AUTOMATIC SEARCH OF RECTANGLE ATTACKS ON FEISTEL CIPHERS

Application to WARP

Virginie Lallemand[1], Marine Minier[1], **Loïc Rouquette**[1,2]

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

CITI, INRIA, INSA Lyon, Villeurbanne, France

March, 21st 2023

Slides: 20

Table of contents

1 Differential Crytanalysis and Boomerang Attacks

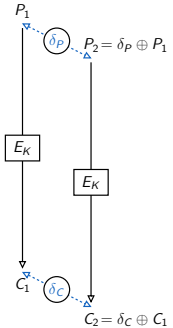
2 Automatic Search of Rectangle Attacks on WARP

3 Outlooks and Conclusion

Differential Crytanalysis and Boomerang Attacks

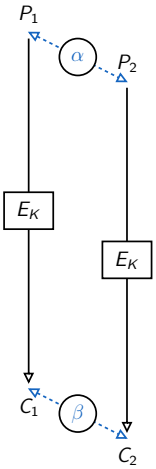
Differential Cryptanalysis [BS91]

- Symmetric ciphers
- Differential Cryptanalysis

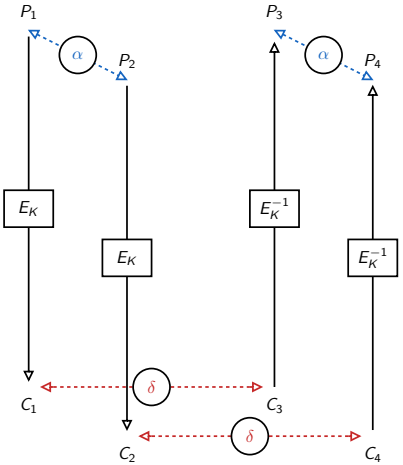


$$\mathbb{P}(\delta_P \rightsquigarrow \delta_C)?$$

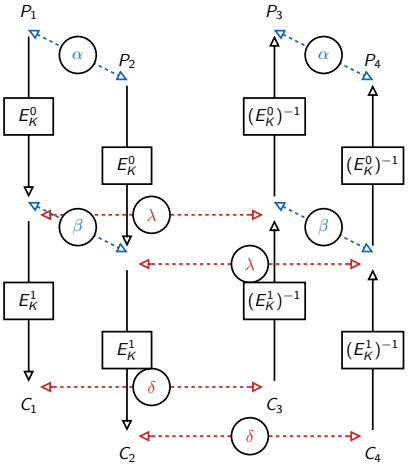
Boomerang [Wag99]



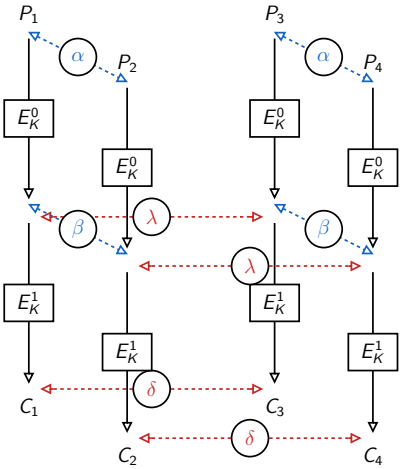
Boomerang [Wag99]



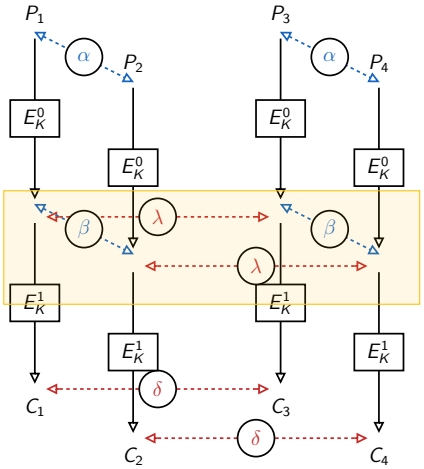
Boomerang [Wag99]



Rectangle Attack [BDK01]



