Double-SP is Weaker than Single-SP: Rebound Attacks on Feistel Ciphers with Several Rounds

Yu Sasaki

NTT Corporation

Indocrypt 2012 (11/Dec/2012@Kolkata)

Research Summary

Comparing the security of single-SP and double-SP round functions on the generalized Feistel.

$$\to \overset{K_i}{\oplus} \to \boxed{S} \to \boxed{P} \to \qquad \to \overset{K_i}{\oplus} \to \boxed{S} \to \boxed{P} \to \boxed{S} \to \boxed{P} \to$$

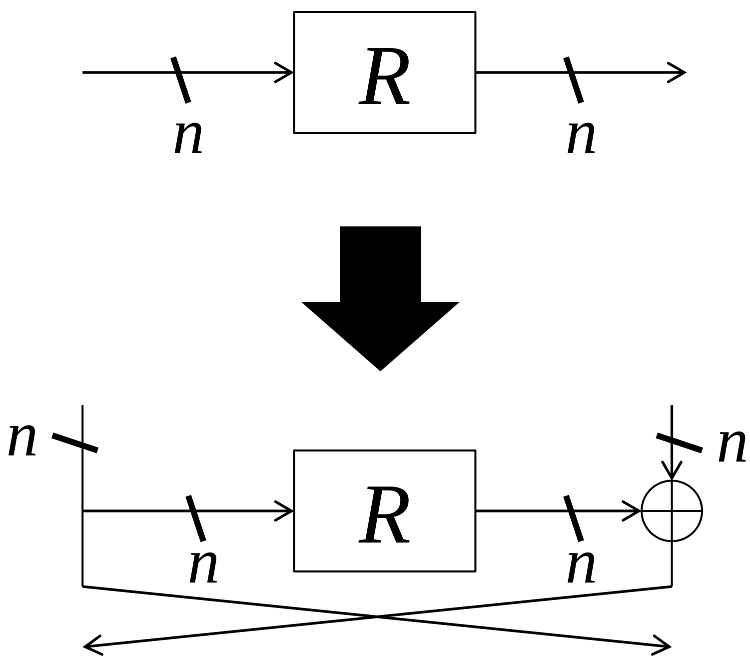
- Previous:
  - Assumption: an infinite number of rounds
  - Results: double-SP causes more active S-boxes than single-SP, and thus double-SP is more secure.
- Ours:
  - Motivation: a number of rounds is small in practice.
  - Results: For 6 or 7 rounds, the rebound attack works more for double-SP than single-SP.

