New Differential Bounds and Division Property of LILLIPUT: Block Cipher with Extended Generalized Feistel Network

Yu Sasaki, and Yosuke Todo

NTT Secure Platform Laboratories

10/August/2016 @ SAC 2016

Security analysis of LW block cipher ***LILLIPUT*** adopting recently devised design (EGFN)

1. New bounds of the #active Sboxes
   - Lilliput is not Markov cipher. Evaluation is hard.
   - Search with Mixed Integer Linear Programing

   → designer's bounds are incorrect / get new bounds
2. Best attack with division property
   - EGFN does not increase algebraic degrees.
   - It resists standard integral attack wells, but does not resist division-property based attacks efficiently.

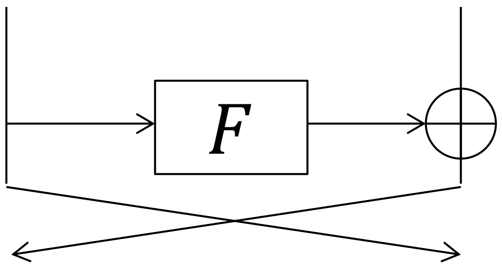
Lightweight Block Cipher

- Designing a secure/efficient block cipher is a long-term challenge in symmetric-key field.
- Lightweight cipher has been actively discussed.
  - standardization by ISO
  - lightweight workshop by NIST
- A huge number of designs were proposed in the last decade.
  - 40+ designs, e.g. PRESENT or Simon/Speck
  - Yet another one, Skinny, appears in CRYPTO 2016.

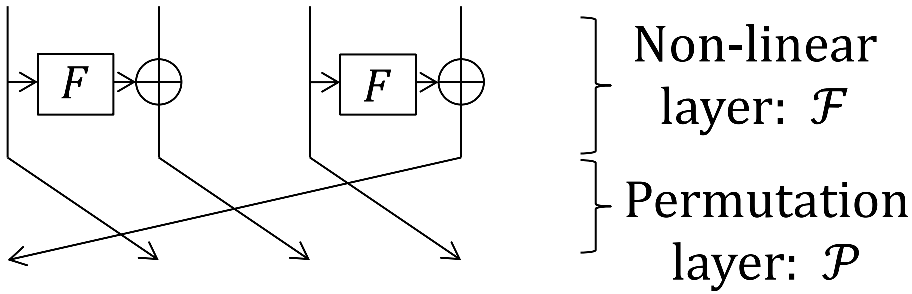
Progress of Feistel Based Designs

Feistel network is a major design approach.

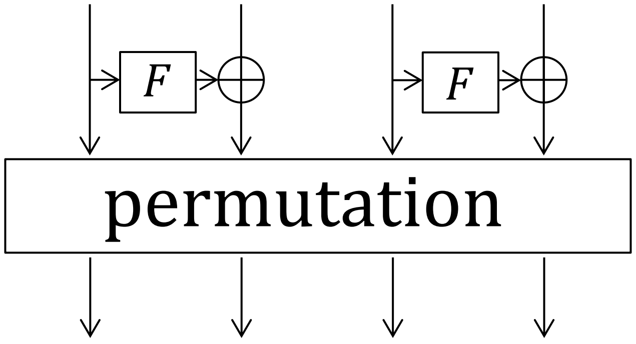
1. Feistel Network (FN)