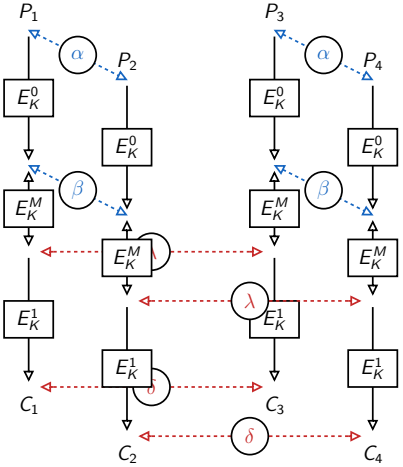
Rectangle Attack [BDK01]



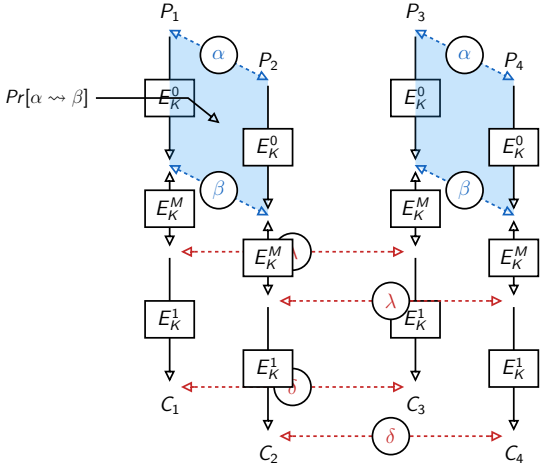
Are the two trails compatibles ?

Sometimes better [BK09]
Sometimes worst [Mur11]

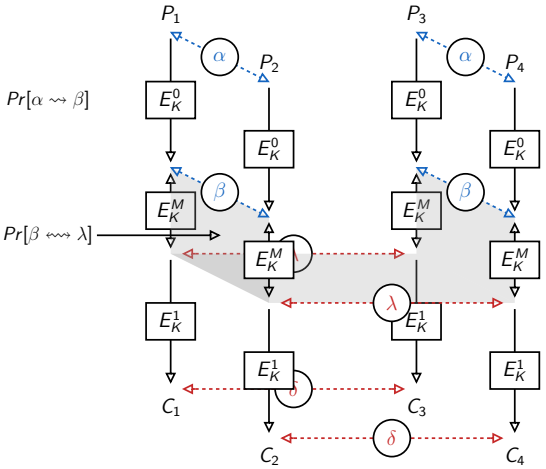
Sandwich Attack [DKS10]



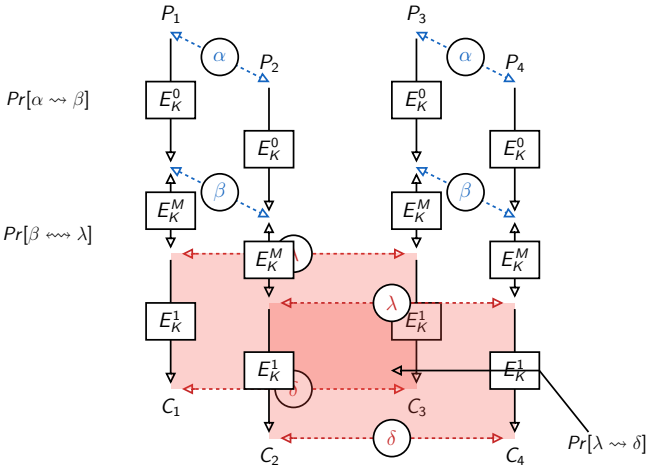
Sandwich Attack [DKS10]