Contents

- Background and Our Goal
- 6 Rounds Attack
- Concluding Remarks

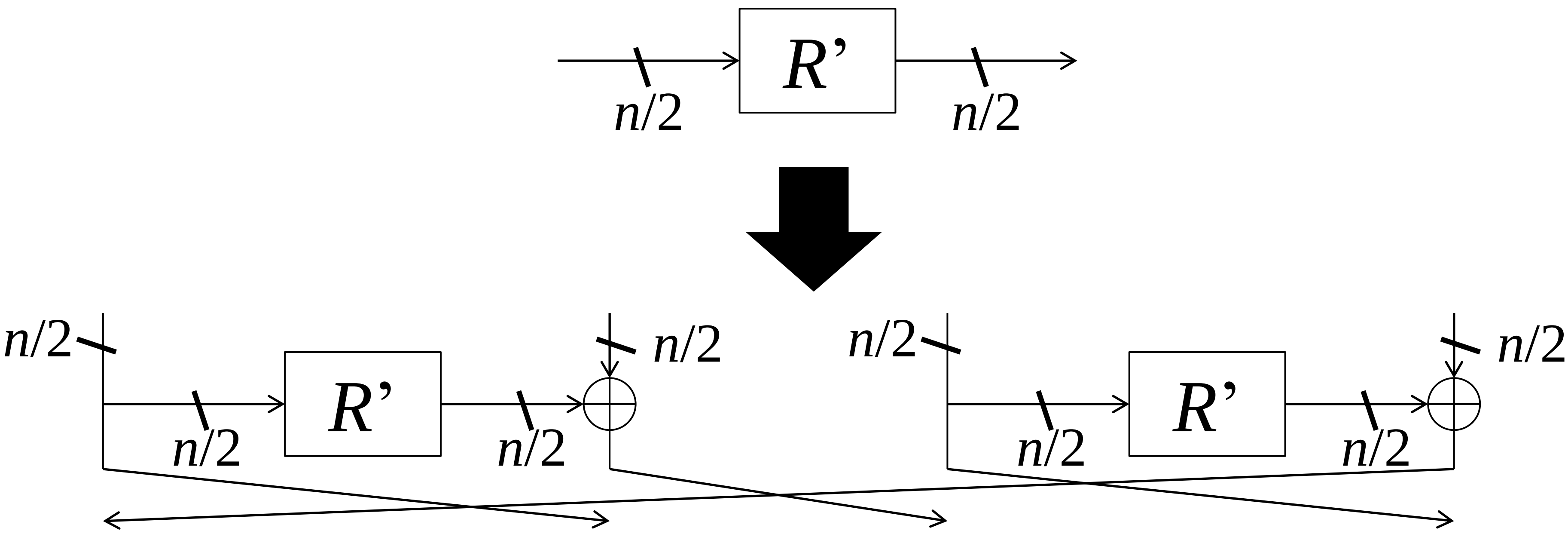
Feistel Network

- Suppose you want to build a $2n$-bit permutation.
- Feistel: A construction to build a $2n$-bit permutation from n-bit permutations.



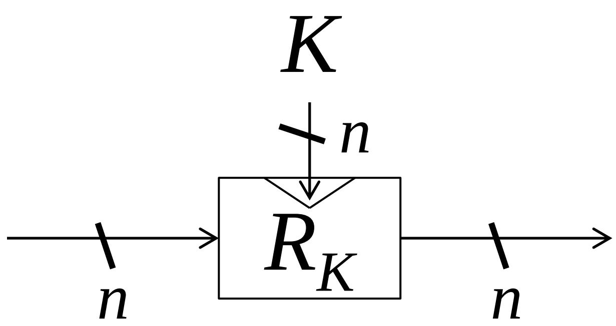
(4-Branch) Generalized Feistel Network

- Suppose you want to build a $2n$-bit permutation.
- 4-branch type-2 generalized Feistel (GFN-4): A construction to build a $2n$-bit permutation from $n/2$-bit permutations.



Keyed Permutation for Ciphers

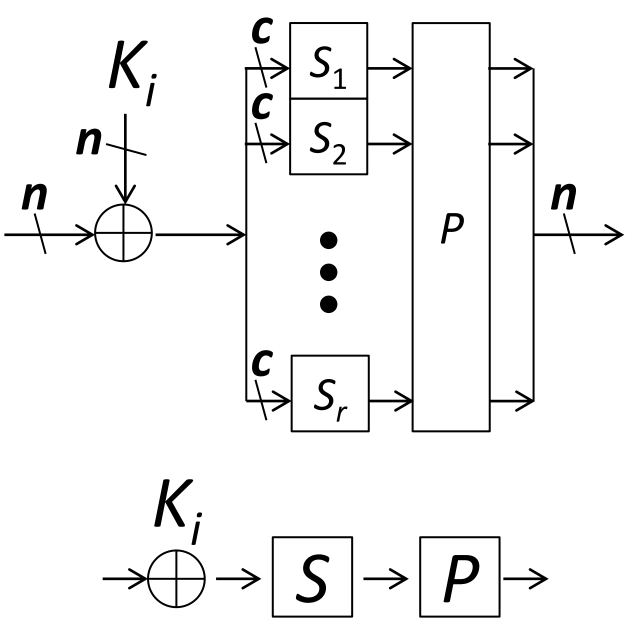
- For block-cipher constructions, the round function takes additional input for subkeys.