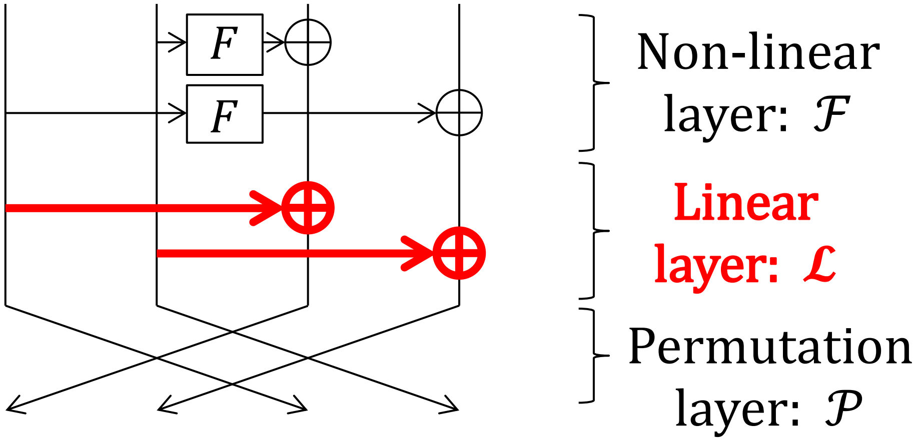
2. Generalized FN (GFN)



3. Block-shuffle GFN



4. Extended GFN (EGFN)



Extended Generalized Feistel Network (EGFN)

EGFN was proposed by Berger et al. at SAC 2013.

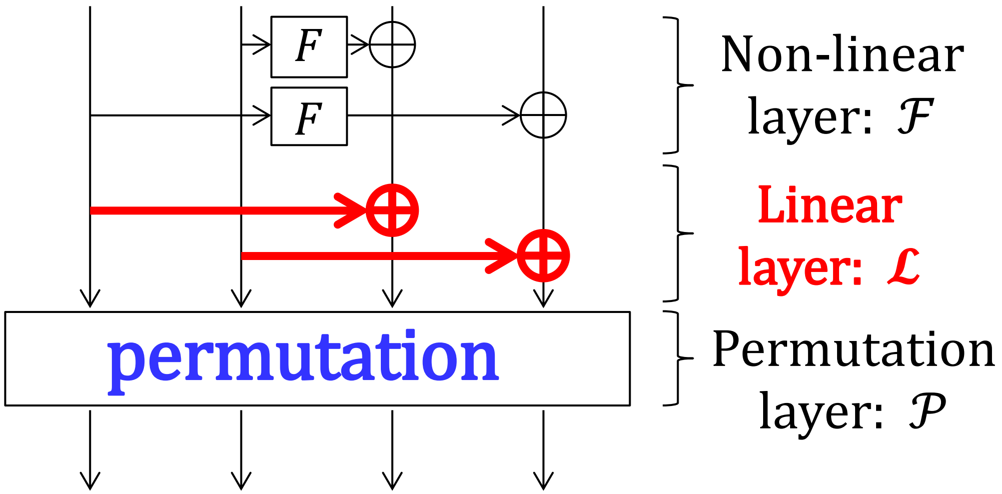
- faster diffusion
- more active S-boxes in DC and LC
- stronger security against impossible differential and integral attacks

- Permutation layer is a simple swap of each side
- Two instantiations of EGFN were specified with some security arguments.

