Throwing Boomerangs into Feistel Structures

Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE

Hosein Hadipour Marcel Nageler Maria Eichlseder

FSE 2023 - Kobe, Japan

> hossein.hadipour@iaik.tugraz.at

TU Graz

SCIENCE PASSION TECHNOLOGY

Research Gap and Our Contributions

Motivation and Our Contributions

Research gap:

- The lack of a tool to automatically find boomerang distinguishers for Feistel cipher

Contributions:

- Providing an easy to use and fast method to find boomerang distinguishers
- We applied our method to `CLEFIA`, `WARP`, `LBlock`, and `TWINE`
  - We improved the boomerang distinguisher of `WARP` by 2 rounds
  - We improved the boomerang distinguisher/attack of `CLEFIA` by 1 round
- Our method is applicable to any strongly aligned (Sbox-based) block cipher, e.g., SKINNY

Motivation and Our Contributions

Research gap:

- The lack of a tool to automatically find boomerang distinguishers for Feistel cipher

Contributions:

- Providing an easy to use and fast method to find boomerang distinguishers
- We applied our method to `CLEFIA`, `WARP`, `LBlock`, and `TWINE`
  - We improved the boomerang distinguisher of `WARP` by 2 rounds
  - We improved the boomerang distinguisher/attack of `CLEFIA` by 1 round
- Our method is applicable to any strongly aligned (Sbox-based) block cipher, e.g., SKINNY

Motivation and Our Contributions

Research gap:

- The lack of a tool to automatically find boomerang distinguishers for Feistel cipher

Contributions:

- Providing an easy to use and fast method to find boomerang distinguishers
- We applied our method to `CLEFIA`, `WARP`, `LBlock`, and `TWINE`
  - We improved the boomerang distinguisher of `WARP` by 2 rounds
  - We improved the boomerang distinguisher/attack of `CLEFIA` by 1 round
- Our method is applicable to any strongly aligned (Sbox-based) block cipher, e.g., SKINNY

Motivation and Our Contributions

Research gap:

- The lack of a tool to automatically find boomerang distinguishers for Feistel cipher

Contributions:

- Providing an easy to use and fast method to find boomerang distinguishers
- We applied our method to `CLEFIA`, `WARP`, `LBlock`, and `TWINE`
  - We improved the boomerang distinguisher of `WARP` by 2 rounds
  - We improved the boomerang distinguisher/attack of `CLEFIA` by 1 round
- Our method is applicable to any strongly aligned (Sbox-based) block cipher, e.g., SKINNY

Motivation and Our Contributions

Research gap:

- The lack of a tool to automatically find boomerang distinguishers for Feistel cipher

Contributions:

- Providing an easy to use and fast method to find boomerang distinguishers
- We applied our method to `CLEFIA`, `WARP`, `LBlock`, and `TWINE`
  - We improved the boomerang distinguisher of `WARP` by 2 rounds
  - We improved the boomerang distinguisher/attack of `CLEFIA` by 1 round
- Our method is applicable to any strongly aligned (Sbox-based) block cipher, e.g., SKINNY

Motivation and Our Contributions

Research gap:

- The lack of a tool to automatically find boomerang distinguishers for Feistel cipher

Contributions:

- Providing an easy to use and fast method to find boomerang distinguishers
- We applied our method to `CLEFIA`, `WARP`, `LBlock`, and `TWINE`
  - We improved the boomerang distinguisher of `WARP` by 2 rounds
  - We improved the boomerang distinguisher/attack of `CLEFIA` by 1 round
- Our method is applicable to any strongly aligned (Sbox-based) block cipher, e.g., SKINNY

Outline

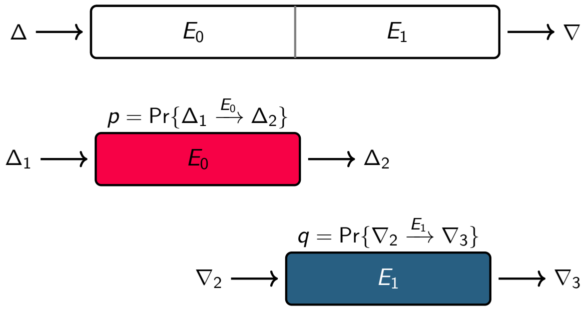
Effective Parameters in the Success Probability of Boomerang Distinguishers

Boomerang Distinguishers [Wag99]

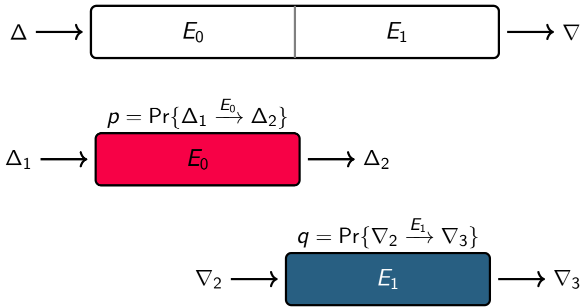
$$\Delta \longrightarrow \boxed{E : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n} \longrightarrow \nabla$$

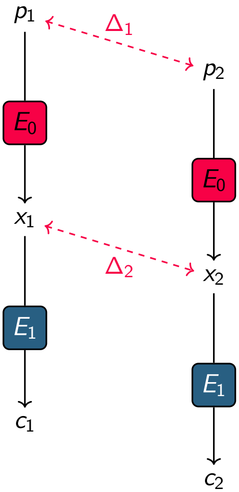
$$0 \lneq \Pr\{\Delta \xrightarrow{E} \nabla\} \lll 2^{-n}$$

Boomerang Distinguishers [Wag99]

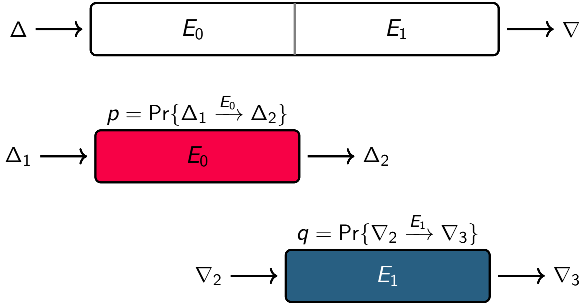


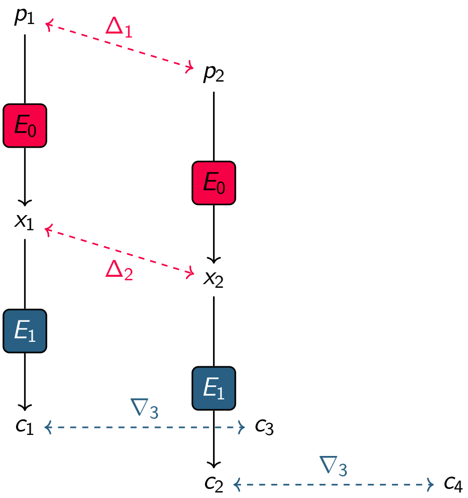
Boomerang Distinguishers [Wag99]





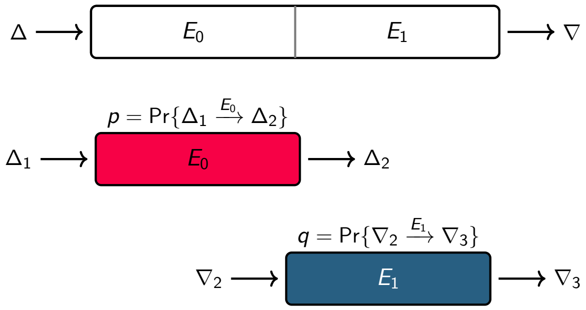
Boomerang Distinguishers [Wag99]

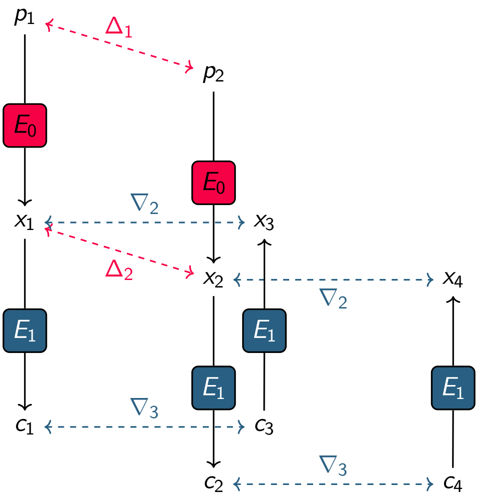




Hosein Hadipour, Marcel Nageler, Maria Eichlseder

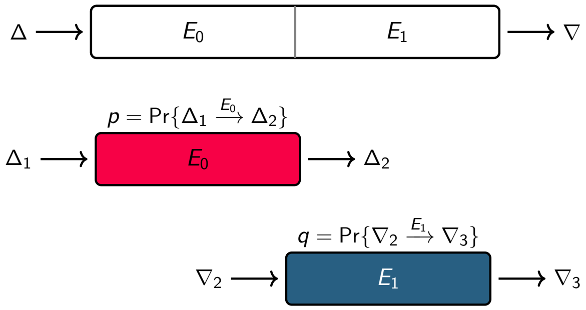
Boomerang Distinguishers [Wag99]



