Refined Probability of Differential Characteristics Including Dependency Between Multiple Rounds

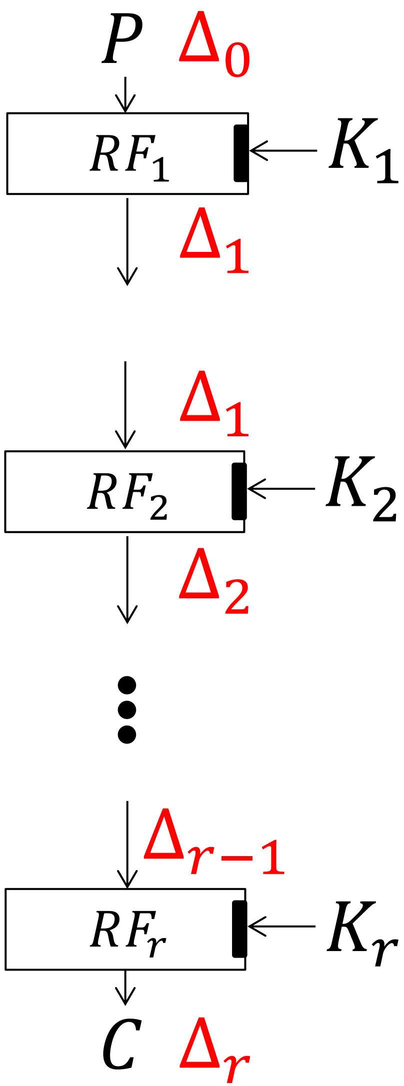
Anne Canteaut	Inria
Eran Lambooij	Technische Universiteit Eindhoven
Samuel Neves	University of Coimbra
Shahram Rasoolzadeh	Ruhr-Universität Bochum
Yu Sasaki	NTT Secure Platform Laboratories
Marc Stevens	CWI Amsterdam

7 Mar 2018 @ FSE 2018

Differential Cryptanalysis

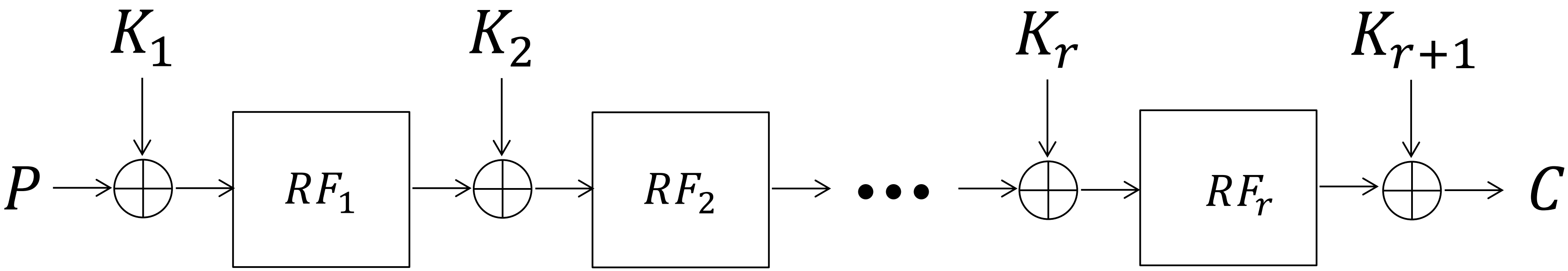
- In differential cryptanalysis, attackers construct a chain of differential propagations for each round.

- Probability for each round is often assumed to be independent.
  - $p_i = \Pr_{RF_i}[\Delta_{i-1} \rightarrow \Delta_i]$
  - $p = \prod_{i=1}^{r} p_i$



Validity of Assumption

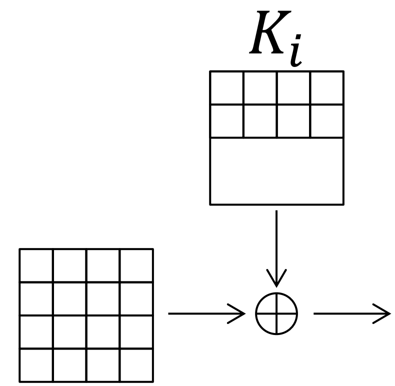
Assumption is true when each state is XORed by independently chosen subkeys before each non-linear operation.

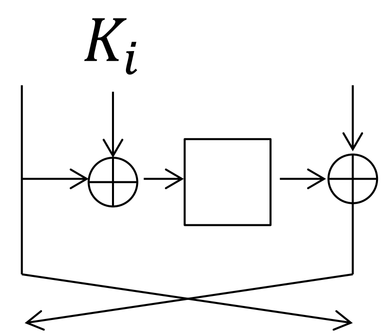


Invalidity of Assumption

Assumptions are not always true:

- Keyless primitives
  - Hash function
  - Even-Mansour construction
  - Key schedule function
- State is partially update by key
  - SPN with partial subkey XOR
  - Feistel network
- Subkeys are not independent





Our Target

- Key dependent analysis?
- Plateau characteristics?