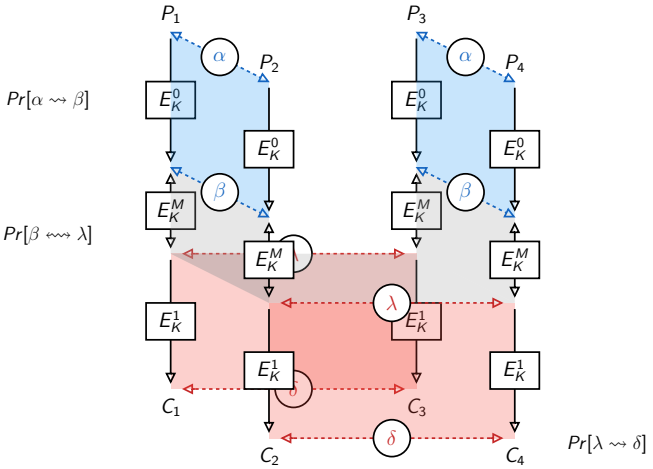
Sandwich Attack [DKS10]



Sandwich Attack [DKS10]

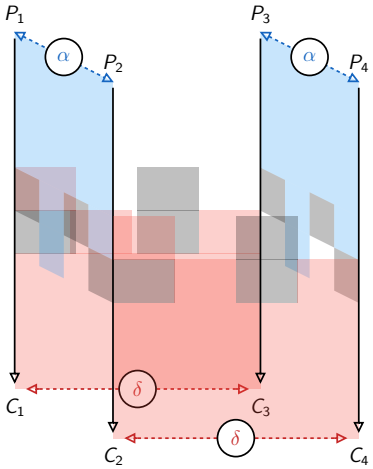


Sandwich Attack [DKS10]

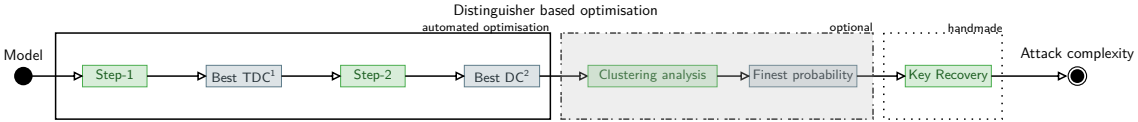


$$Pr[\alpha \leftrightsquigarrow \delta] = Pr[\alpha \rightsquigarrow \beta]^2 \times Pr[\beta \leftrightsquigarrow \lambda] \times Pr[\lambda \rightsquigarrow \delta]^2$$

Model of Delaune et al. [DDV20]

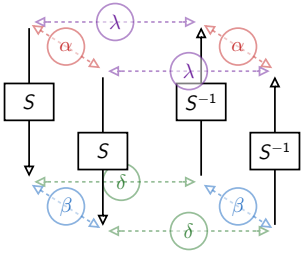


2 Steps (+KeyRecovery) solving process

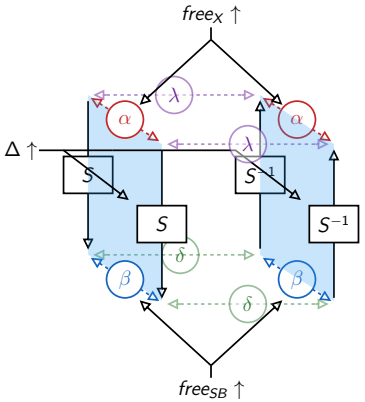


[1]: Truncated Differential Characteristic
[2]: Differential Characteristic

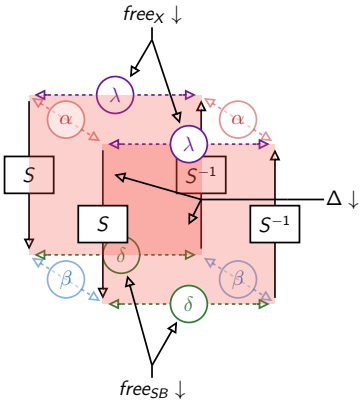
Boomerang Transition in the Model of Delaune et al.



Boomerang Transition in the Model of Delaune et al.



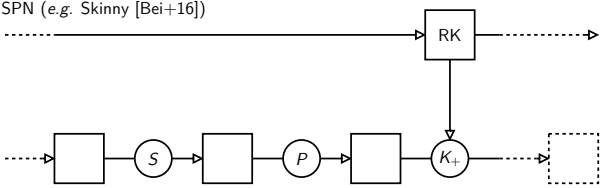
Boomerang Transition in the Model of Delaune et al.