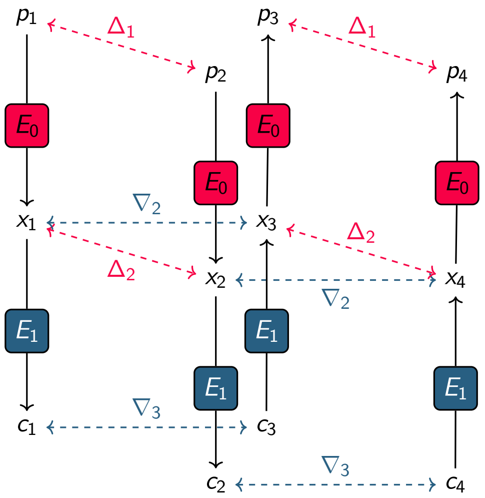


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Boomerang Distinguishers [Wag99]

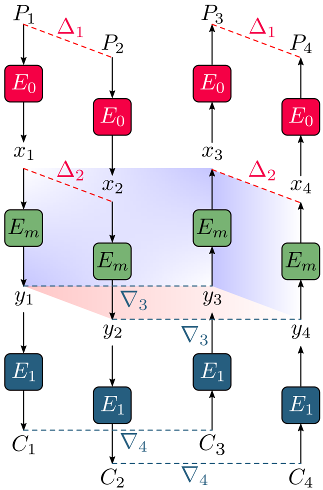


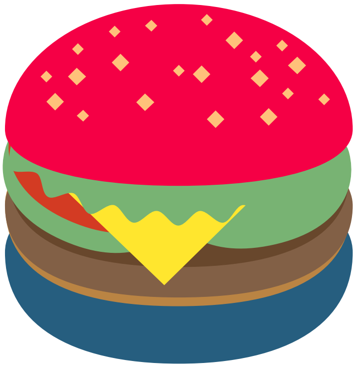
$$\Pr\{p_3 \oplus p_4 = \Delta_1\} = p^2 q^2$$



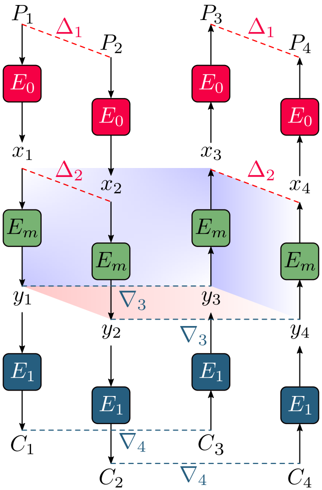
Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Sandwiching the Differentials! [DKS10]





Sandwiching the Differentials! [DKS10]

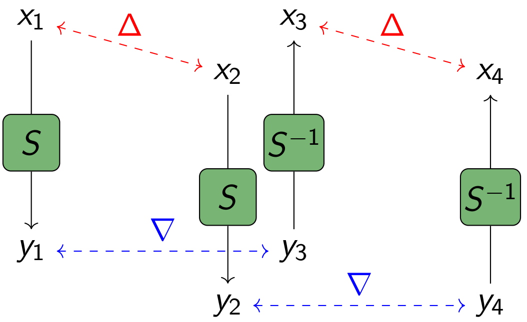


$$\Pr(P_3 \oplus P_4 = \Delta_1) \approx p^2 \times r \times q^2$$

$$r = \Pr(\Delta_2 \rightleftarrows \nabla_3)$$

Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Boomerang Switch For SPN Block Ciphers

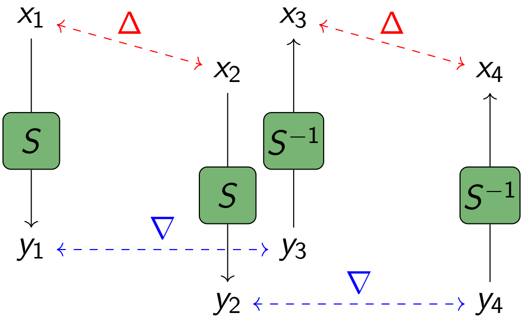


$$\mathrm{BCT}(\Delta, \nabla) := \#\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus \nabla) \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta\}$$

$$\mathrm{BCT}(0, \nabla) = \mathrm{BCT}(\Delta, 0) = 2^n$$

Hosein Hadipour, Marcel Nageler, Maria Eichlseder

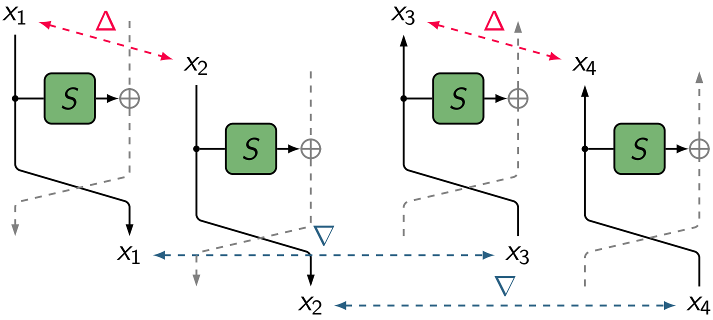
Boomerang Switch For SPN Block Ciphers



$$\mathrm{BCT}(\Delta, \nabla) := \#\{x \in \mathbb{F}_2^n \mid S^{-1}(S(x) \oplus \nabla) \oplus S^{-1}(S(x \oplus \Delta) \oplus \nabla) = \Delta\}$$

$$\mathrm{BCT}(0, \nabla) = \mathrm{BCT}(\Delta, 0) = 2^n$$

Boomerang Switch For Feistel Ciphers

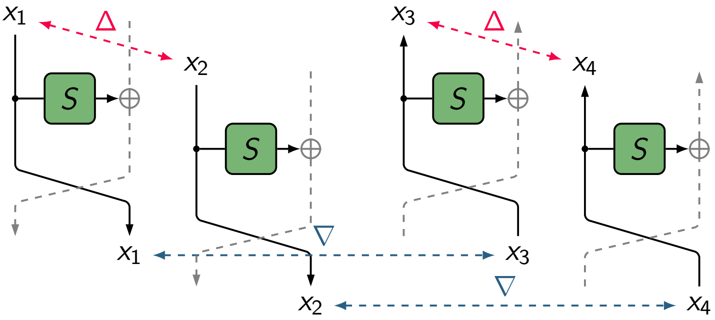


$$\mathtt{FBCT}(\Delta, \nabla) := \#\{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \Delta) \oplus S(x \oplus \nabla) \oplus S(x \oplus \Delta \oplus \nabla) = 0\}$$

$$\mathtt{FBCT}(\Delta, 0) = \mathtt{FBCT}(0, \nabla) = 2^n$$

Hosein Hadipour, Marcel Nageler, Maria Eichlseder
FSE 2023 - Kobe, Japan

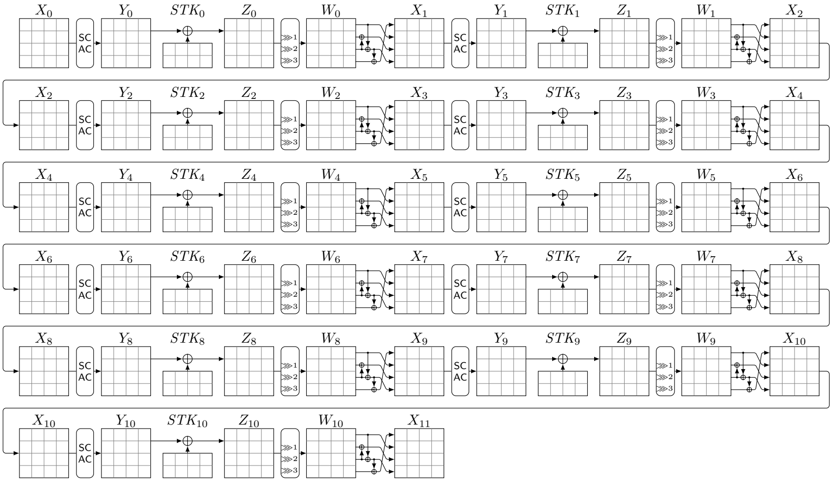
Boomerang Switch For Feistel Ciphers



$$\mathrm{FBCT}(\Delta, \nabla) := \#\{x \in \mathbb{F}_2^n : S(x) \oplus S(x \oplus \Delta) \oplus S(x \oplus \nabla) \oplus S(x \oplus \Delta \oplus \nabla) = 0\}$$