-> decent, but analysis requires long time

This work:

- Keyless updates appear in many parts of practical designs especially in lightweight designs.
- We focus on the keyless function and give the analysis including dependency of multiple S-box layers.

Contributions of This Research

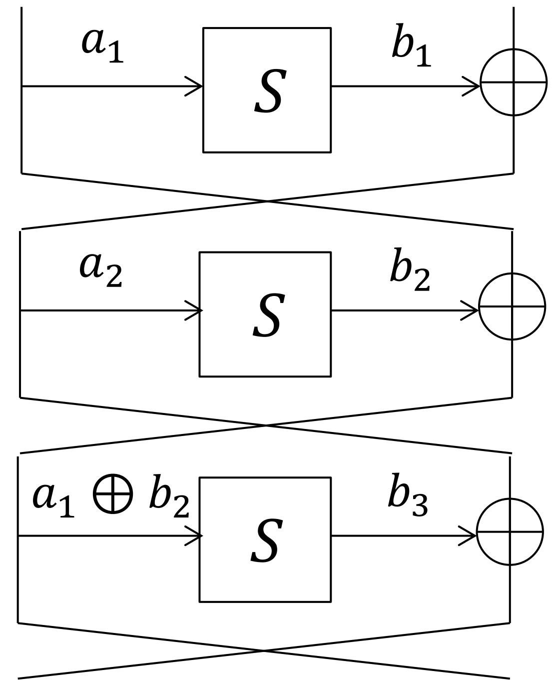
- Focus on the gap between two probabilities
  - p_{ind} : each S-box is assumed to be independent
  - p_{exact}: dependency is considered

  p_{exact} can be higher than p_{ind}.

  p_{exact} can be lower bounded.

- Generic analysis against 3-round Feistel network
  - Lower-bounding the ratio of p_{ind} to p_{exact}
- Applications in actual designs
  - RoadRunneR (Feistel)
  - Minalpher (SPN)

3-Round Feistel



Evaluation of p_{ind} and p_{exact}

p_{ind} (straightforward)

$$p_{\mathrm{ind}} = \Pr_{x_3 \in \mathbb{F}_2^n}[S(x_3 \oplus a_1 \oplus b_2) \oplus S(x_3) = b_3] \times \Pr_{x_2 \in \mathbb{F}_2^n}[S(x_2 \oplus a_2) \oplus S(x_2) = b_2] \times \Pr_{x_1 \in \mathbb{F}_2^n}[S(x_1 \oplus a_1) \oplus S(x_1) = b_1] .$$

p_{exact}

$$\mathcal{X}_S(a,b) \triangleq \{x \in \mathbb{F}_2^n : S(x \oplus a) \oplus S(x) = b\}$$

$$\mathcal{Y}_S(a,b) \triangleq \{S(x) \in \mathbb{F}_2^n : S(x \oplus a) \oplus S(x) = b\}$$

p_{exact} for the 3rd S-box is

$$\Pr_{x_1 \in \mathcal{X}_S(a_1,b_1), y_2 \in \mathcal{Y}(a_2,b_2)}[S(x_1 \oplus y_2 \oplus a_1 \oplus b_2) \oplus S(x_1 \oplus y_2)]$$

NTT

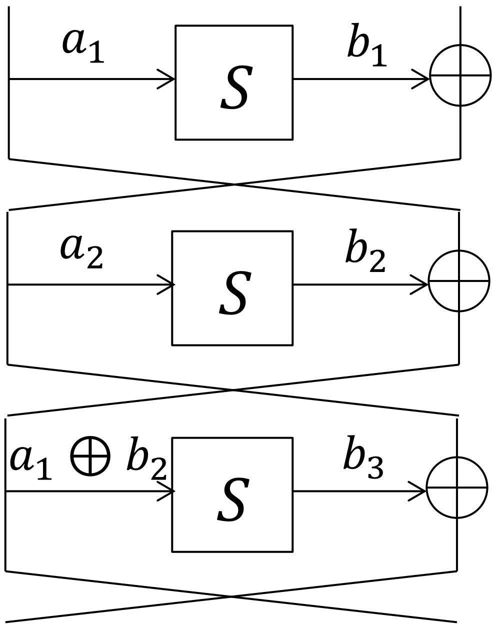
Analysis Example

- Suppose that the differential uniformity of the round function is 4.
- Define λ as $p_{exact} = \lambda \cdot p_{ind}$

λ is lower-bounded by $\max\{1, 2^{n-6}\}$.

