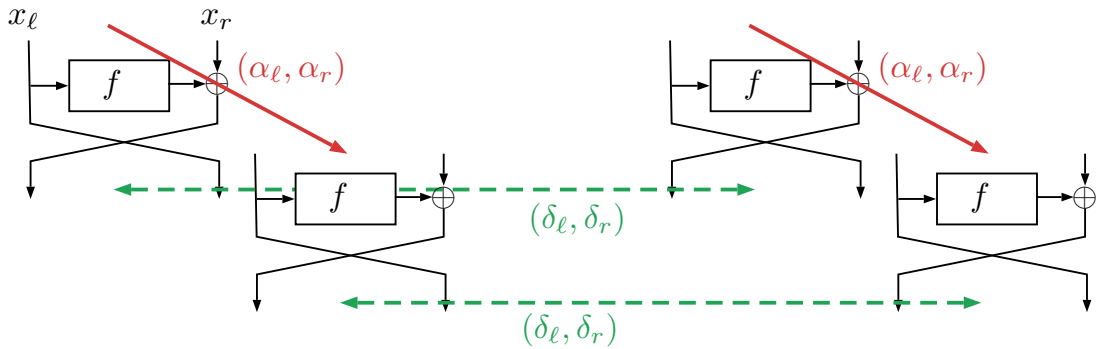


A boomerang returns from 1 round of Feistel cipher with round function f for the input x_ℓ, x_r if and only if

$$f(x_\ell) \oplus f(x_\ell \oplus \delta_r) \oplus f(x_\ell \oplus \alpha_\ell) \oplus f(x_\ell \oplus \delta_r \oplus \alpha_\ell) = 0,$$

that is, the **second derivative** of f at points α_ℓ, δ_r must be zero.

Generic 1-round Boomerang on a Feistel cipher



A boomerang returns from 1 round of Feistel cipher with round function f for the input x_ℓ, x_r if and only if

$$f(x_\ell) \oplus f(x_\ell \oplus \delta_r) \oplus f(x_\ell \oplus \alpha_\ell) \oplus f(x_\ell \oplus \delta_r \oplus \alpha_\ell) = 0,$$

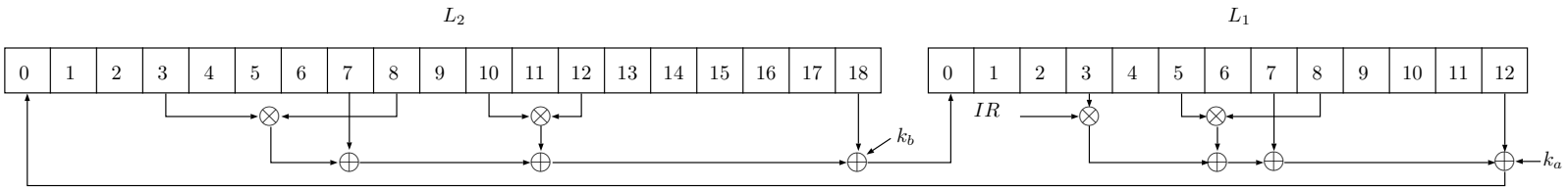
that is, the **second derivative** of f at points α_ℓ, δ_r must be zero.

If f is a quadratic function, its second order derivative is a constant.

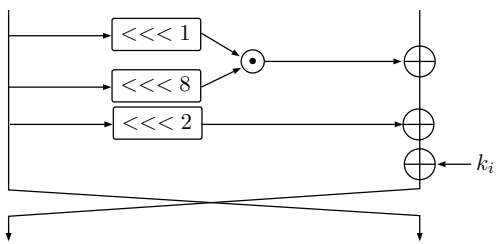
Either the boomerang always returns, or never