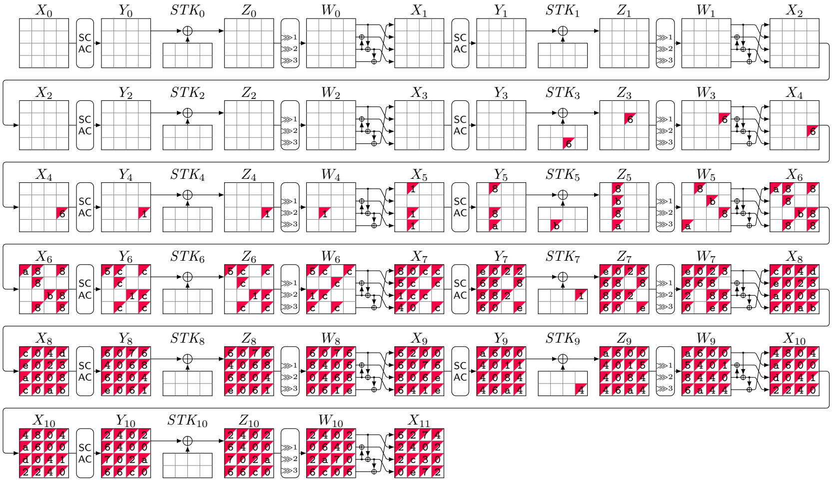
$$\mathrm{FBCT}(\Delta, 0) = \mathrm{FBCT}(0, \nabla) = 2^n$$

Building Deterministic Boomerang from Impossible Trails [HBS21]



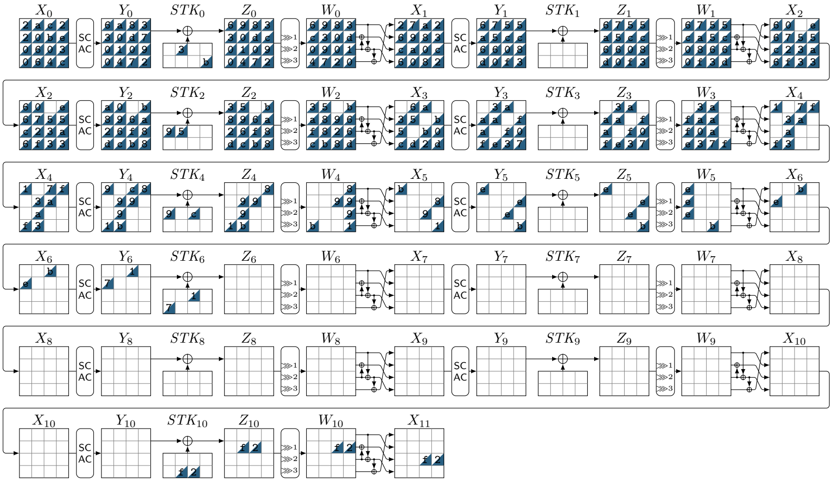
- $p = 2^{-146}$ (impossible due to dependencies [PT22])
- $q = 2^{-179}$ (impossible due to dependencies [PT22])
- $\Pr_{\text{boom}} = 1$

Building Deterministic Boomerang from Impossible Trails [HBS21]



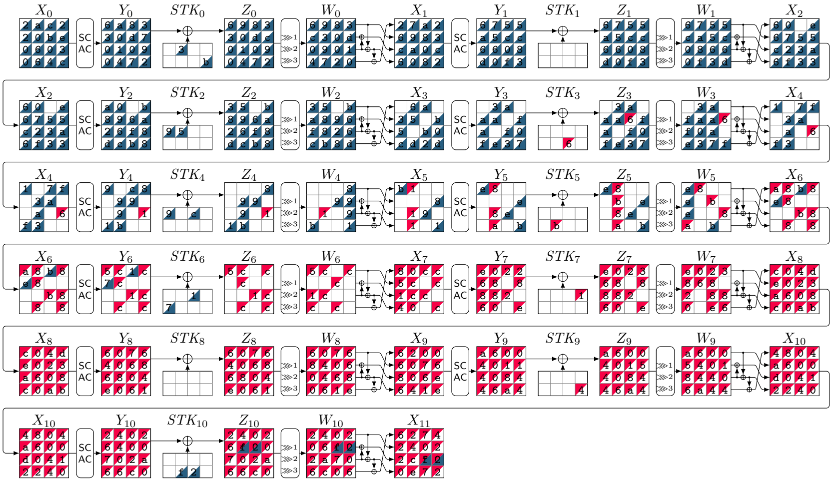
- $p = 2^{-146}$ (impossible due to dependencies [PT22])
- $q = 2^{-179}$ (impossible due to dependencies [PT22])
- $\Pr_{\mathrm{boom}} = 1$

Building Deterministic Boomerang from Impossible Trails [HBS21]



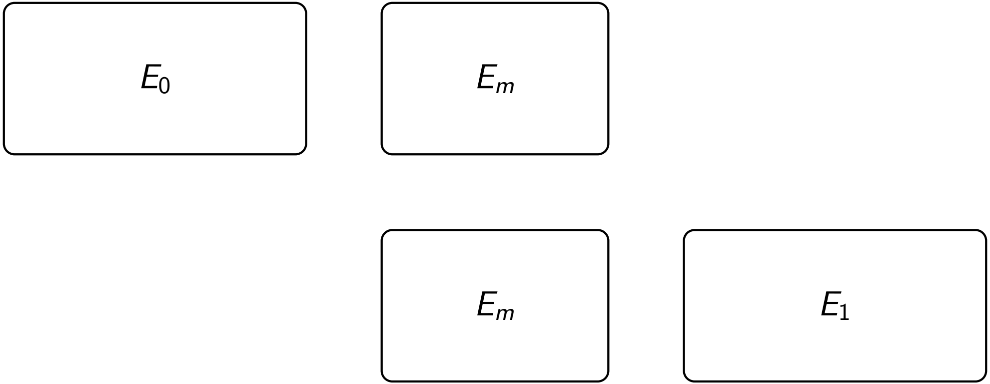
- $p = 2^{-146}$ (impossible due to dependencies [PT22])
- $q = 2^{-179}$ (impossible due to dependencies [PT22])
- $\Pr_{\text{boom}} = 1$

Building Deterministic Boomerang from Impossible Trails [HBS21]

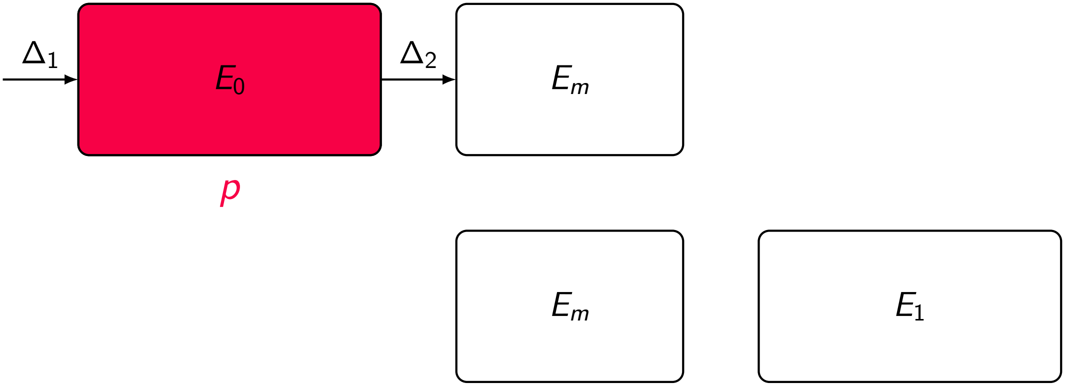


- $p = 2^{-146}$ (impossible due to dependencies [PT22])
- $q = 2^{-179}$ (impossible due to dependencies [PT22])
- $\Pr_{\text{boom}} = 1$