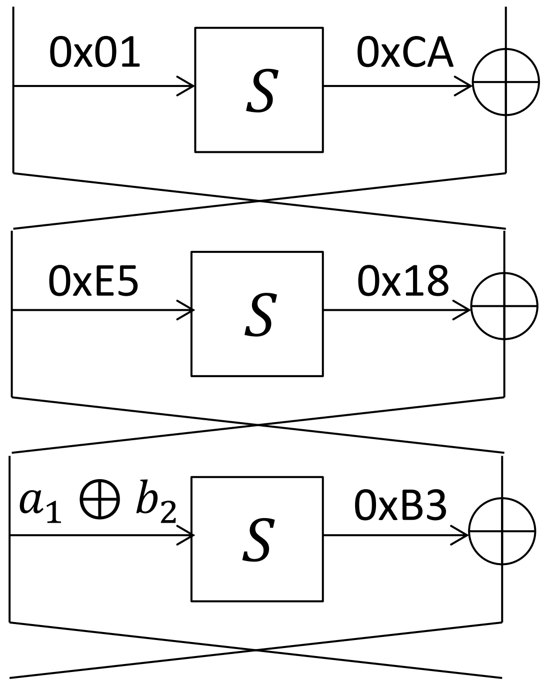
$\Rightarrow$

p_{exact} is always higher than p_{ind} when $n > 6$



- When differences are propagated with prob 2^{-n+1}, $p_{ind} = 2^{-3n+3}$, while $p_{exact} = 0 \text{ or } 2^{-2n+1}$.

Demonstration with AES-Sbox ($n = 8$)



	p_{ind}	p_{exact}
	2^{-7}	2^{-7}
	2^{-7}	2^{-7}
	2^{-7}	$0 \; or \; 2^{-1}$

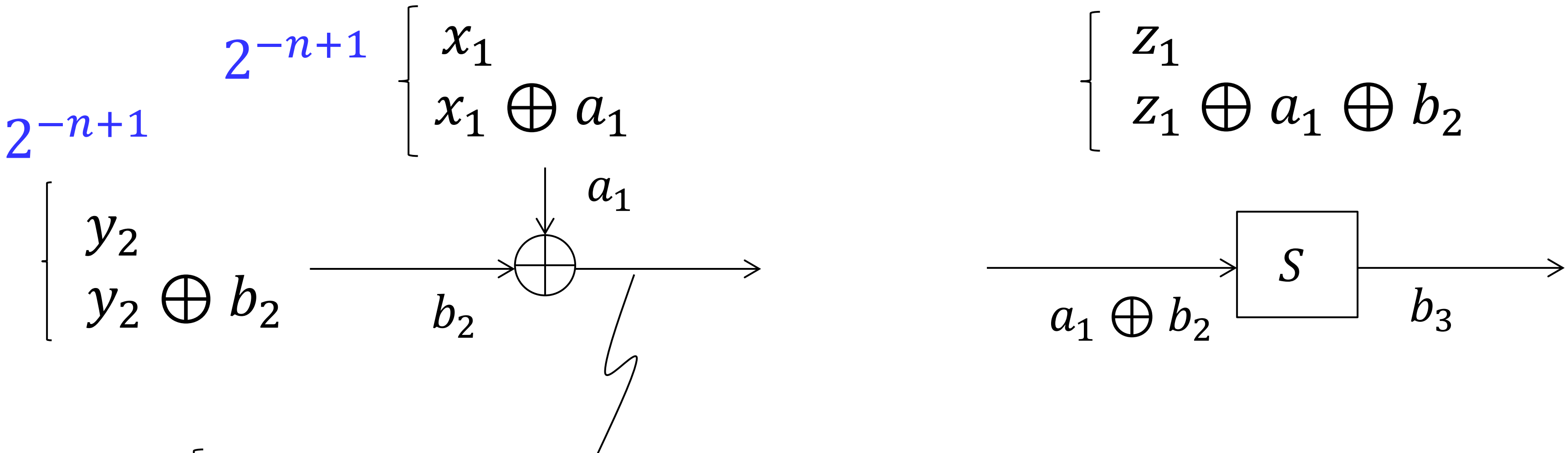
$$p_{ind} = 2^{-3\times8+3} = 2^{-21}$$

$$p_{exact} = 2^{-2\times8+1} = 2^{-15}$$

Analysis for 2^{-n+1} Transitions

The first two S-boxes are satisfied with $2^{2\times(-n+1)}$.

- $\mathcal{X}_S(a_1, b_1) = \{x_1, x_1 \oplus a_1\}$,
- $\mathcal{Y}_S(a_2, b_2) = \{y_2, y_2 \oplus b_2\}$,
- $\mathcal{X}_S(a_1 \oplus b_2, b_3) = \{z_1, z_1 \oplus a_1 \oplus b_2\}$.



$$\left\{\begin{array}{l} (x_1 \oplus y_2, \quad x_1 \oplus y_2 \oplus a_1 \oplus b_2) \\ (x_1 \oplus y_2 \oplus b_2, x_1 \oplus a_1 \oplus y_2) \end{array}\right.$$

Probability to hit z_1 is 0 *or* 2^{-1}

Generalization

- The analysis can be extended to differential transitions of any probability as long as the $\mathcal{X}_S$ and $\mathcal{Y}_S$ form affine space.