Attack on EGFN and New Design, LILLIPUT

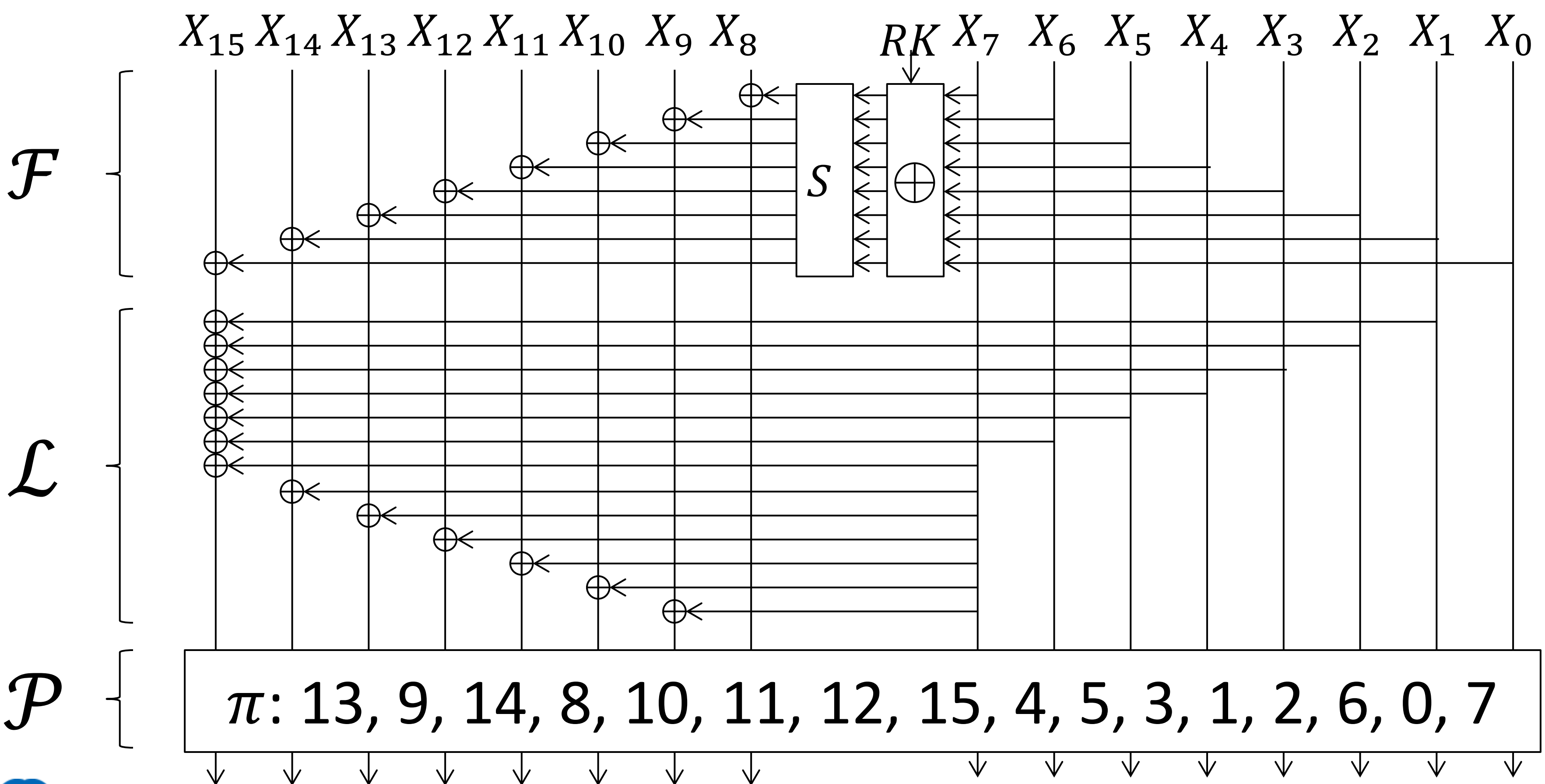
- Security argument of EGFN instances are flawed, and efficient attacks exist [ZW2014].
- The problem is caused by the simple swap of EGFN.

- Berger et al. adopted the block-shuffle.
- This is LILLIPUT [Berger++2015].



LILLIPUT Specification

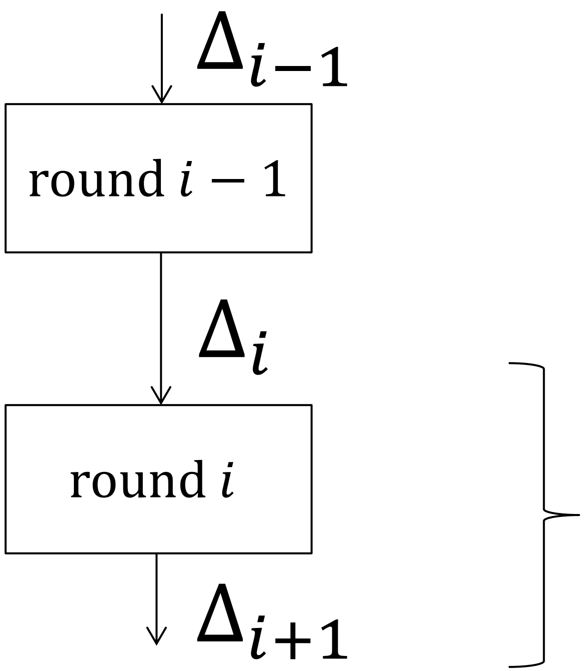
- 64-bit block, 80-bit key
- 16 branches of size 4 bits, 30 rounds