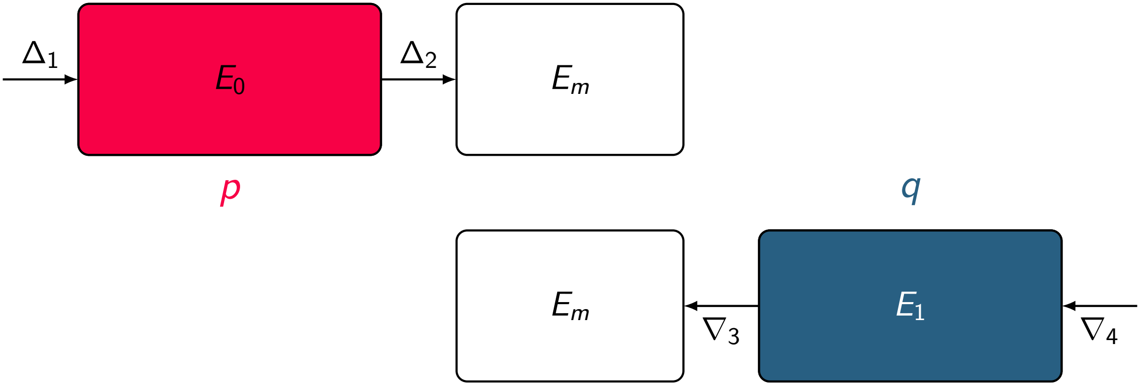
Effective Parameters in p^2q^2r Formula



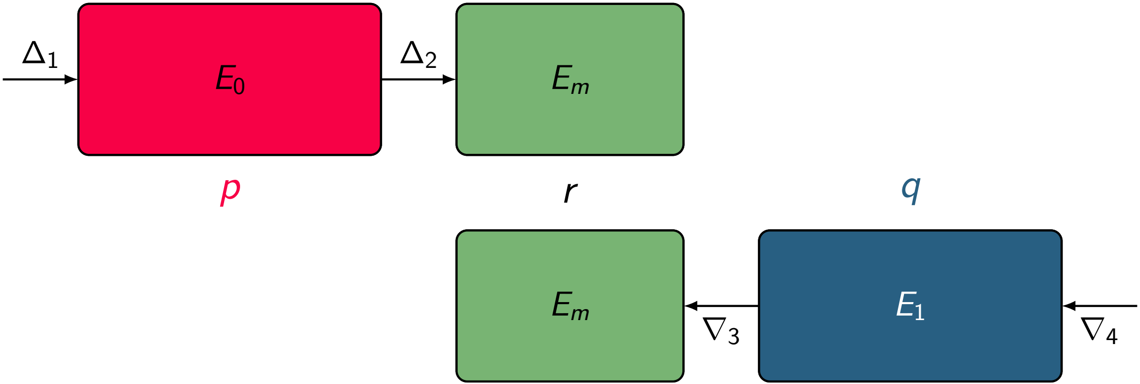
Effective Parameters in p^2q^2r Formula



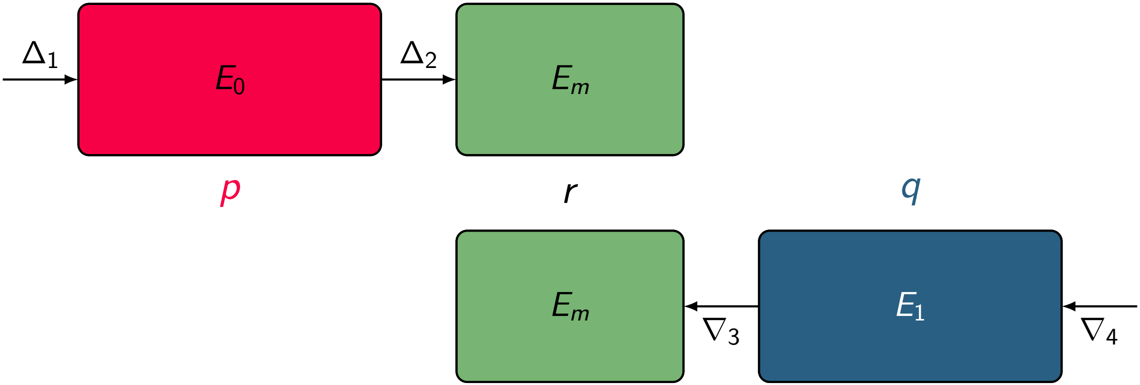
Effective Parameters in p^2q^2r Formula



Effective Parameters in p^2q^2r Formula



Effective Parameters in p^2q^2r Formula



Active S-boxes in E_0, E_1 are more expensive than common active S-boxes in E_m

Our Method to Search for Boomerang Distinguishers

Our Method to Find Boomerang Distinguishers

Our method has three steps:

- Find good truncated upper and lower trails:
  - minimize number of active S-boxes in outer parts, i.e., E_0, and E_1
  - minimize number of common active S-boxes in the middle part, i.e., E_m
- Instantiate discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Our Method to Find Boomerang Distinguishers

Our method has three steps:

- Find good truncated upper and lower trails:
  - minimize number of active S-boxes in outer parts, i.e., E_0, and E_1
  - minimize number of common active S-boxes in the middle part, i.e., E_m
- Instantiate discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Our Method to Find Boomerang Distinguishers

Our method has three steps:

- Find good truncated upper and lower trails:
  - minimize number of active S-boxes in outer parts, i.e., E_0, and E_1
  - minimize number of common active S-boxes in the middle part, i.e., E_m
- Instantiate discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

Our Method to Find Boomerang Distinguishers

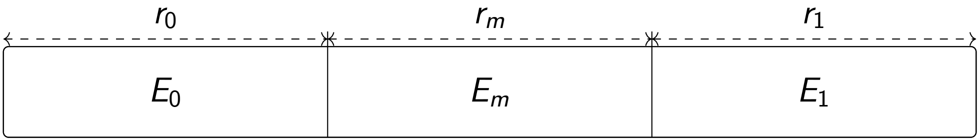
Our method has three steps:

- Find good truncated upper and lower trails:
  - minimize number of active S-boxes in outer parts, i.e., E_0, and E_1
  - minimize number of common active S-boxes in the middle part, i.e., E_m
- Instantiate discovered truncated trails with concrete differential trails
- Compute p, q and r to derive the entire probability, i.e., p^2q^2r

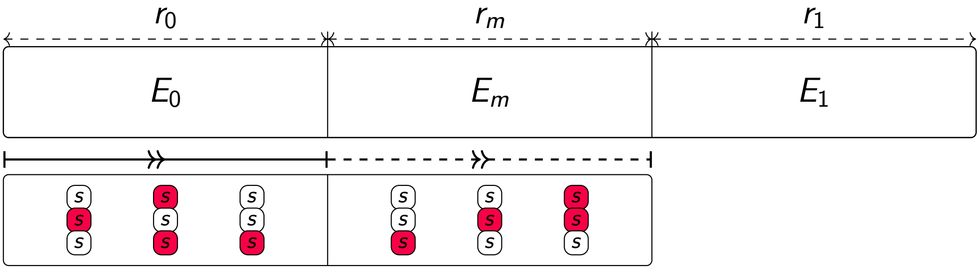
Find Good Truncated Upper and Lower Trails

E

Find Good Truncated Upper and Lower Trails

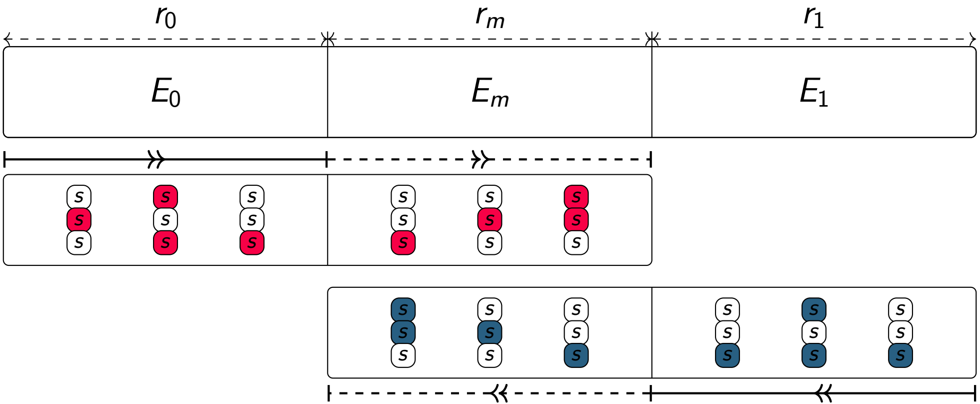


Find Good Truncated Upper and Lower Trails

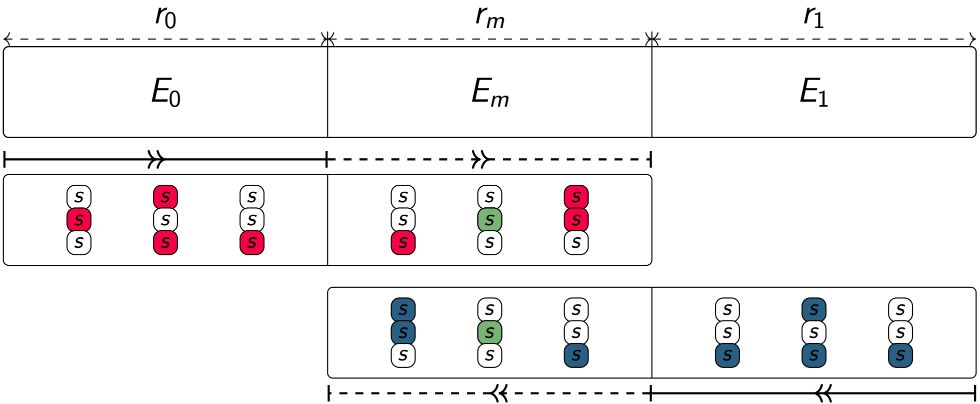


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

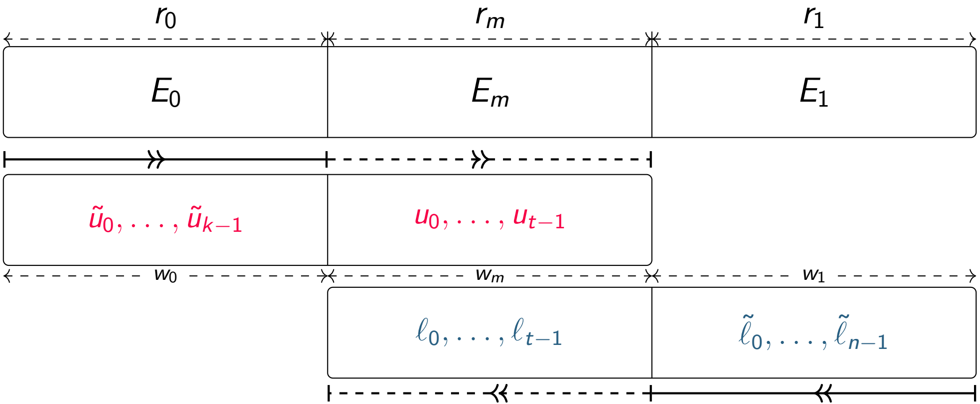
Find Good Truncated Upper and Lower Trails