Theorem 1. *Let S be a permutation of $\mathbb{F}_2^n$, and let a_1, b_1, a_2, b_2, b_3 be five elements in $\mathbb{F}_2^n$. Assume that there exist $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_2^n$ and three linear subspaces $V_1, V_2, V_3 \subseteq \mathbb{F}_2^n$ such that*

$$\mathcal{X}_S(a_1, b_1) = \alpha_1 + V_1,\ \mathcal{Y}_S(a_2, b_2) = \alpha_2 + V_2,\ \text{and } \mathcal{X}_S(a_1 \oplus b_2, b_3) = \alpha_3 + V_3\,.$$

Then, the multiset

$$\{(x_1, x_2) \in \mathcal{X}_S(a_1, b_1) \times \mathcal{X}_S(a_2, b_2) : S(S(x_2) \oplus x_1 \oplus a_1 \oplus b_2) \oplus S(S(x_2) \oplus x_1) = b_3\}$$

is either empty or has size 2^d with

$$d = \dim V_1 + \dim V_2 + \dim V_3 - \dim(V_1 + V_2 + V_3)$$

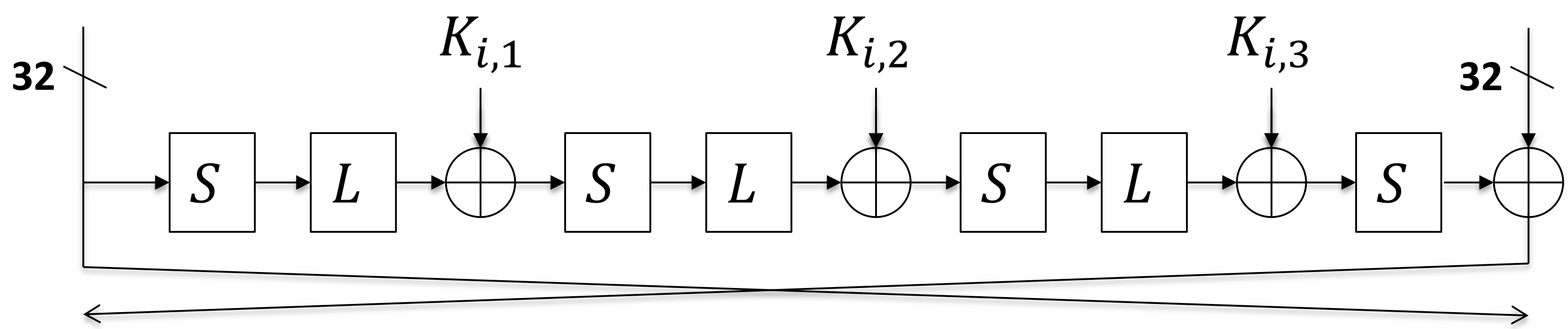
NTT

Applications to Practical Designs

- RoadRunneR
- Minalpher

Introduction of RoadRunneR

- Lightweight BC with 64-bit block, 80- or 128-bit key
- Feistel network with an SPSPSPS round function
- RK diff trail with 2 active S-boxes per round
- Lower bound of the prob of diff chara: 2^{-4r}