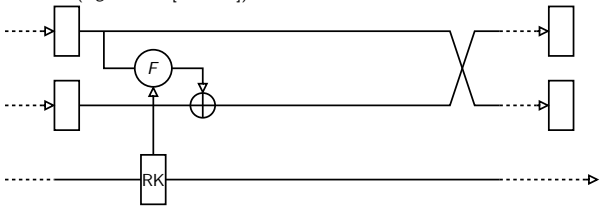
Motivation

Adapt the model of Delaune et al. to Feistel Networks

SPN (*e.g.* Skinny [Bei+16])



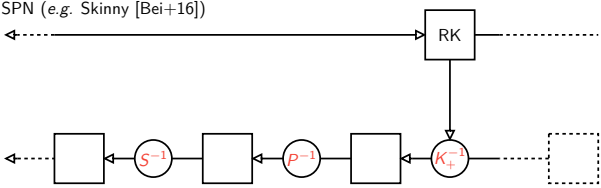
Feistel Network (*e.g.* WARP [Ban+20])



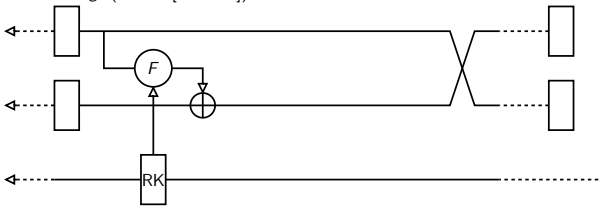
Motivation

Adapt the model of Delaune et al. to Feistel Networks

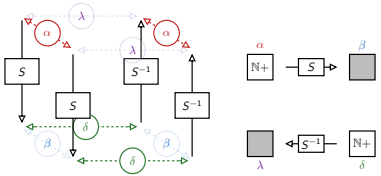
SPN (*e.g.* Skinny [Bei+16])



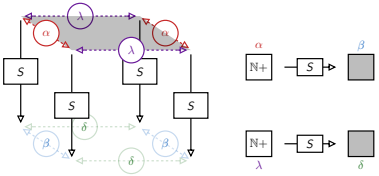
Feistel Network *e.g.* (WARP [Ban+20])



SPN vs Feistel Boomerang Transitions



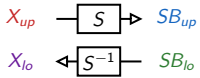
BCT [Cid+18]



FBCT [Bou+20]

S-Box Rules

Delaune et al.



- Rule 1

$$free_{Xup} \implies free_{SBup}$$
$$free_{SBlo} \implies free_{Xlo}$$

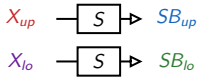
- Rule 2

$$free_{SBup} \implies \Delta_{Xup}$$
$$free_{Xlo} \implies \Delta_{Xlo}$$

- Rule 3

$$\neg free_{Xup} \vee \neg free_{Xlo}$$
$$\neg free_{SBup} \vee \neg free_{SBlo}$$

Feistel Adaptation



- Rule 1

$$free_{Xup} \implies free_{SBup}$$
$$free_{Xlo} \implies free_{SBlo}$$

- Rule 2

$$free_{SBup} \implies \Delta_{Xup}$$
$$free_{SBlo} \implies \Delta_{Xlo}$$

- Rule 3

$$\neg free_{Xup} \vee \neg free_{SBlo}$$
$$\neg free_{Xlo} \vee \neg free_{SBup}$$

Automatic Search of Rectangle Attacks on WARP

WARP

- Presented at SAC 2020 by Banik et al. [Ban+20]
- Compact hardware implementation
- 128-bit key and block (41 rounds)

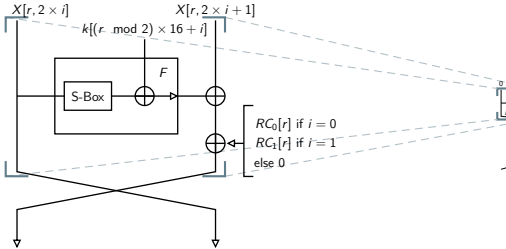


FIGURE 1 Close-up of two branches

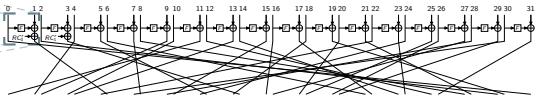


FIGURE 2 One round of WARP

Similarities with Delaune et al.'s model?