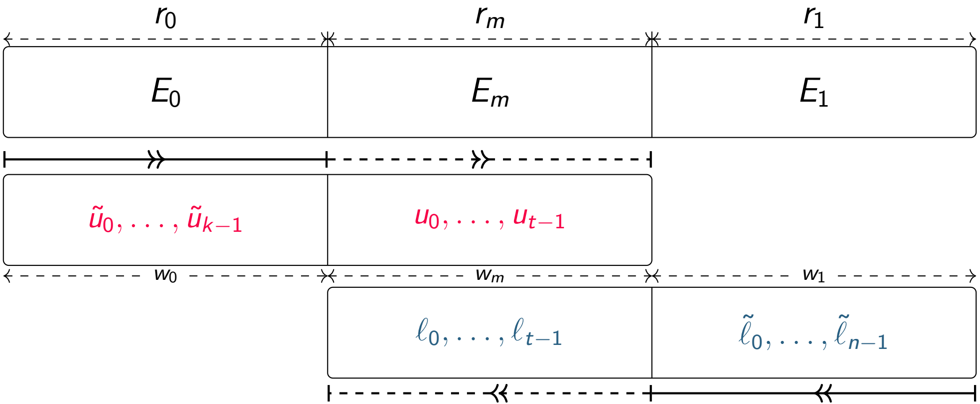
Find Good Truncated Upper and Lower Trails



Find Good Truncated Upper and Lower Trails



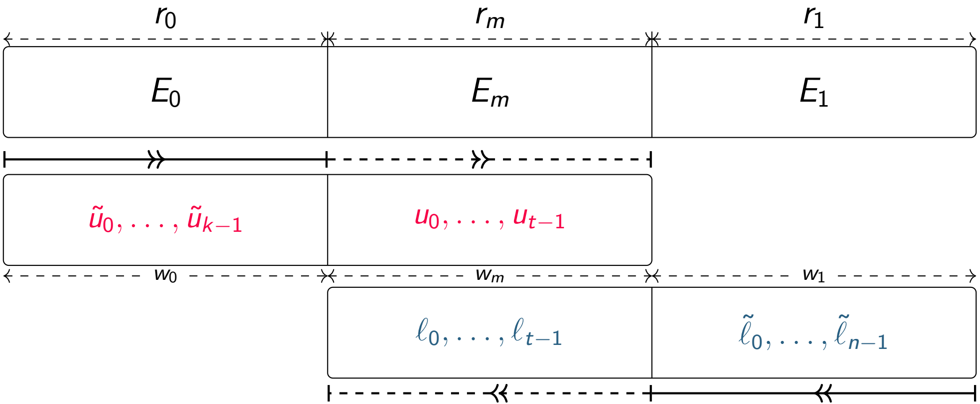
Find Good Truncated Upper and Lower Trails



$$u_i - s_i \geq 0, \quad \ell_i - s_i \geq 0, \quad -u_i - \ell_i + s_i \geq -1$$

Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Find Good Truncated Upper and Lower Trails

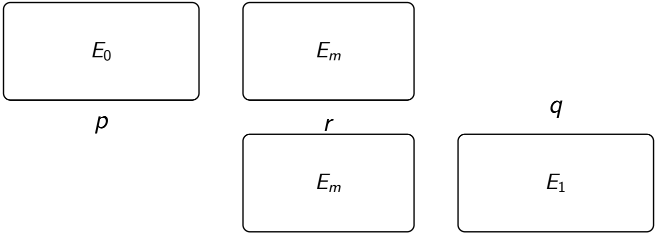


$$\min \sum_{i=0}^{k-1} w_0 \cdot \tilde{u}_i + \sum_{j=0}^{t-1} w_m \cdot s_j + \sum_{k=0}^{n-1} w_1 \cdot \tilde{\ell}_k$$

$$u_i - s_i \geq 0, \quad \ell_i - s_i \geq 0, \quad -u_i - \ell_i + s_i \geq -1$$

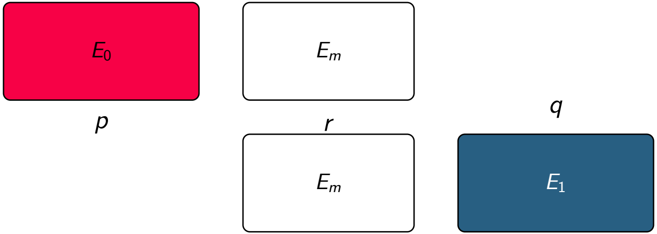
Instantiate Discovered Truncated Trails with Real Differentials

- We instantiate the truncated trails for E0 and E1 with bit-wise trails
- We only fix $\Delta_1, \Delta_2, \nabla_3$, and ∇_4 to compute p, and q
- We compute $r = \Pr\{\Delta_2 \rightleftarrows \nabla_3\}$ for E_m



Instantiate Discovered Truncated Trails with Real Differentials

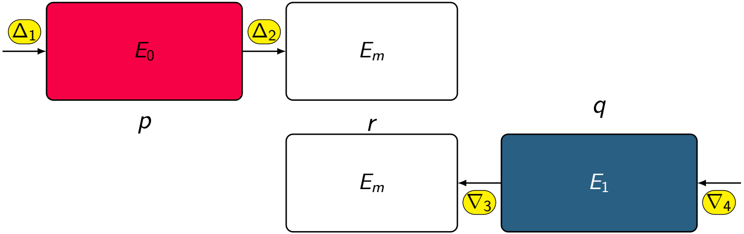
- We instantiate the truncated trails for E0 and E1 with bit-wise trails
- We only fix $\Delta_1, \Delta_2, \nabla_3$, and ∇_4 to compute p, and q
- We compute $r = \Pr\{\Delta_2 \rightleftarrows \nabla_3\}$ for E_m



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

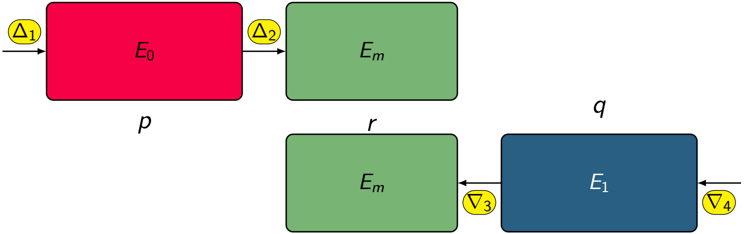
Instantiate Discovered Truncated Trails with Real Differentials

- We instantiate the truncated trails for E0 and E1 with bit-wise trails
- We only fix $\Delta_1, \Delta_2, \nabla_3$, and ∇_4 to compute p, and q
- We compute $r = \Pr\{\Delta_2 \rightleftarrows \nabla_3\}$ for E_m



Instantiate Discovered Truncated Trails with Real Differentials

- We instantiate the truncated trails for E0 and E1 with bit-wise trails
- We only fix $\Delta_1, \Delta_2, \nabla_3$, and ∇_4 to compute p, and q
- We compute $r = \Pr\{\Delta_2 \rightleftarrows \nabla_3\}$ for E_m

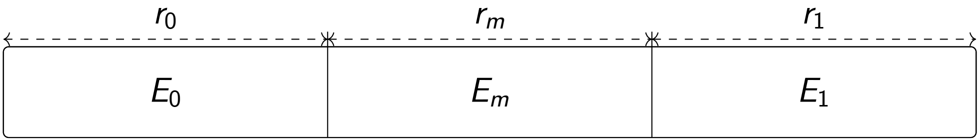


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Applications of Our Method to CLEFIA, WARP, LBlock, and TWINE

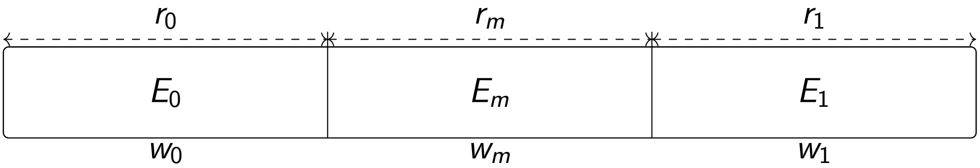
Usage of Our Tool

```
python3 boom.py -r0 6 -rm 10 -r1 7
```