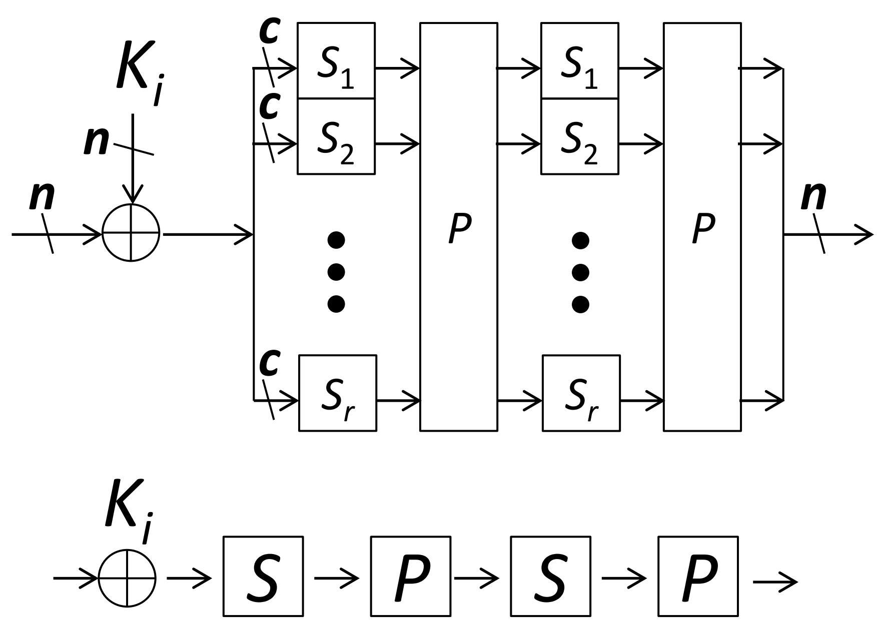
Round Functions

- Iterative use of an S-box layer (S) and a diffusion layer (P) is quite popular.