Concrete study

KATAN



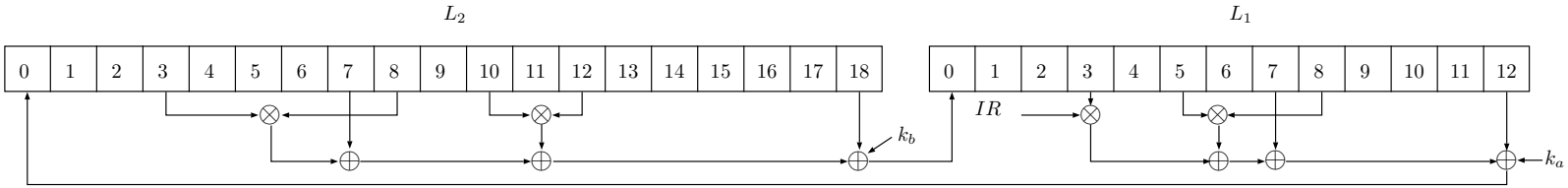
Simon



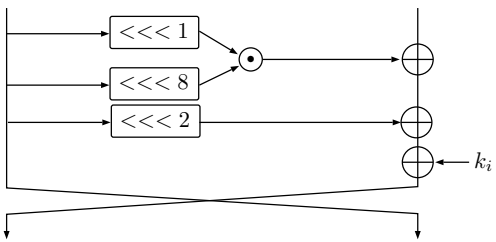
- Many variants, from 32 bits size to 64 (KATAN) or 128 (Simon)
- Both Feistel-like
- Quadratic round function

Concrete study

KATAN



Simon



Boomerang constraint for KATAN32

$$\begin{cases} \alpha_{12} \cdot \delta_{11} \oplus \alpha_{10} \cdot \delta_{13} \oplus \alpha_8 \cdot \delta_4 \oplus \alpha_3 \cdot \delta_9 = 0 \\ \alpha'_8 \cdot \delta'_6 \oplus \alpha'_5 \cdot \delta'_9 = 0 \end{cases}$$

Boomerang constraint for Simon

$$(\alpha_\ell \lll 8) \cdot (\delta_r \lll 1) \oplus (\alpha_\ell \lll 1) \cdot (\delta_r \lll 8) = 0$$

- Many variants, from 32 bits size to 64 (KATAN) or 128 (Simon)
- Both Feistel-like
- Quadratic round function

Previous boomerang distinguishers on KATAN and Simon

- Identified 20 distinguishers in 6 articles
- All used the naive probability analysis

Previous boomerang distinguishers on KATAN and Simon

- Identified 20 distinguishers in 6 articles
- All used the naive probability analysis

Trail check

- Check the trails using our formulas

Previous boomerang distinguishers on KATAN and Simon

- Identified 20 distinguishers in 6 articles
- All used the naive probability analysis

Trail check

- Check the trails using our formulas
- Results:
  - All pairs are incompatible
  - Inconclusive
  - All pairs are compatible (Simon48)

Previous boomerang distinguishers on KATAN and Simon

- Identified 20 distinguishers in 6 articles
- All used the naive probability analysis

Trail check

- Check the trails using our formulas
- Results:
  - All pairs are incompatible
  - Inconclusive
  - All pairs are compatible (Simon48)

Experimental verification

- Verification of the differences, not the characteristics
- Partial verification for low-probability distinguishers

Previous boomerang distinguishers on KATAN and Simon

- Identified 20 distinguishers in 6 articles
- All used the naive probability analysis

Trail check

- Check the trails using our formulas
- Results:
  - All pairs are incompatible
  - Inconclusive
  - All pairs are compatible (Simon48)

Experimental verification

- Verification of the differences, not the characteristics
- Partial verification for low-probability distinguishers
- Results:
  - Distinguisher doesn't work at all ($P = 2^{-n}$)
  - Distinguisher works much better than expected

Previous boomerang distinguishers on KATAN and Simon

- Identified 20 distinguishers in 6 articles
- All used the naive probability analysis

Trail check

- Check the trails using our formulas
- Results:
  - All pairs are incompatible
  - Inconclusive
  - All pairs are compatible (Simon48)