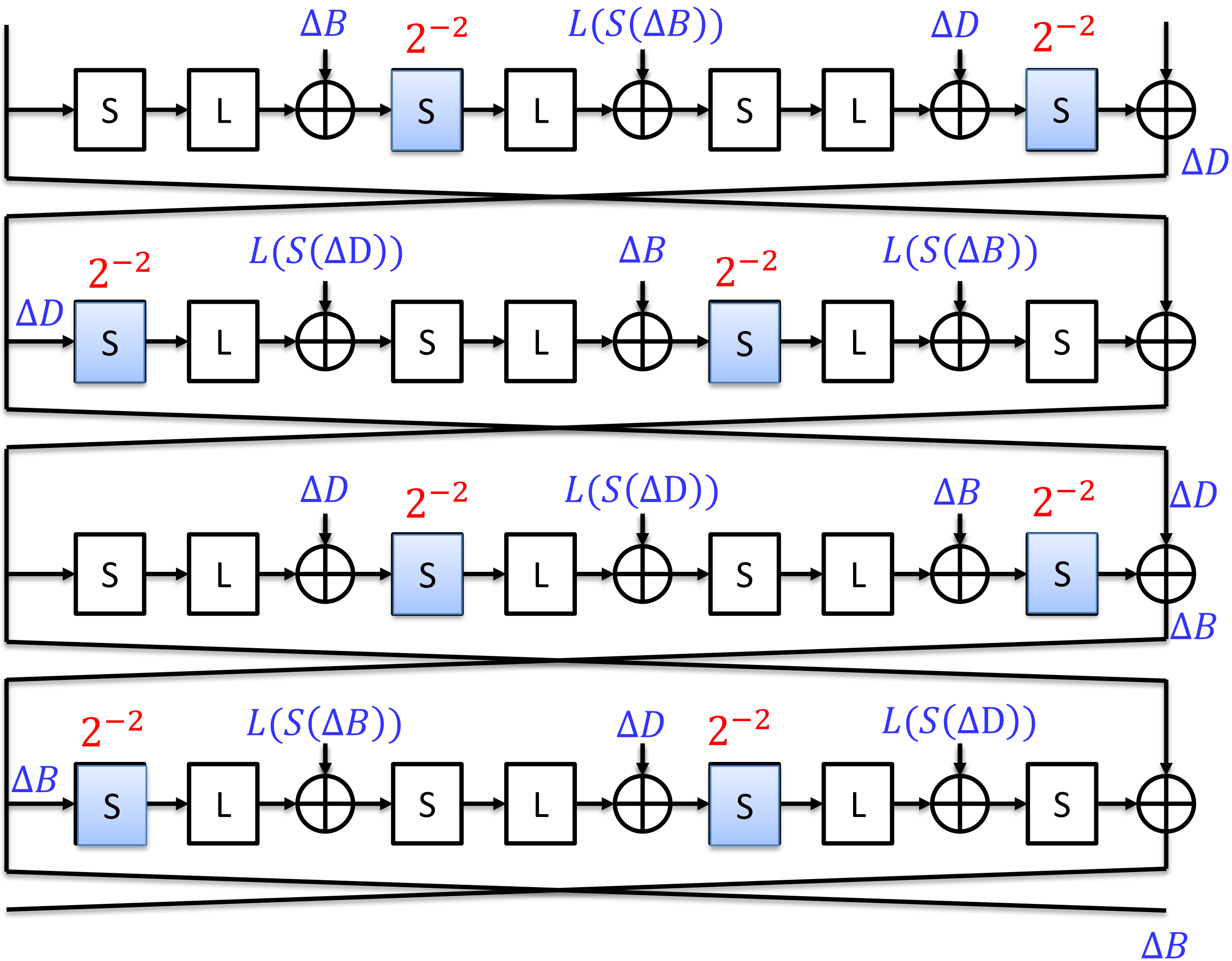


96-bit key per round

Differential trail and p_{ind}

p_{ind}
2^{-16}

p_{exact}
2^{-15}



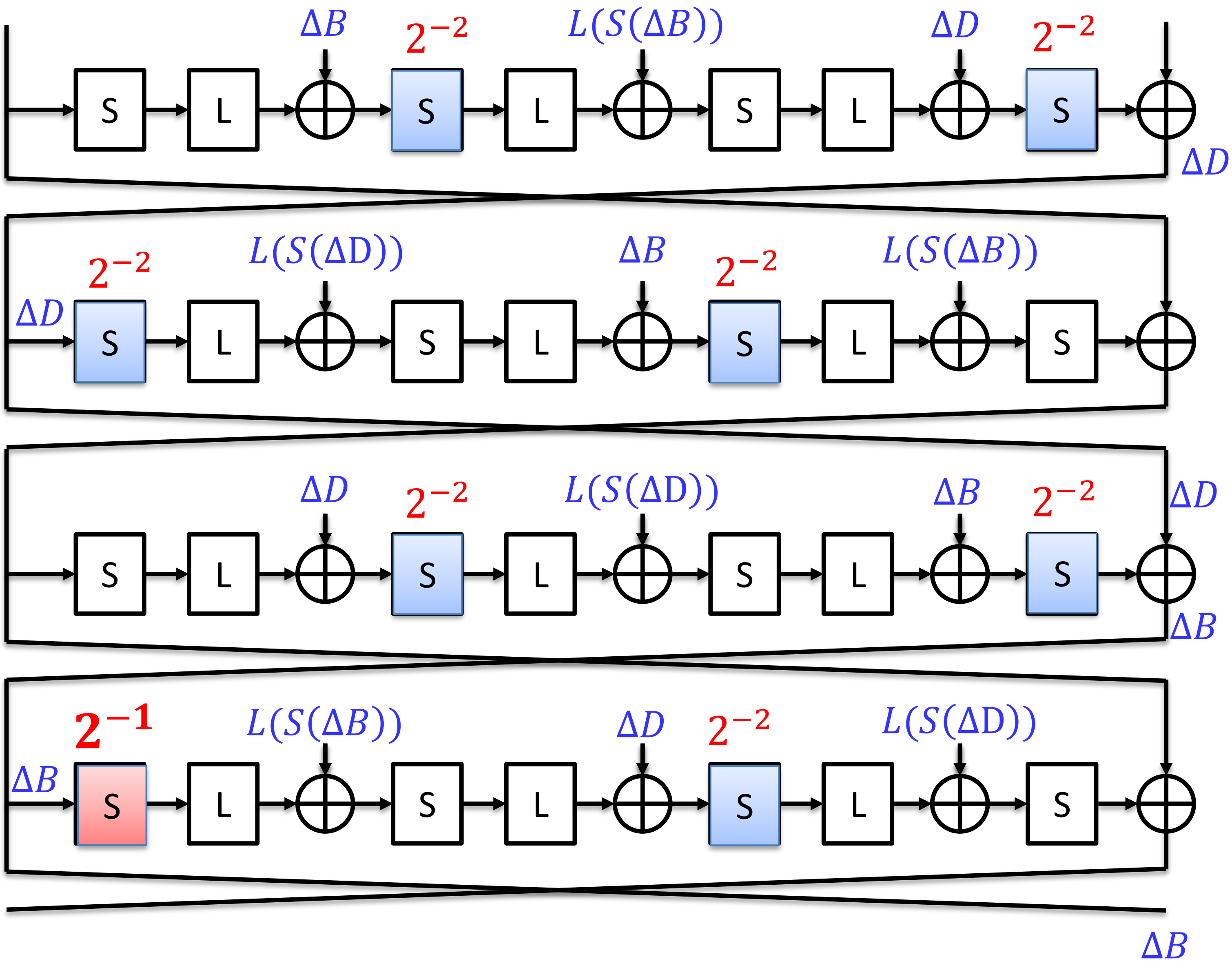
Differential trail and p_{exact}

p_{ind}

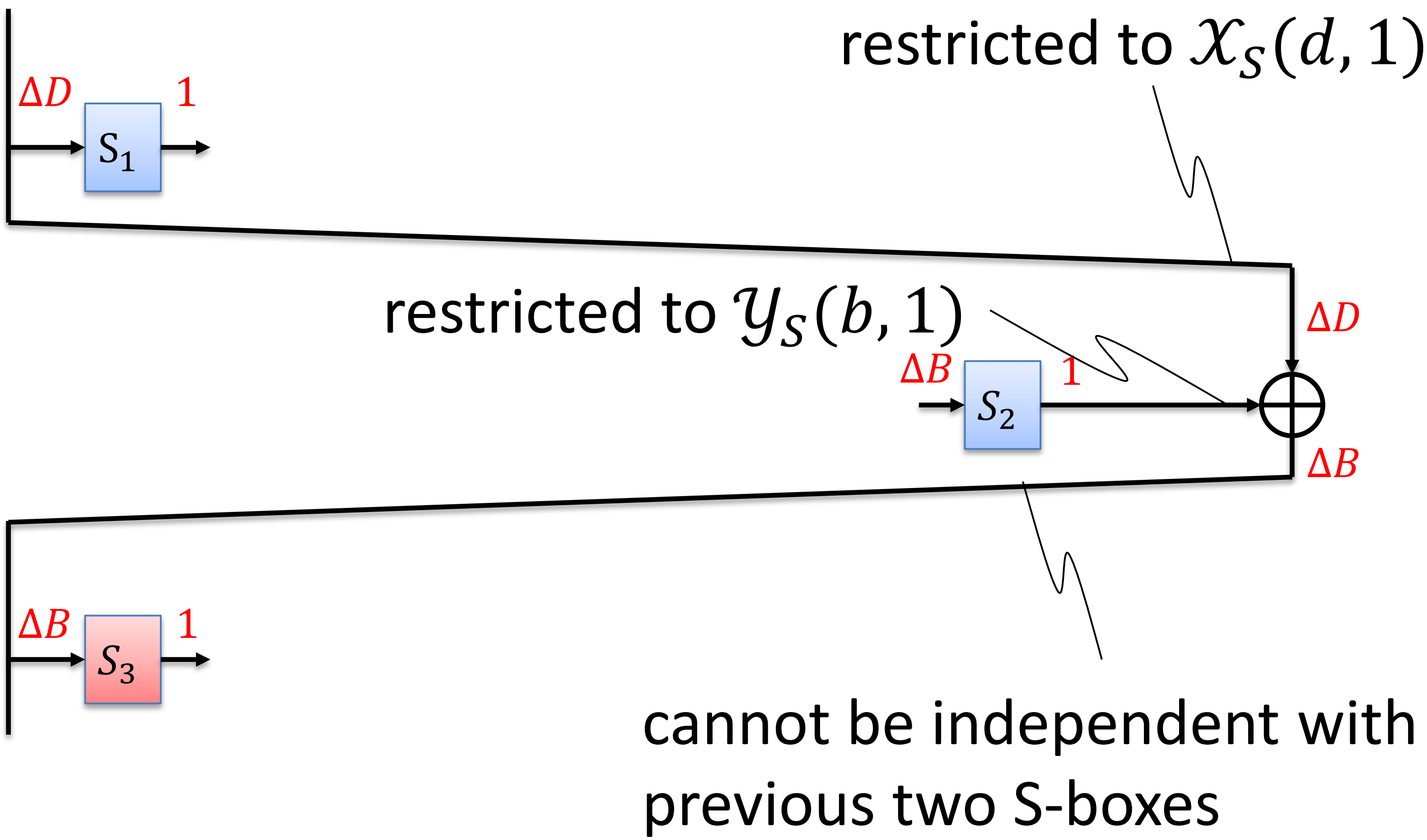
2^{-16}

p_{exact}

2^{-15}



Keyless Structure in RoadRunneR