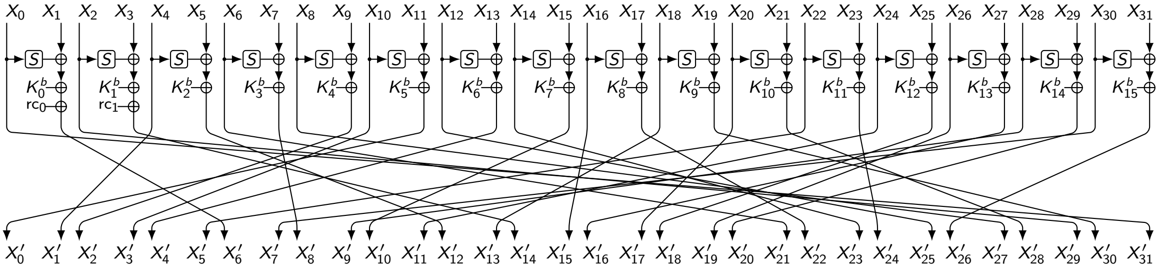
Usage of Our Tool

```
python3 boom.py -r0 6 -rm 10 -r1 7 -w0 2 -wm 1 -w1 2
```

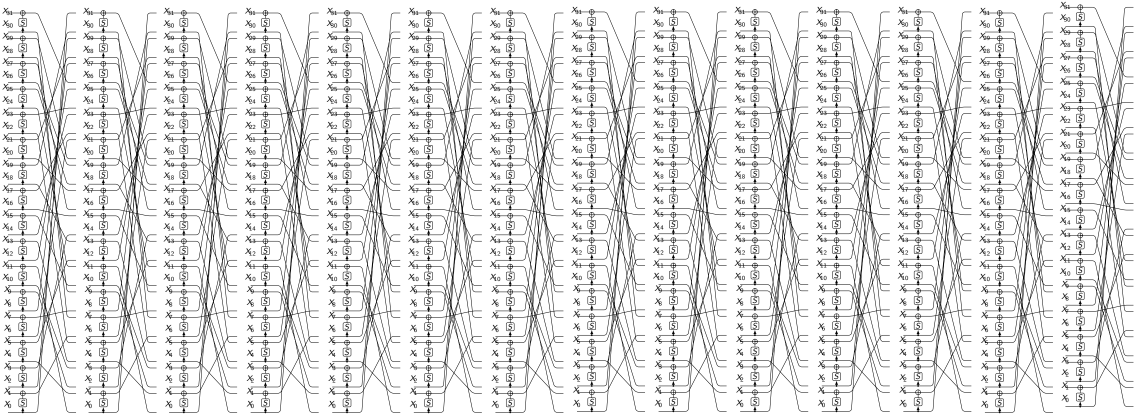


WARP

- Proposed in SAC 2020 [Ban+20] as the lightweight alternative of AES-128
- 128-bit block size, and 128-bit key size
- 41 rounds (40.5 rounds)

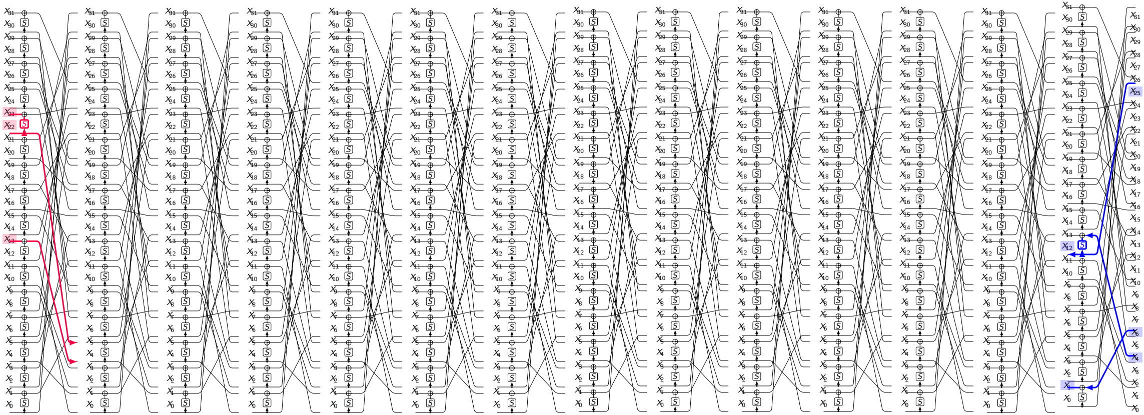


14-Round Boomerang Distinguisher for WARP



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

14-Round Boomerang Distinguisher for WARP

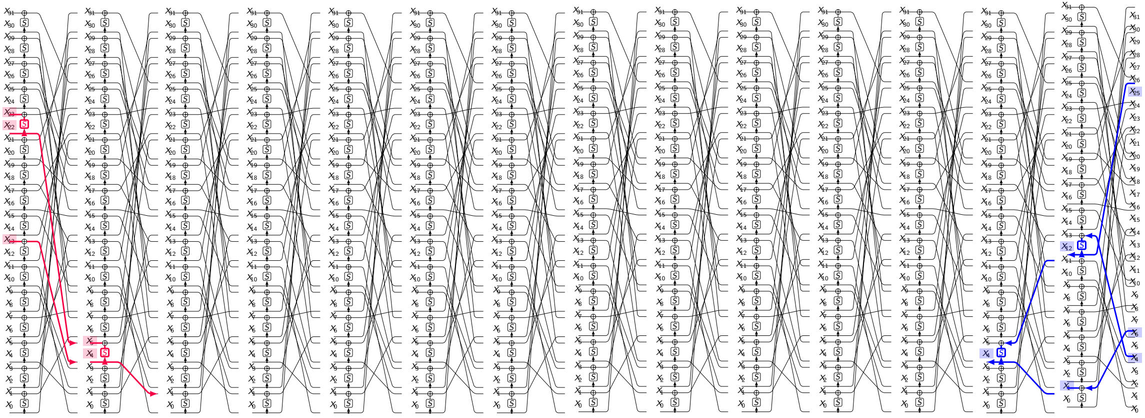


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ $q = 2^{-4}$

E_0 E_1

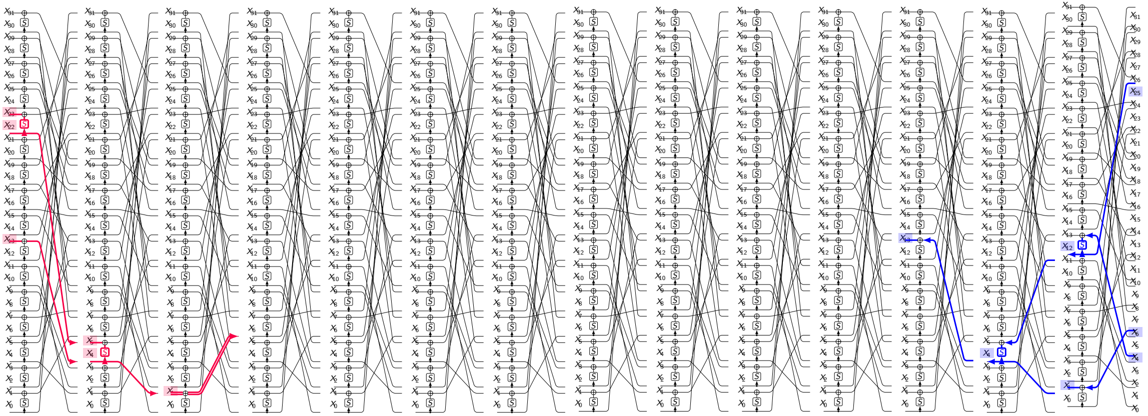


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ E_0

$q = 2^{-4}$ E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

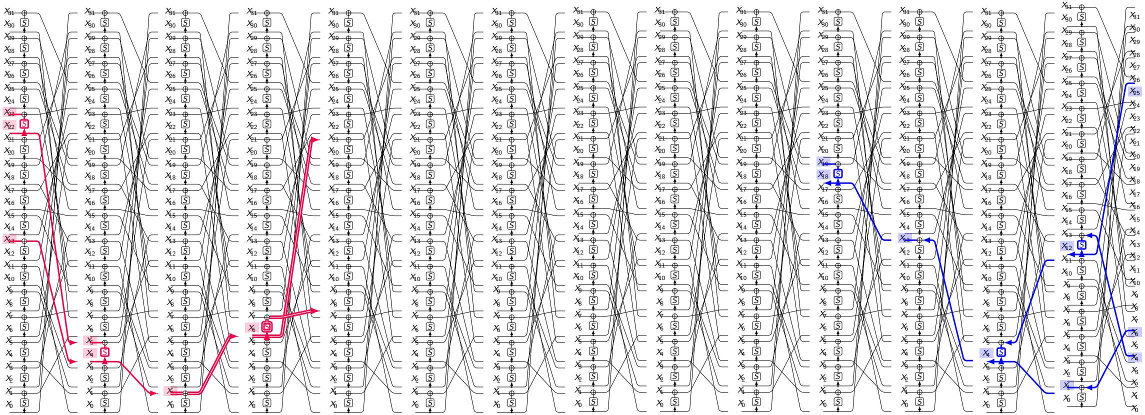
14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$