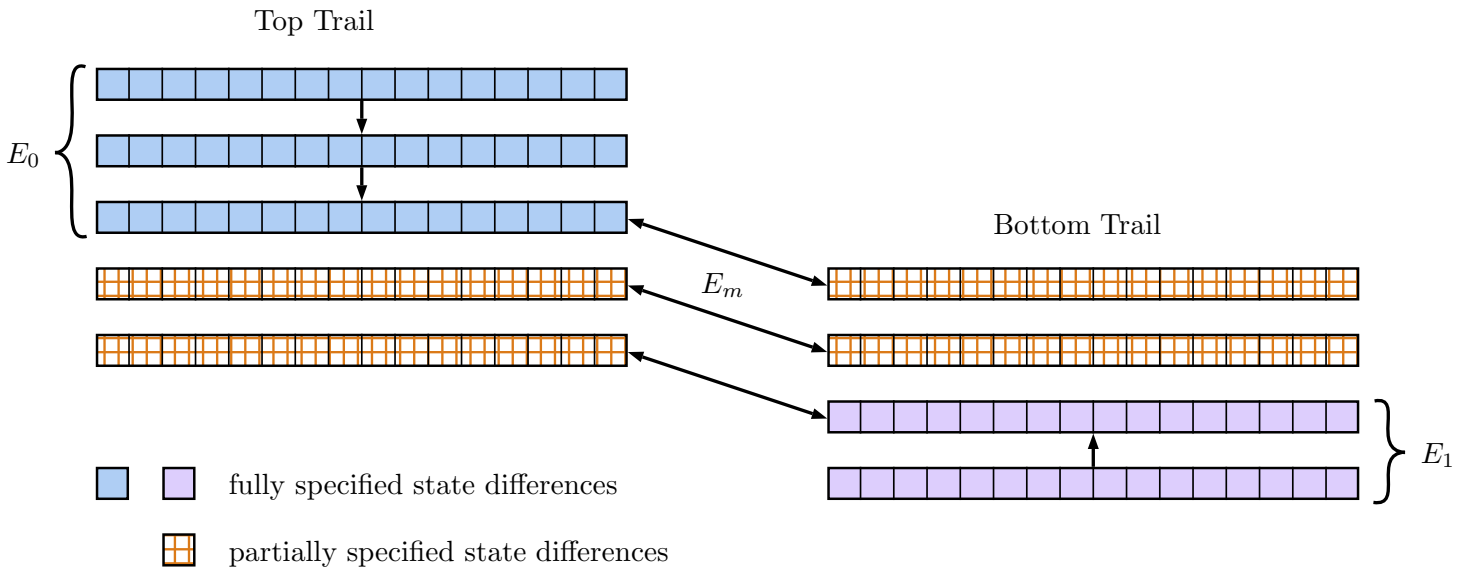
Experimental verification

- Verification of the differences, not the characteristics
- Partial verification for low-probability distinguishers
- Results:
  - Distinguisher doesn't work at all ($P = 2^{-n}$)
  - Distinguisher works much better than expected

- Probabilities are inaccurate
- In most cases, the distinguisher doesn't work

New Distinguishers and Attacks

Our SMT Model



- E_0 and E_1 are considered independent one from the other
  - **fully specified** differential trails
  - p^2 and q^2 probability
- middle rounds cover the interactions
  - boomerang constraints are enforced
  - Truncated differentials $(0, 1, ?)$
  - the model can fix some non-deterministic transitions

Results of our SMT model for RK Boomerang Distinguishers on KATAN 32

Rounds	140	141	142	143	144	145	146	147	148	149	150	151	152
Top	40	40	41	41	42	40	43	43	44	45	45	45	46
Middle	60	61	60	61	60	65	60	61	60	59	60	61	60
Bottom	40	40	41	41	42	40	43	43	44	45	45	45	46
Model proba.$^\diamond$	-17	-17	-20	-21	-22	-23	-25	-25	-27	-29	-31	-31	-33
Exp. proba.$^\diamond$	-16.2	-15.8	-20.2	-19.8	-19.1	-22.5	-24.3	-24.3	-26.3	-28.3	-30.2	-30.1	-31.7

$\diamond$ Binary logarithm of the probabilities.