Summary of Results

Rounds	1	2	3	4	5	6	7	8	9	10	11	12
RoadRunneR-128												
p_{ind}	-4	-8	-12	-16	-20	-24	-28	-32	-36	-40	-44	-48
p_{exact}	-4†	-8†	-12†	-15†	-19†	-22†	-26†	-29†	-33	-36	-40	-43
RoadRunneR-80												
p_{ind}	-8	-17	-26	-34	-42	-51	-60	-68				
p_{exact}	-8†	-17†	-25†	-32†	-39†	-47	-55	-62				

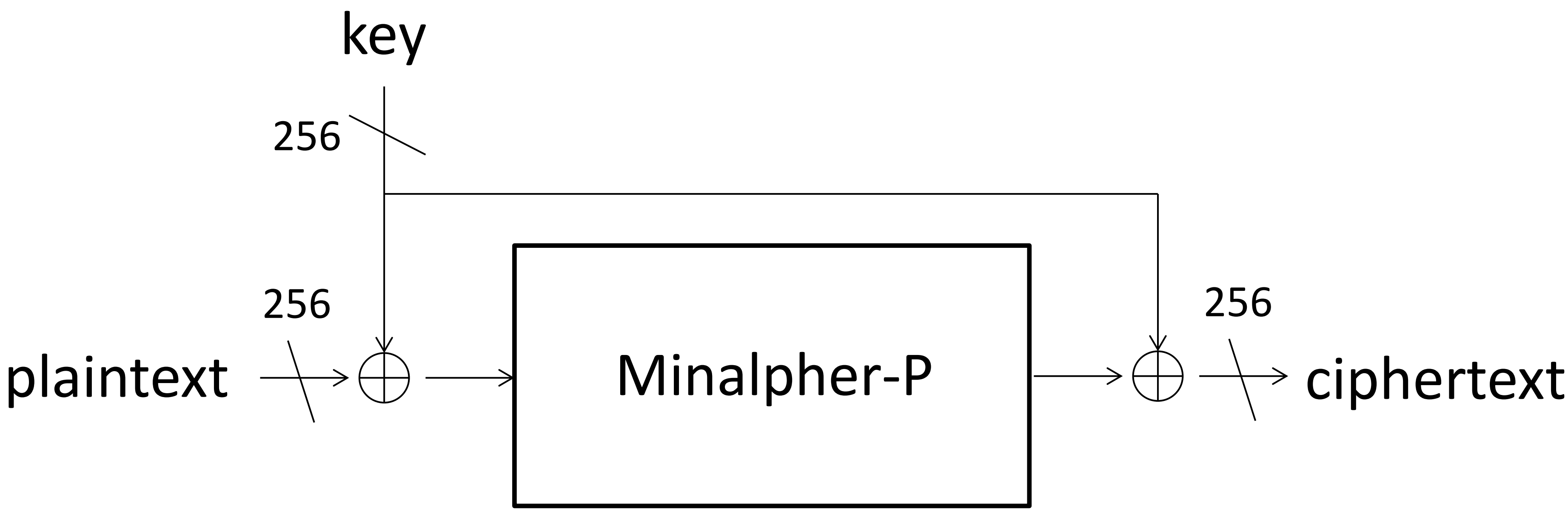
†: experimentally verified

- Each round uses 96-bit round key (more than the block size) but still key-less structure appears.
- Improvement for 8-round RoadRunneR-80 is particularly important because 8 rounds can be satisfied within the full codebook (2^{64}).