- The boomerang representation
- The search steps

Differences with Delaune et al.'s model?

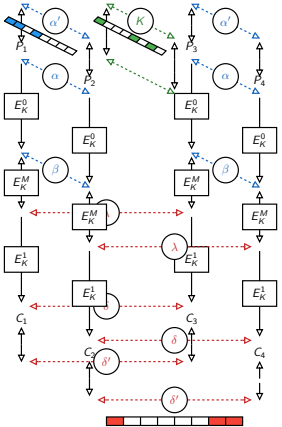
- Specific optimizations dedicated to WARP
- The S-Box representation
  - S-Box rules
  - Transition tables
- **Integration of the attack complexity in the optimisation process**

Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$

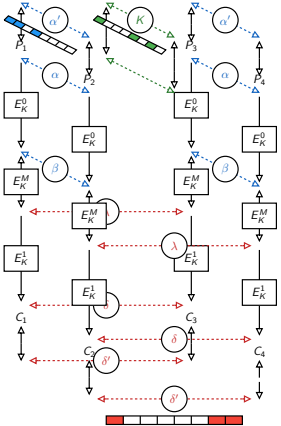


Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$

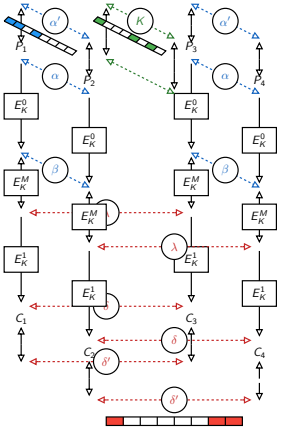


Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$

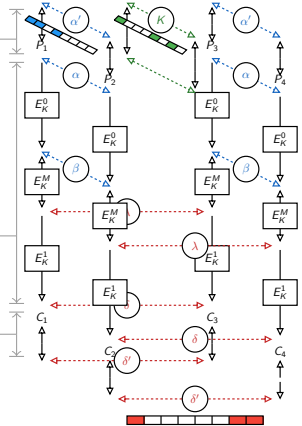


Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$

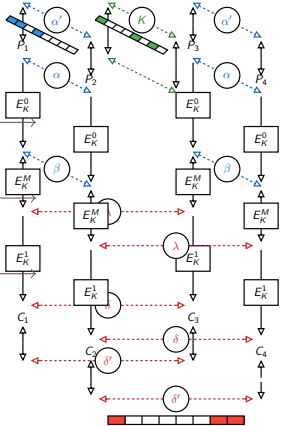


Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f} / (p^2q^2r)$$

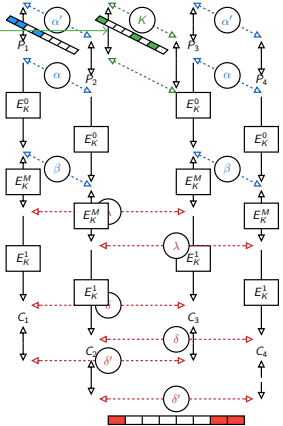


Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$

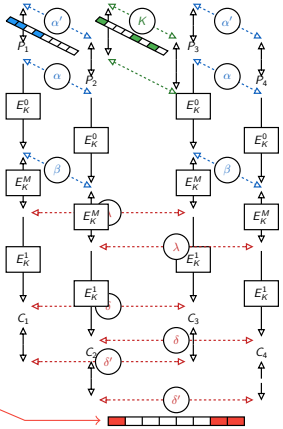


Key Recovery Automatisation

Attack of Zhao and co-authors [Zha+20]