New Differential Bounds

Difficulty of Analyzing Truncated Differential

- Previous approach assumes Markov cipher

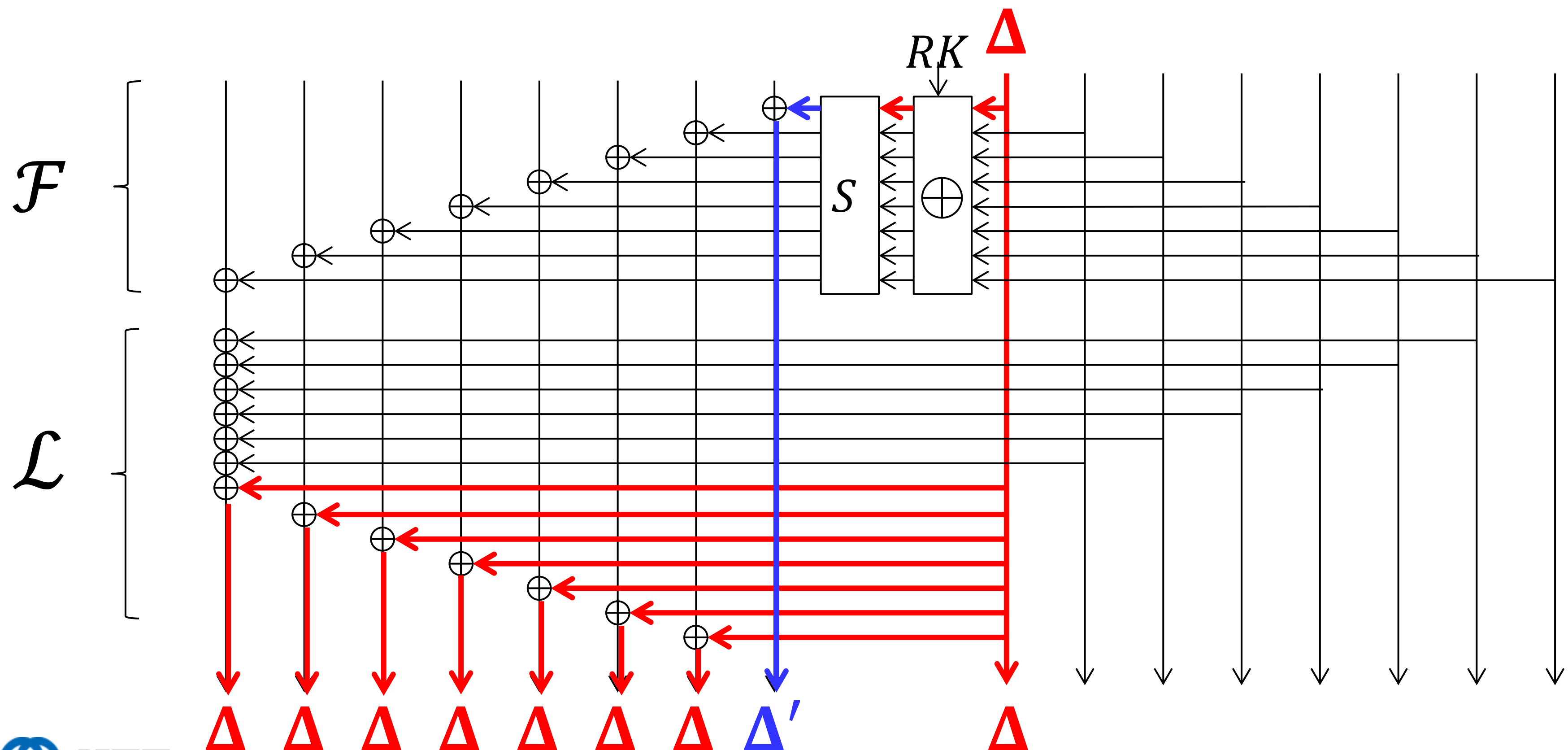


Evaluation in round i is independent from round $i - 1$.