E_0

$q = 2^{-4}$

E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

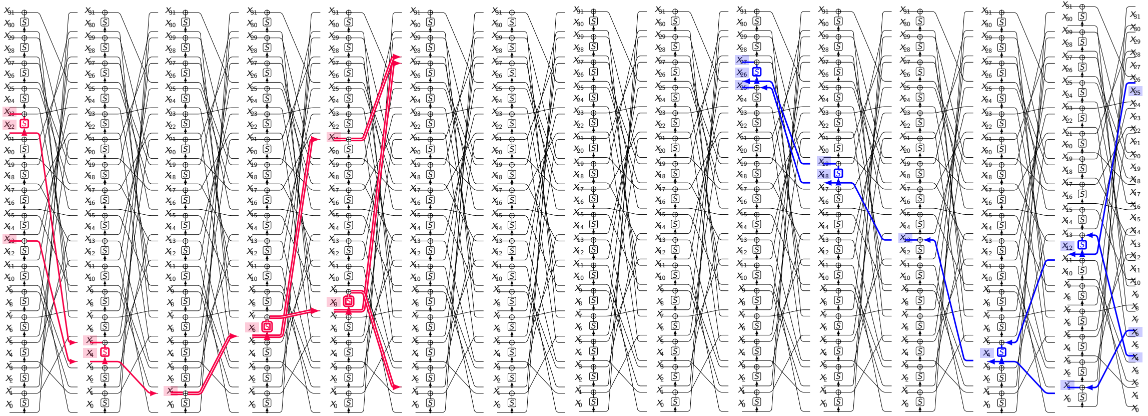
14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$

E_0

$q = 2^{-4}$

E_1

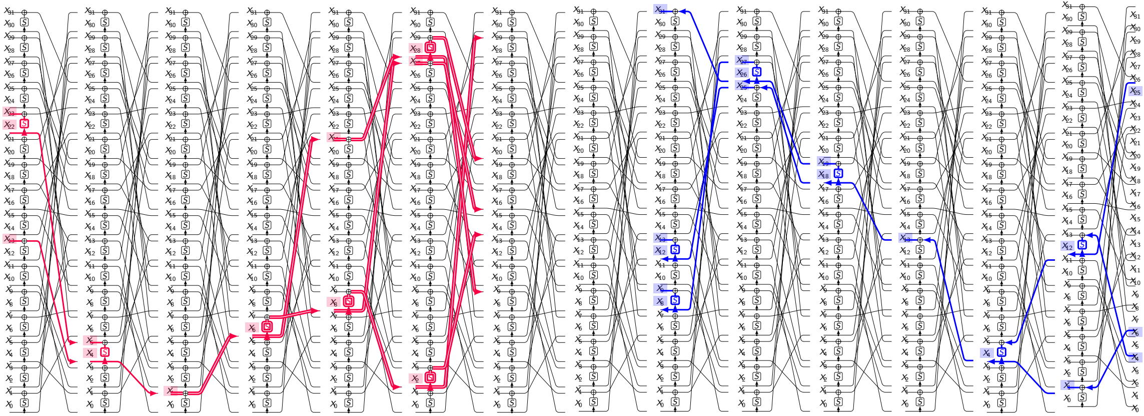


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ E_0

$q = 2^{-4}$ E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

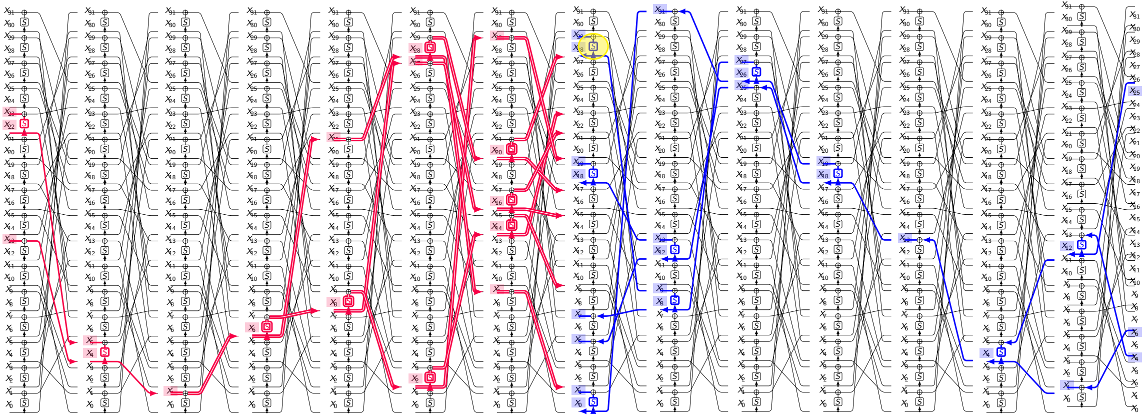
14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$

E_0

$q = 2^{-4}$

E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

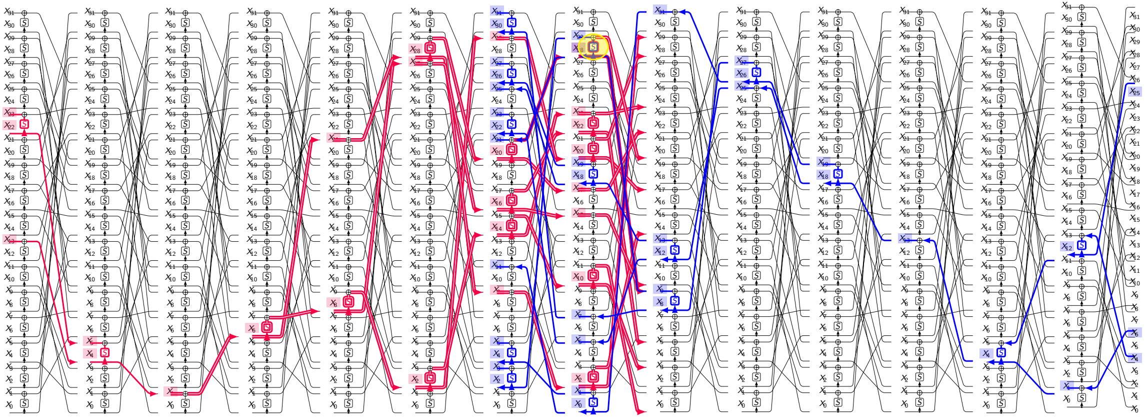
14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$

E_0

$q = 2^{-4}$

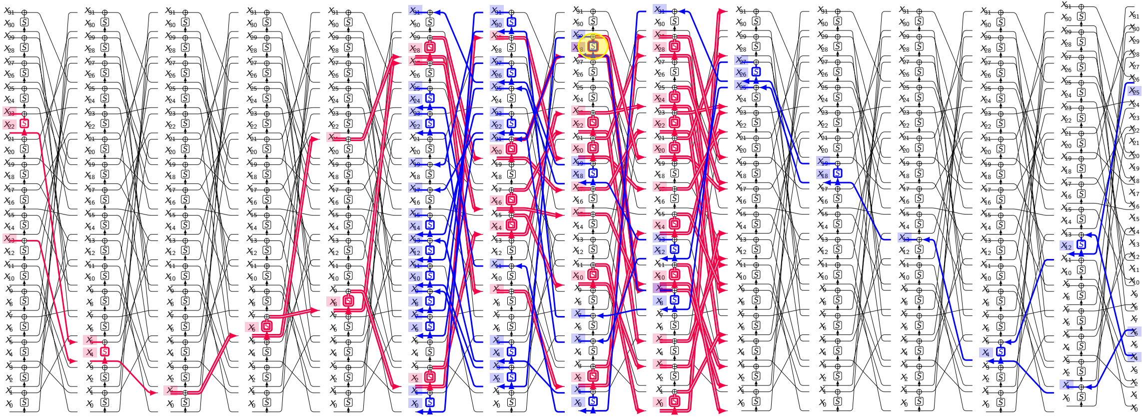
E_1



14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ E_0

$q = 2^{-4}$ E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

FSE 2023 - Kobe, Japan

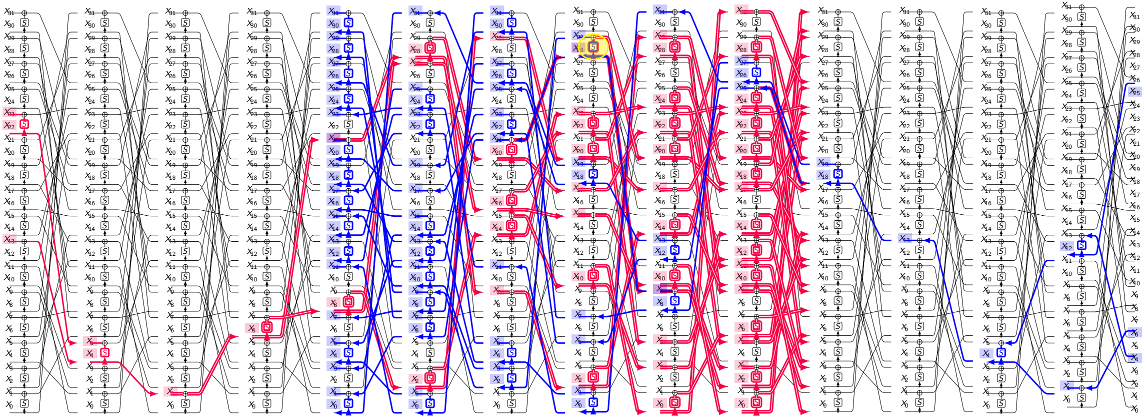
14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$