$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$

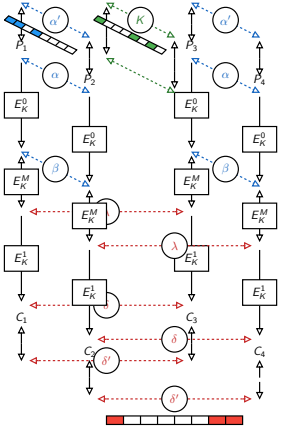


Key Recovery Automatisation

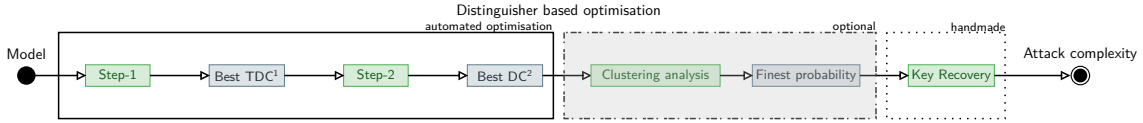
Attack of Zhao and co-authors [Zha+20]

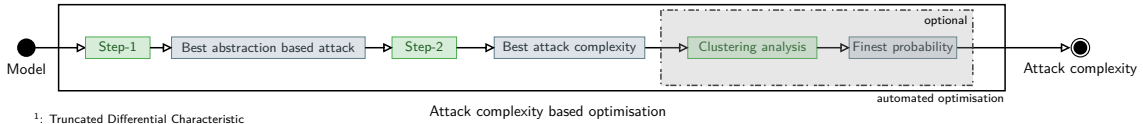
$$2^{m_b+n/2} \cdot \sqrt{s} \cdot \frac{1}{\sqrt{p^2q^2r}} \cdot \frac{N_b}{N_b+N_d+N_f}$$

$$2^{m_b-n+2r_f}/(p^2q^2r)$$



Optimisation Process





[1]: Truncated Differential Characteristic
[2]: Differential Characteristic

Results on WARP

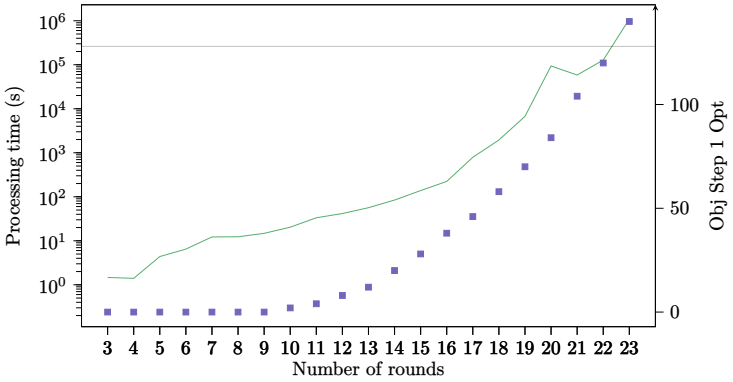


FIGURE 3

Execution time for Step-1 and Step-2 (—).
Best probability found with Step-1 Opt (■).
The black line corresponds to the probability 2^{-128}.

Experimental evaluation

Rounds	Model	Experiment	Number of tries
3	2^{0}	2^{0}	$2^{4} \times 16$
4	2^{0}	2^{0}	$2^{4} \times 16$
5	2^{0}	2^{0}	$2^{4} \times 16$
6	2^{0}	2^{0}	$2^{4} \times 16$
7	2^{0}	2^{0}	$2^{4} \times 16$
8	2^{0}	2^{0}	$2^{4} \times 16$
9	2^{0}	2^{0}	$2^{4} \times 16$
10	2^{-2}	$2^{-1.93}$	$2^{6} \times 16$
11	2^{-4}	$2^{-3.94}$	$2^{8} \times 16$
12	2^{-8}	$2^{-6.39}$	$2^{12} \times 16$
13	2^{-12}	$2^{-8.80}$	$2^{16} \times 16$
14	2^{-20}	$2^{-18.02}$	$2^{24} \times 16$
15	2^{-28}	$2^{-25.65}$	$2^{28} \times 16$
16	2^{-38}	$2^{-35.65}$	$2^{36} \times 11$

TABLE 1 The experimental evaluation of our Model on Warp.