Single-SP function

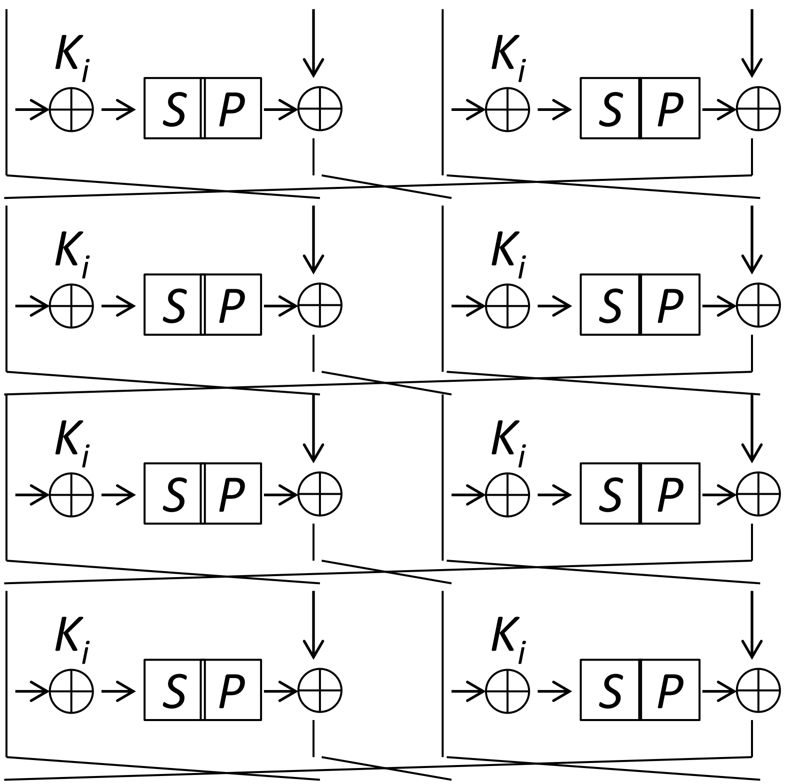


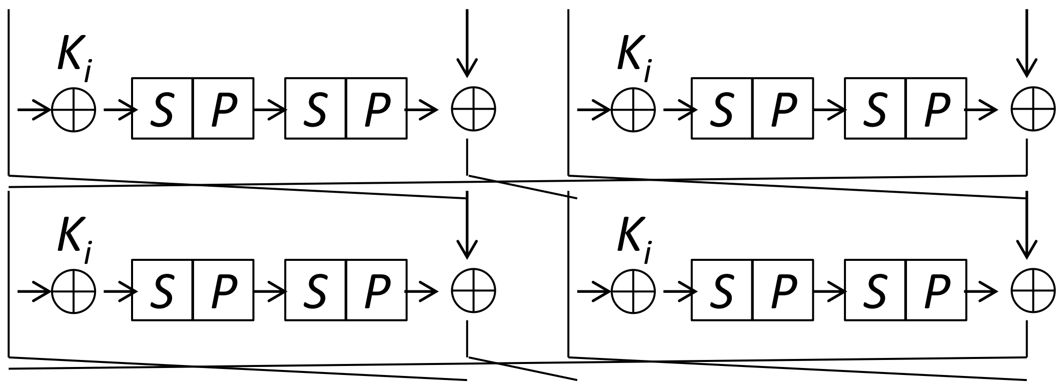
Double-SP function



Previous Results (1/2)

- Bogdanov and Shibutani compared #active S-boxes in GFN-4 with single-SP/double-SP functions.
  - r rounds for single-SP and $r/2$ rounds for double-SP





Previous Results (2/2)

- r: #attacked rounds for single-SP
- $r/2$: rounds for double-SP
- b: #Sboxes in one SP-layer
- $A(x,b)$: minimum #active Sboxes in x rounds.
- $T(x,b)$: total #Sboxes in x rounds.

If r approaches to infinity, $A(r,b)/T(r,b)$ for single-SP is smaller than $A(r/2,b)/T(r/2,b)$.

Double-SP is more secure against DC and LC.