Results of our SMT model for RK Boomerang Distinguishers on KATAN 32

Rounds	140	141	142	143	144	145	146	147	148	149	150	151	152
Top	40	40	41	41	42	40	43	43	44	45	45	45	46
Middle	60	61	60	61	60	65	60	61	60	59	60	61	60
Bottom	40	40	41	41	42	40	43	43	44	45	45	45	46
Model proba.$^\diamond$	-17	-17	-20	-21	-22	-23	-25	-25	-27	-29	-31	-31	-33
Exp. proba.$^\diamond$	-16.2	-15.8	-20.2	-19.8	-19.1	-22.5	-24.3	-24.3	-26.3	-28.3	-30.2	-30.1	-31.7

$\diamond$ Binary logarithm of the probabilities.

Previous boomerang(s) [JRS22]

- 140 Round
- Estimated 2^{-22}
- Experimental $2^{-15.8}$

Results of our SMT model for RK Boomerang Distinguishers on KATAN 32

Rounds	140	141	142	143	144	145	146	147	148	149	150	151	152
Top	40	40	41	41	42	40	43	43	44	45	45	45	46
Middle	60	61	60	61	60	65	60	61	60	59	60	61	60
Bottom	40	40	41	41	42	40	43	43	44	45	45	45	46
Model proba.$^\diamond$	-17	-17	-20	-21	-22	-23	-25	-25	-27	-29	-31	-31	-33
Exp. proba.$^\diamond$	-16.2	-15.8	-20.2	-19.8	-19.1	-22.5	-24.3	-24.3	-26.3	-28.3	-30.2	-30.1	-31.7

$\diamond$ Binary logarithm of the probabilities.

Previous boomerang(s) [JRS22]

- 140 Round
- Estimated 2^{-22}
- Experimental $2^{-15.8}$

Best attack [RR16]

206 rounds, MITM, Single-key

Rotational-Xor and Rotational-Xor Differential Rectangles

Normal Differences

$$x \oplus x' = \alpha$$

Rotational-Xor differences

$$x \oplus (x' \lll 1) = \alpha$$

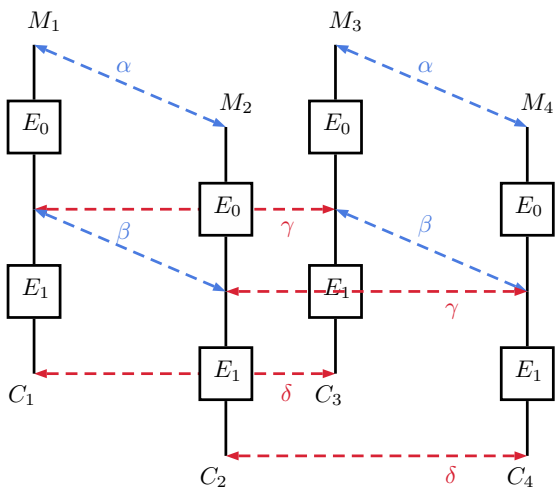
Rotational-Xor and Rotational-Xor Differential Rectangles