The source code is available at:
`https://gitlab.inria.fr/lrouquet/boomerang-distinguisher-experimental-evaluation-on-WARP`

Results on WARP

Technique	Rounds	Probability	Time	Data	Mem.	Ref.
DC distinguisher	18	2^{-122}	-	-	-	[KY21]
DC distinguisher	20	$2^{-122.71}$	-	-	-	[TB22]
ID distinguisher	21	1	-	-	-	[Ban+20]
Boomerang distinguisher	21	$2^{-121.11}$	-	-	-	[TB22]
Boomerang distinguisher	23	2^{-124}	-	-	-	[This Work]
Boomerang distinguisher	23	$2^{-115.59}$	-	-	-	[HNE22]
Differential attack	21	-	2^{113}	2^{113}	2^{72}	[KY21]
Differential attack	23	-	$2^{106.68}$	$2^{106.62}$	$2^{106.62}$	[TB22]
Rectangle attack	24	-	$2^{125.18}$	$2^{126.06}$	$2^{127.06}$	[TB22]
Rectangle attack	26	-	$2^{115.9}$	$2^{120.6}$	$2^{120.6}$	[This Work]

Results on TWINE and LBlock-s

Cipher	Distinguishers	Rounds	Probability	Ref.
TWINE	Boomerang distinguisher	15	$2^{-58.92}$	[TB22]
TWINE	Boomerang Distinguisher + Clustering	15	$2^{-47.7}$	[This Work]
TWINE	Boomerang Distinguisher	15	$2^{-51.03}$	[HNE22]
TWINE	Boomerang distinguisher	16	$2^{-61.62}$	[TB22]
TWINE	Boomerang Distinguisher + Clustering	16	$2^{-59.8}$	[This Work]
TWINE	Boomerang Distinguisher	16	$2^{-58.04}$	[HNE22]
LBlock-s	Boomerang distinguisher	15	$2^{-58.64}$	[TB22]
LBlock-s	Boomerang Distinguisher + Clustering	16	$2^{-56.14}$	[Bou+20]
LBlock-s	Boomerang Distinguisher + Clustering	16	$2^{-54.8}$	[This Work]
LBlock-s	Boomerang Distinguisher	16	$2^{-53.59}$	[HNE22]

Outlooks and Conclusion

Summary

- We provide an automatic tool to search rectangle attacks on WARP
- The model can be easily adapted to other Feistel networks
- The model can be overtaken by the model of [HNE22] when the clustering effect is important
- We make a concession on distinguisher probabilities in favour of the lower attack complexities

Further search

- Integration of Boomerang and Rectangle attacks in Tagada [Lib+21]

[Ban+20] Subhadeep Banik, Zhenzhen Bao, Takanori Isobe, Hiroyasu Kubo, Fukang Liu, Kazuhiko Minematsu, Kosei Sakamoto, Nao Shibata, and Maki Shigeri. "WARP : Revisiting GFN for Lightweight 128-Bit Block Cipher". In: *SAC 2020*. LNCS. Springer, Heidelberg, 2020, pp. 535–564. DOI: 10.1007/978-3-030-81652-0_21.

[BDK01] Eli Biham, Orr Dunkelman, and Nathan Keller. "The Rectangle Attack - Rectangling the Serpent". In: *EUROCRYPT 2001*. Ed. by Birgit Pfitzmann. Vol. 2045. LNCS. Springer, Heidelberg, May 2001, pp. 340–357. DOI: 10.1007/3-540-44987-6_21.

[Bei+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. "The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS". In: *CRYPTO 2016, Part II*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9815. LNCS. Springer, Heidelberg, Aug. 2016, pp. 123–153. DOI: 10.1007/978-3-662-53008-5_5.

[BK09] Alex Biryukov and Dmitry Khovratovich. "Related-Key Cryptanalysis of the Full AES-192 and AES-256". In: *ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Vol. 5912. LNCS. Springer, Heidelberg, Dec. 2009, pp. 1–18. DOI: 10.1007/978-3-642-10366-7_1.