E_0

$q = 2^{-4}$

E_1

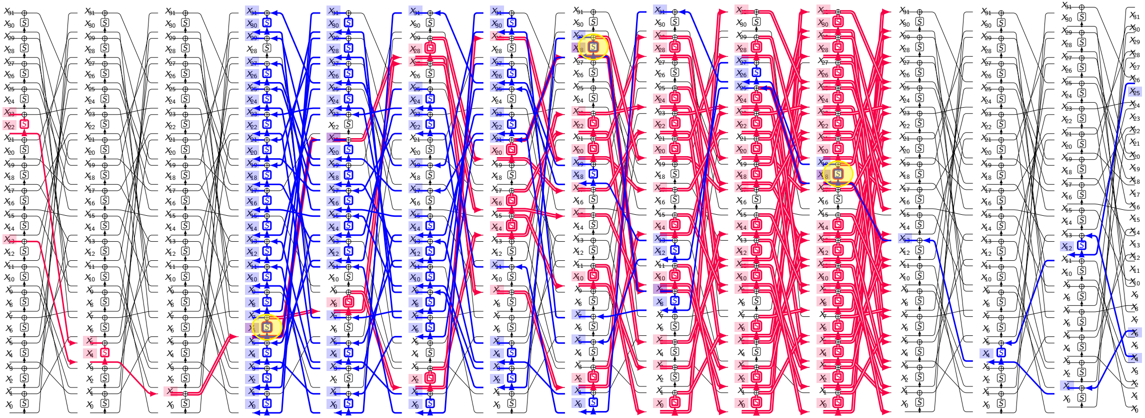


Hosein Hadipour, Marcel Nageler, Maria Eichlseder

14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ E_0

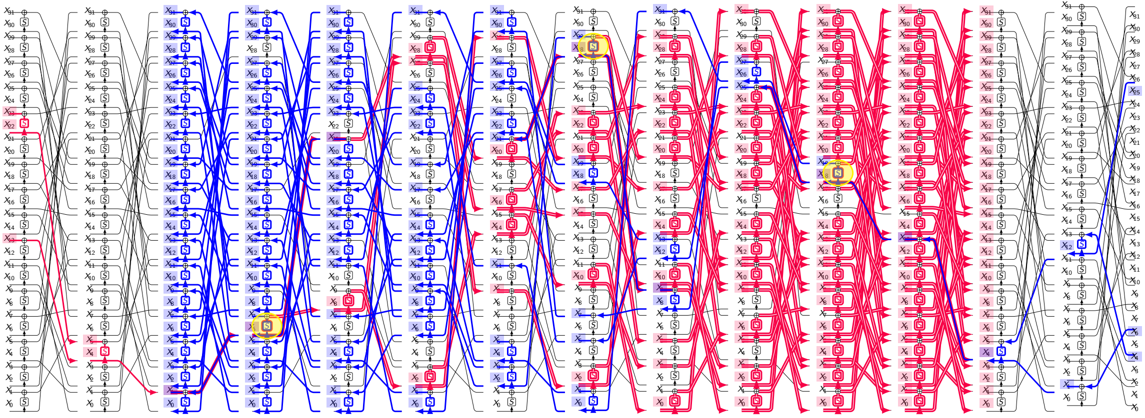
$q = 2^{-4}$ E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ E_0 $r = 2^{-4.58}$ E_m $q = 2^{-4}$ E_1



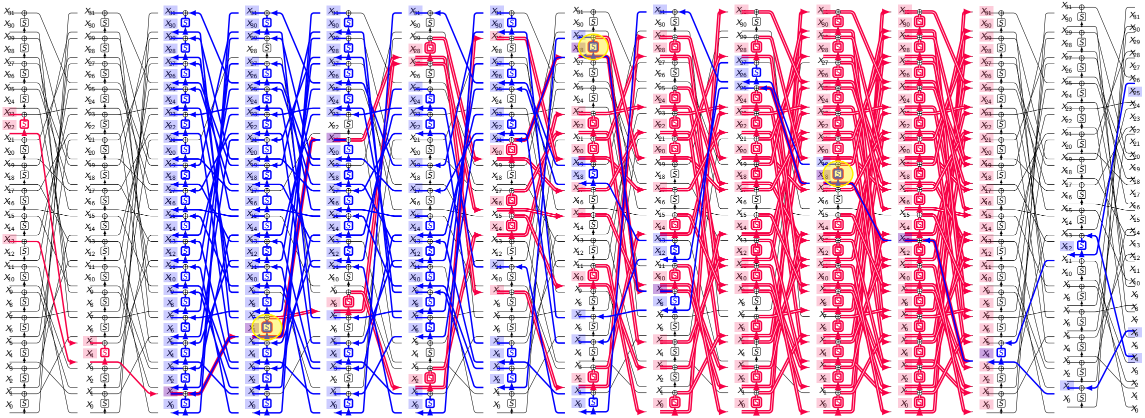
14-Round Boomerang Distinguisher for WARP

$p = 2^{-4}$ E_0

$r = 2^{-4.58}$ E_m

$p^2 q^2 r = 2^{-20.58}$

$q = 2^{-4}$ E_1



Hosein Hadipour, Marcel Nageler, Maria Eichlseder

Our Discoveries for WARP

Block cipher	#Rounds	Probability	Reference
WARP	20 / 40	$2^{-114.24}$	[TB22]
	20 / 40	$2^{-75.96}$	This paper
	21 / 40	$2^{-121.11}$	[TB22]
	21 / 40	$2^{-84.55}$	This paper
	22 / 40	$2^{-96.55}$	This paper
	23 / 40	$2^{-115.59}$	This paper

Conclusion

Our Main Contribution

- We provided an easy to use and fast method to find boomerang distinguishers
- We improved the boomerang distinguisher/attack of CLEFIA by 1 round
- We improved the boomerang distinguisher of WARP by 2 rounds
- Our method is applicable to any strongly aligned S-box based block cipher

Thanks for your attention!

: https://github.com/hadipourh/comeback

: https://github.com/hadipourh/sboxanalyzer

Bibliography I

[Ban+20] Subhadeep Banik et al. **WARP: Revisiting GFN for Lightweight 128-Bit Block Cipher**. SAC 2020. Vol. 12804. LNCS. Springer, 2020, pp. 535–564. DOI: 10.1007/978-3-030-81652-0_21.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. **A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony**. CRYPTO. Vol. 6223. Lecture Notes in Computer Science. Springer, 2010, pp. 393–410. DOI: 10.1007/978-3-642-14623-7_21.

[HBS21] Hosein Hadipour, Nasour Bagheri, and Ling Song. **Improved Rectangle Attacks on SKINNY and CRAFT**. *IACR Trans. Symmetric Cryptol.* 2021.2 (2021), pp. 140–198. DOI: 10.46586/tosc.v2021.i2.140-198.

[PT22] Thomas Peyrin and Quan Quan Tan. **Mind Your Path: On (Key) Dependencies in Differential Characteristics**. *IACR Trans. Symmetric Cryptol.* 2022.4 (2022), pp. 179–207. DOI: 10.46586/tosc.v2022.i4.179-207. URL: https://doi.org/10.46586/tosc.v2022.i4.179-207.

Bibliography II

[TB22] Je Sen Teh and Alex Biryukov. **Differential cryptanalysis of WARP**. *J. Inf. Secur. Appl.* 70 (2022), p. 103316. DOI: 10.1016/j.jisa.2022.103316.

[Wag99] David A. Wagner. **The Boomerang Attack**. FSE. Vol. 1636. Lecture Notes in Computer Science. Springer, 1999, pp. 156–170. DOI: 10.1007/3-540-48519-8_12.

FBCT of WARP

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