Normal Differences

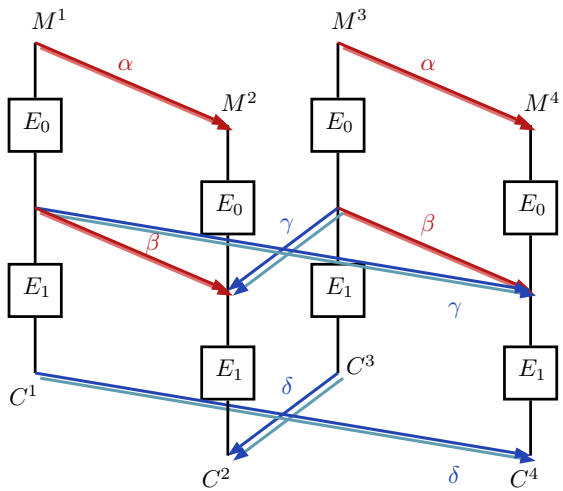
$$x \oplus x' = \alpha$$

Rotational-Xor differences

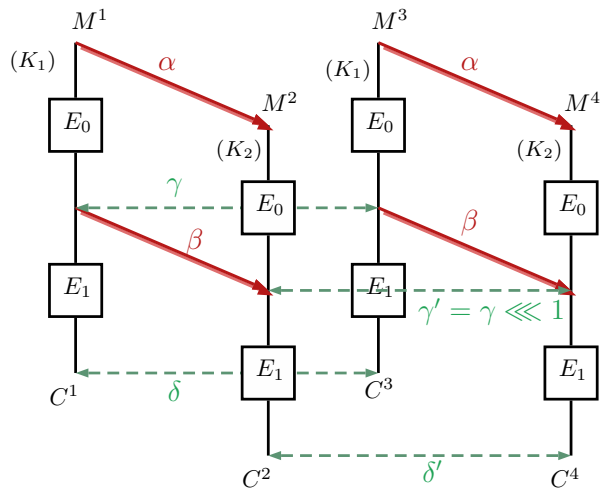
$$x \oplus (x' \lll 1) = \alpha$$



Normal Boomerang



Rotational-Xor Boomerang



Rotational-Xor Differential Boomerang

Results of our SMT model on Simon-32/64

Related-key boomerang distinguishers

Rounds	12	13	14	15	16	17
Cut	5+2+5	5+3+5	5+4+5	6+3+6	5+6+5	6+5+6
Model proba.	0	-3	-7	-11	-19	-25
Experimental proba.	0	-2.7	-6.7	-10.4	-18.8	-23.6

RX-boomerang distinguishers

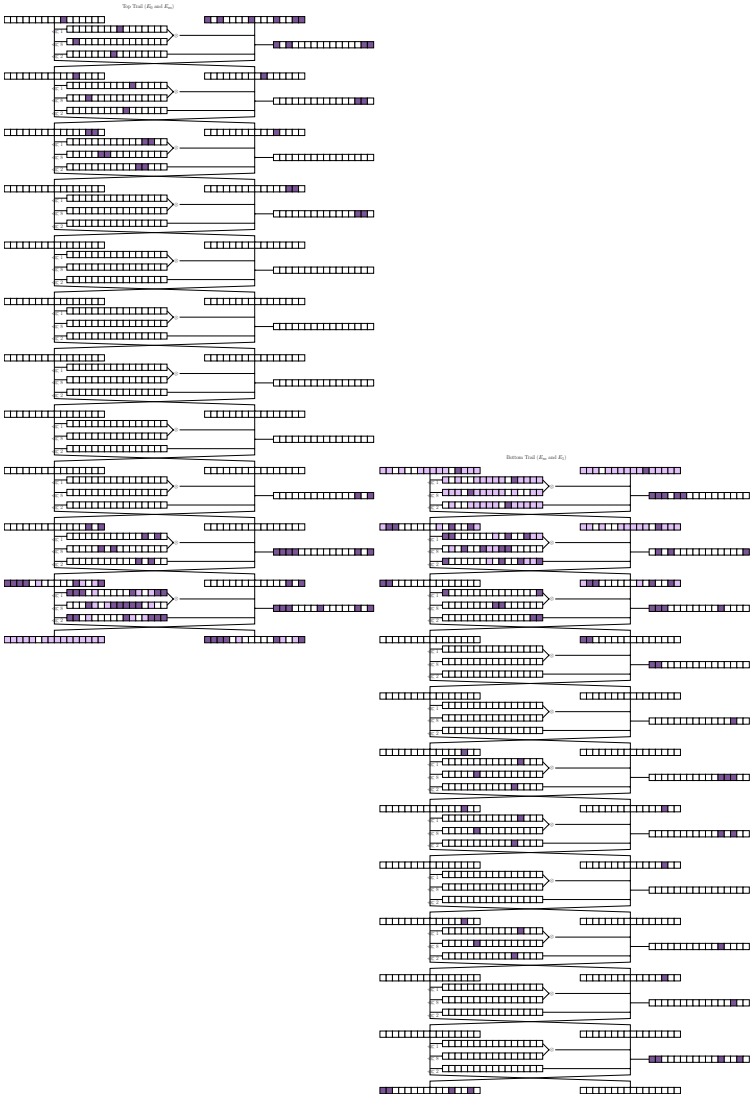
Rounds	13	14	15	16	17	18	19
Starting round	3	3	10	3	3	3	3
Cut	4+5+4	5+4+5	5+5+5	5+6+5	6+5+6	6+6+6	7+5+7
Model proba.	0	-3	-6	-12	-16	-24	-30
Experimental proba.	0	-3	-6	-12	-16	-24	-29.5