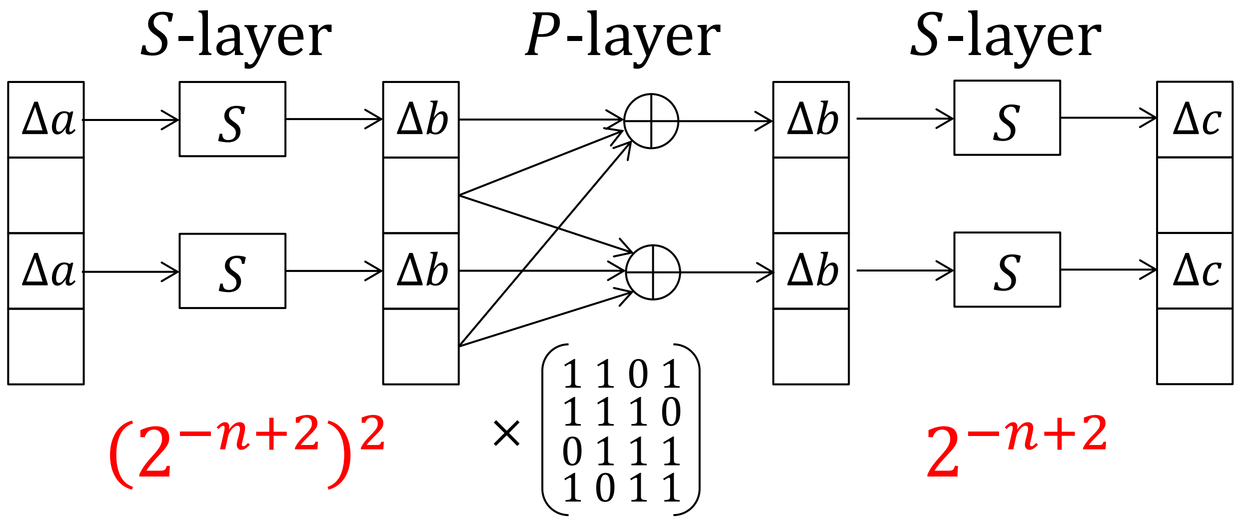
Introduction of Minalpher

An Even-Mansour construction with a 256-bit permutation using an SPN structure with almost-MDS binary matrix.

$$\times \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

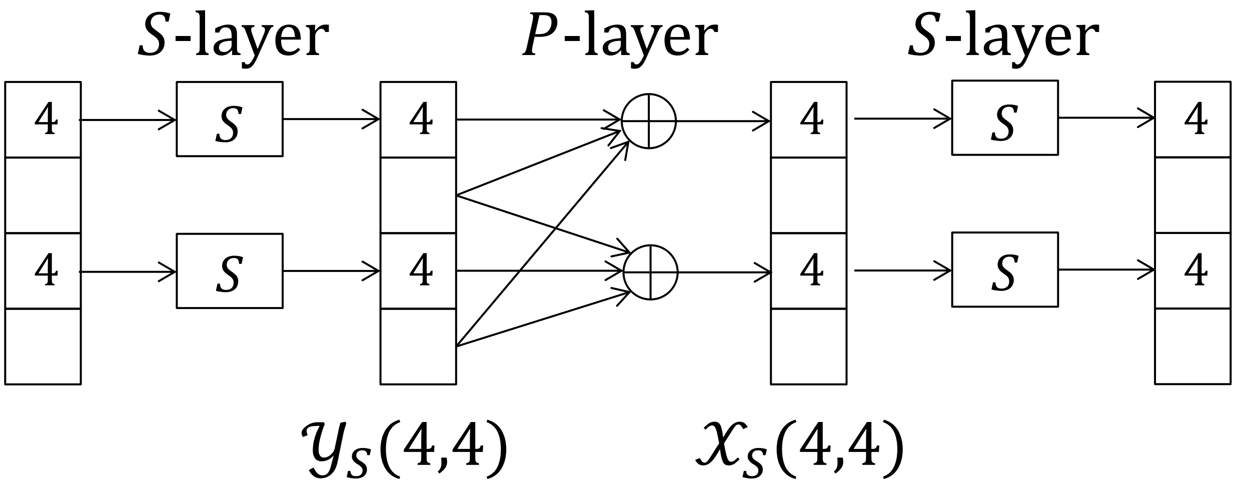


Core Observation (S-P-S for a column)



- Two S-layers with 4 active S-boxes
- Save one S-box in the 2nd S-layer.
- 6-round trail is improved from 2^{-128} to 2^{-96}.
- The attack is extended to 8 rounds.

Analysis



- $\mathcal{X}_S(4,4) = \mathcal{Y}_S(4,4) = \{9, a, d, e\} =< 3,4 > +9.$
- In the middle P-layer, two active nibbles are XORed with an identical value, con.
- The condition that $\mathcal{Y}_S(4,4)$ is mapped to $\mathcal{X}_S(4,4)$ by con is that $con \in< 3,4 >$, which occurs with 2^{-2} instead of 2^{-4}.

Concluding Remarks

- Even if the primitive uses a key, keyless computations can appear in various places.

- Then, p_{exact} can be higher than p_{ind}.

- Generic analysis on 3-round Feistel to lower bound the ratio of p_{exact} and p_{ind}.

- Applications to existing designs show that the analysis affects in practice.

Thank you for your attention!!