This is true for many ciphers including AES by assuming each subkey is independent.

Difficulty of Analyzing Truncated Differential

- The assumption is not true for LILLIPUT.
- Truncated diff traces that the left 8 are active, which drops the info that the left 7 are identical.



Difficulty of Analyzing Truncated Differential

- The difficulty is caused by the linear layer, a unique structure of EGFN.
- Efficient analysis method is unknown.

Designer's Approach (Branching)

rounds															
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	2	3	5	9	12	14	15	17	21	24	26	28	29	31

- Lower bounds of the number of active S-boxes were derived with branching method. (Details are not explained)
- The bounds are tight.
    - Input and output differential masks with 31 active S-boxes for 16 rounds are claimed.

Our Approach (MILP)

- Mixed-Integer-Linear-Programming (MILP) can be used to obtain the number of active S-boxes in truncated differential [Mouha++11].
- Assumption: all nibble-differences can change into any difference in every round.
- In reality, differences cannot change via $\mathcal{L}$ layer.
- MILP only can derive lower bounds

Results

	rounds															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
designers:	0	1	2	3	5	9	12	14	15	17	21	24	26	28	29	31
Ours:	0	1	2	3	5	9	12	14	15	17	19	23	25	28	30	32

- Our bounds do not match with designers' ones. (Our code is available in the paper.)
- MILP shows that even lower bounds are higher than the original expectation by the designers.

Towards Tight Bounds (Bitwise MILP)

- Bounds for truncated diff cannot be tight.
- Sun et al. discussed bitwise differential search for ciphers with 4-bit S-boxes [Sun++2014].
  - SAGE, a tool in computational geometry
  - Logical Condition Model ✓
- tight, but slow (1 week for 11 rounds)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
designers:	0	1	2	3	5	9	12	14	15	17	21	24	26	28	29	31
Ours:	0	1	2	3	5	9	12	14	15	17	19	23	25	28	30	32
Bitwise:	0	1	2	3	5	9	12	15	17	19	22	?	?	?	?	?

Best Attack with Division Property

Division Property

- Division property is the generalization of the integral property [Todo2015].

- Start by 2^{63} plaintexts with algebraic degrees

  (4,4,4,4,4,4,4, 4,4,4,4,4,4,4,4,3).

- The *balanced* property (sum is 0) is precisely traced by considering algebraic .

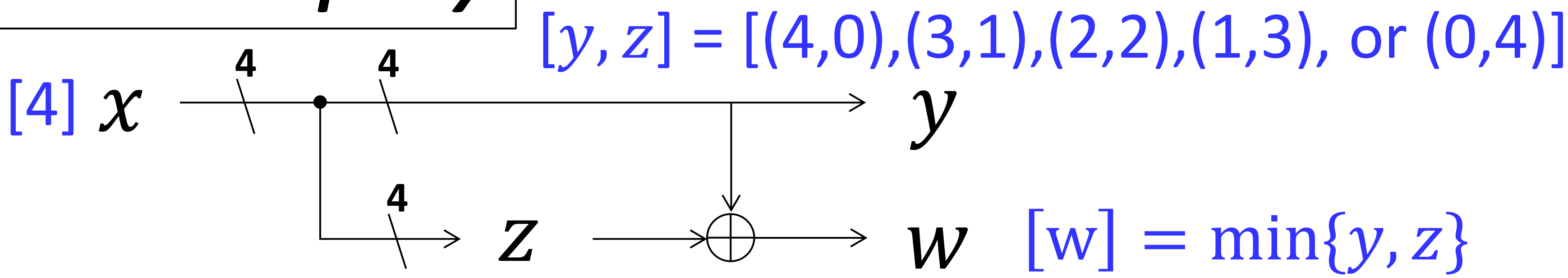
- E.g. S-box: deg 4 → deg 4,

  deg 3 or deg 2 → deg 1.