RX-differential boomerang distinguishers

Rounds	13	14	15
Starting round	3	3	3
Cut	7+4+2	5+5+4	6+5+4
Model proba.	-17	-23	-28
Experimental proba.	-17.2	-21	-27.6

(Binary logarithm of the probabilities)

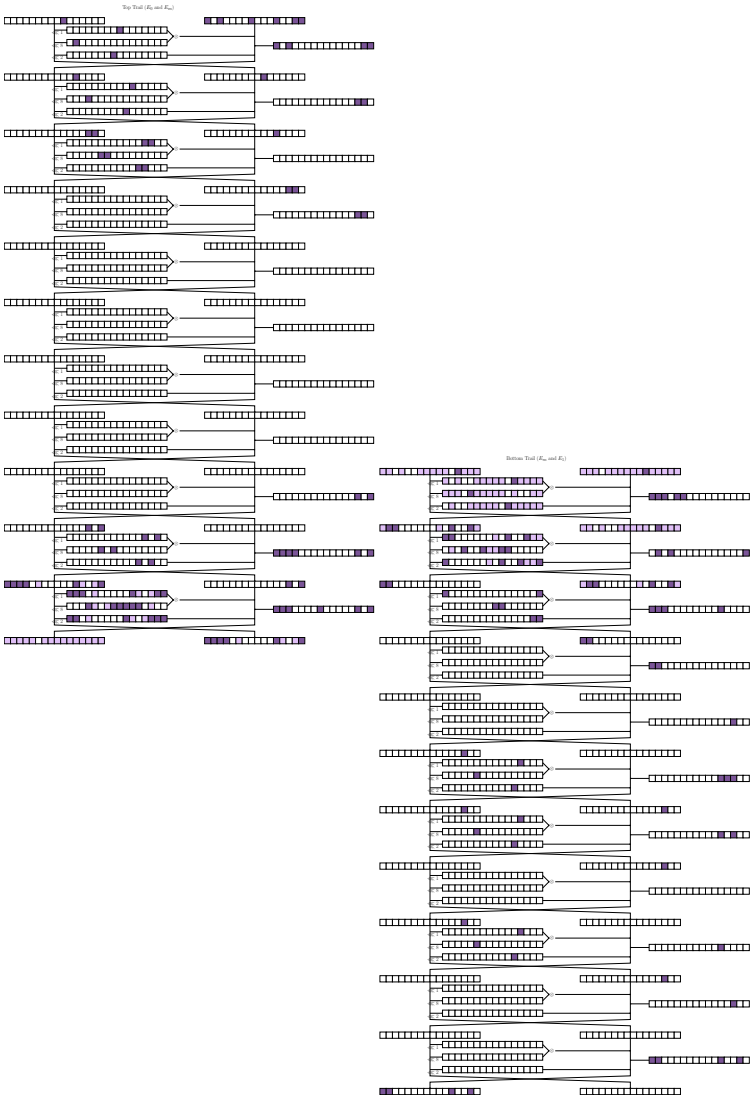
Attacks against Simon32



- Start from an RX-boomerang distinguisher
- Add 3 rounds above and below
- Results:

Rounds	Data	Time
24	2^{31}	$2^{54.6}$
25	2^{34}	$2^{59.7}$

Attacks against Simon32



- Start from an RX-boomerang distinguisher
- Add 3 rounds above and below
- Results:

Rounds	Data	Time
24	2^{31}	$2^{54.6}$
25	2^{34}	$2^{59.7}$

Previous best attack [CCW+18]

24 Rounds, Linear, Single key, 2^{32} Data

Conclusion

Summary

- Found issues in most boomerangs against KATAN and Simon
- Obtained new, more accurate boomerang distinguishers
- First (related-key) attack against 25-round Simon 32

Conclusion

Summary

- Found issues in most boomerangs against KATAN and Simon
- Obtained new, more accurate boomerang distinguishers
- First (related-key) attack against 25-round Simon 32

Advices to cryptanalysts

- Don't be naive with boomerangs!
- If possible, verify experimentally