[Bou+20] Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, and Marine Minier. "On the Feistel Counterpart of the Boomerang Connectivity Table (Long Paper)". In: *IACR Trans. Symm. Cryptol.* 2020.1 (2020), pp. 331–362. ISSN: 2519-173X. DOI: 10.13154/tosc.v2020.i1.331-362.

[BS91] Eli Biham and Adi Shamir. "Differential Cryptanalysis of DES-like Cryptosystems". In: *CRYPTO'90*. Ed. by Alfred J. Menezes and Scott A. Vanstone. Vol. 537. LNCS. Springer, Heidelberg, Aug. 1991, pp. 2–21. DOI: 10.1007/3-540-38424-3_1.

[Cid+18] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. "Boomerang Connectivity Table: A New Cryptanalysis Tool". In: *EUROCRYPT 2018, Part II*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Vol. 10821. LNCS. Springer, Heidelberg, Apr. 2018, pp. 683–714. DOI: 10.1007/978-3-319-78375-8_22.

[DDV20] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. "Catching the Fastest Boomerangs Application to SKINNY". In: *IACR Trans. Symm. Cryptol.* 2020.4 (2020), pp. 104–129. ISSN: 2519-173X. DOI: 10.46586/tosc.v2020.i4.104-129.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. "A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony". In: *CRYPTO 2010*. Ed. by Tal Rabin. Vol. 6223. LNCS. Springer, Heidelberg, Aug. 2010, pp. 393–410. DOI: 10.1007/978-3-642-14623-7_21.

[HNE22] Hosein Hadipour, Marcel Nageler, and Maria Eichlseder. "Throwing Boomerangs into Feistel Structures: Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE". In: *IACR Transactions on Symmetric Cryptology* 2022.3 (Sept. 2022), pp. 271–302. DOI: 10.46586/tosc.v2022.i3.271-302. URL: https://tosc.iacr.org/index.php/ToSC/article/view/9858.

[KY21] Manoj Kumar and Tarun Yadav. "MILP Based Differential Attack on Round Reduced WARP". In: *Security, Privacy, and Applied Cryptography Engineering - 11th International Conference, SPACE 2021, Kolkata, India, December 10-13, 2021, Proceedings*. Ed. by Lejla Batina, Stjepan Picek, and Mainack Mondal. Vol. 13162. Lecture Notes in Computer Science. Springer, 2021, pp. 42–59. DOI: 10.1007/978-3-030-95085-9_3. URL: https://doi.org/10.1007/978-3-030-95085-9%5C_3.

[Lib+21] Luc Libralesso, François Delobel, Pascal Lafourcade, and Christine Solnon. "Automatic Generation of Declarative Models For Differential Cryptanalysis". In: *CP*. Vol. 210. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 40:1–40:18.

[Mur11] Sean Murphy. "The Return of the Cryptographic Boomerang". In: *IEEE Trans. Inf. Theory* 57.4 (2011), pp. 2517–2521.

[TB22] Je Sen Teh and Alex Biryukov. "Differential cryptanalysis of WARP". In: *Journal of Information Security and Applications* 70 (2022), p. 103316. ISSN: 2214-2126. DOI: https://doi.org/10.1016/j.jisa.2022.103316. URL: https://www.sciencedirect.com/science/article/pii/S2214212622001648.

[Wag99] David Wagner. "The Boomerang Attack". In: *FSE'99*. Ed. by Lars R. Knudsen. Vol. 1636. LNCS. Springer, Heidelberg, Mar. 1999, pp. 156–170. DOI: 10.1007/3-540-48519-8_12.

[Zha+20] Boxin Zhao, Xiaoyang Dong, Willi Meier, Keting Jia, and Gaoli Wang. "Generalized related-key rectangle attacks on block ciphers with linear key schedule: applications to SKINNY and GIFT". In: *Des. Codes Cryptogr.* 88.6 (2020), pp. 1103–1126.