S-layer decreases algebraic degrees of the state.

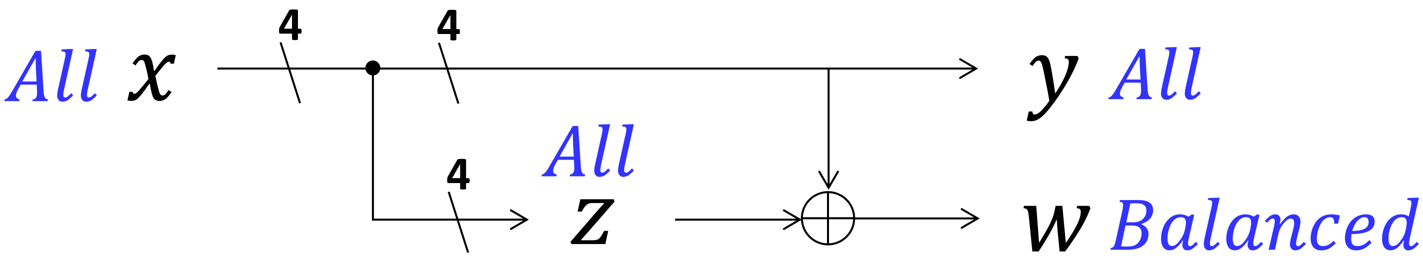
Property Propagation in Linear Layer

Division Property



L-layer does not decrease sum of algebraic degrees.

Integral Property



L-layer is effective in integral analysis.

- Additional linear layer does not contribute to reduce algebraic degrees of the whole state.

Comparison about Integral-type distinguisher

	distinguisher	#rounds
TWINE, LBlock	integral	16
EGFN (Lilliput)	integral	9
EGFN (Lilliput)	**division prop.**	**13**

Contribution of EGFN is limited (only by 3 rounds).

Results

- Our machine search found 13-round distinguisher.

(A,A,A,A,A,A,A,A, A,A,A,A,A,A,A,3)

--13R--> (U,U,U,U,U,U,B,U, U,U,U,U,U,U,U,U)

- 4-rouns are appended for key recovery, which improves the previous best attack by 3 rounds.

approaches	distinguisher	key recovery	data	time	ref.
integral	9 rounds	13 rounds	2^{62}	2^{72}	[7]
impossible differential	8 rounds	14 rounds	2^{63}	2^{77}	[7]
division property	13 rounds	17 rounds	2^{63}	2^{77}	**Ours**

Concluding Remarks

Concluding Remarks

EGFN looks efficient, but requires complicated techniques for security evaluation.

- Differential analysis:
  - Previous bounds are wrong.
  - Nibble-wise MILP: loose bounds, but fast
  - Bit-wise MILP: tight bounds, but slow
- Division property:
  - $\mathcal{L}$-layer does not increase algebraic degrees. This prevents classic integral, but not division property.
  - Current best key recovery attacks for 17 rounds.

Thank you for your attention !!

Results Summary

approach	rounds															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
branching [7]	0	1	2	3	5	9	12	14	15	17	21	24	26	28	29	31
MILP (NW, basic)	0	1	2	3	5	9	12	14	15	17	19	22	25	27	29	31
MILP (NW, advanced)	0	1	2	3	5	9	12	14	15	17	19	23	25	28	30	32
MILP (BW)	0	1	2	3	5	9	12	15	17	19	22	?	?	?	?	?

approaches	distinguisher	key recovery	data	time	ref.
integral	9 rounds	13 rounds	2^{62}	2^{72}	[7]
impossible differential	8 rounds	14 rounds	2^{63}	2^{77}	[7]
division property	13 rounds	17 rounds	2^{63}	2^{77}	**Ours**