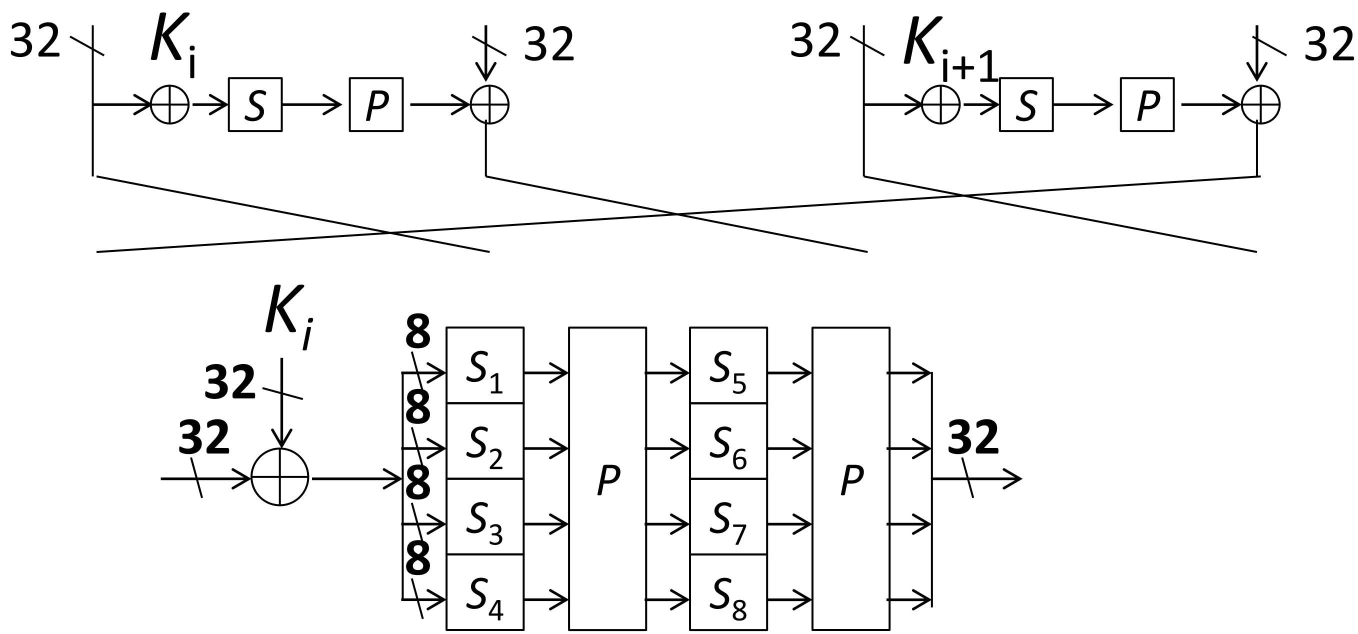
Research Motivation

- In dedicated designs, designers usually minimize #rounds for a high performance.
- Comparing two constructions for a small r by presenting differential attacks.
- We use the rebound attack.

If r approaches to infinity, $A(r,b)/T(r,b)$ for single-SP is smaller than $A(r/2,b)/T(r/2,b)$.

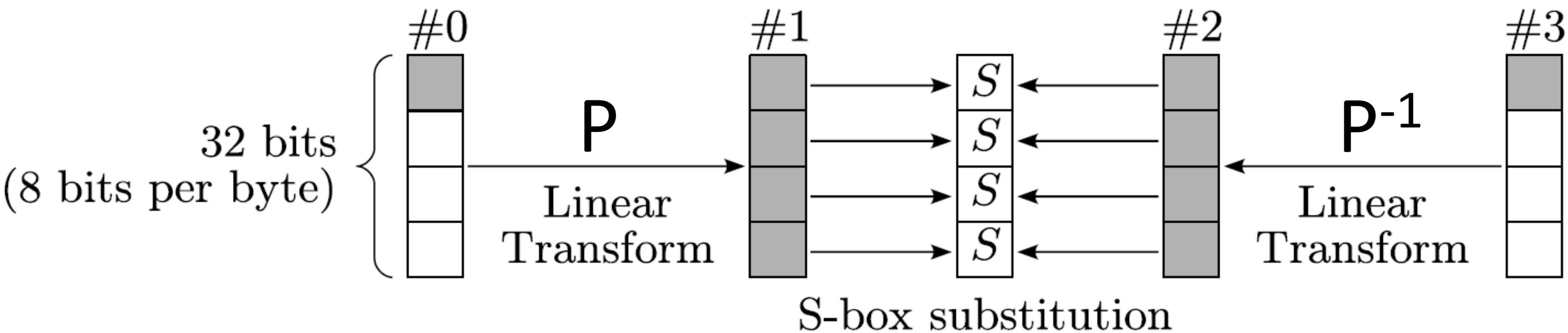
Target Parameter

- There is no concrete design that adopts GFN-4 single-SP or double-SP functions.
- CLEFIA has the closest design.
- Hereafter, we fix the parameters to the same as CLEFIA: branch size is 32, and S-box size is 8.



Rebound Attack

- Proposed by Mendel et al. at FSE 2009.
- Efficiently bypass 2 P-layers and 1 S-layer.



1. Choose Δ for #0, then propagate it to Δ for #1.

2. Choose Δ for #3, then propagate it to Δ for #2.

3. 1 solution of the S-layer is obtained with complexity 1.

Results of the Applications

- Single-SP
  - Presented by Sasaki and Yasuda at FSE 2011.
  - #attacked rounds: 11 rounds
  - #SP-layers is 22.
- Double-SP
  - **Our results**
  - #attacked rounds: 6 or 7 rounds
  - #SP-layers is 24 or 28.
- If a number of rounds is small, single-SP is more secure than double-SP.

Why It Occurs?

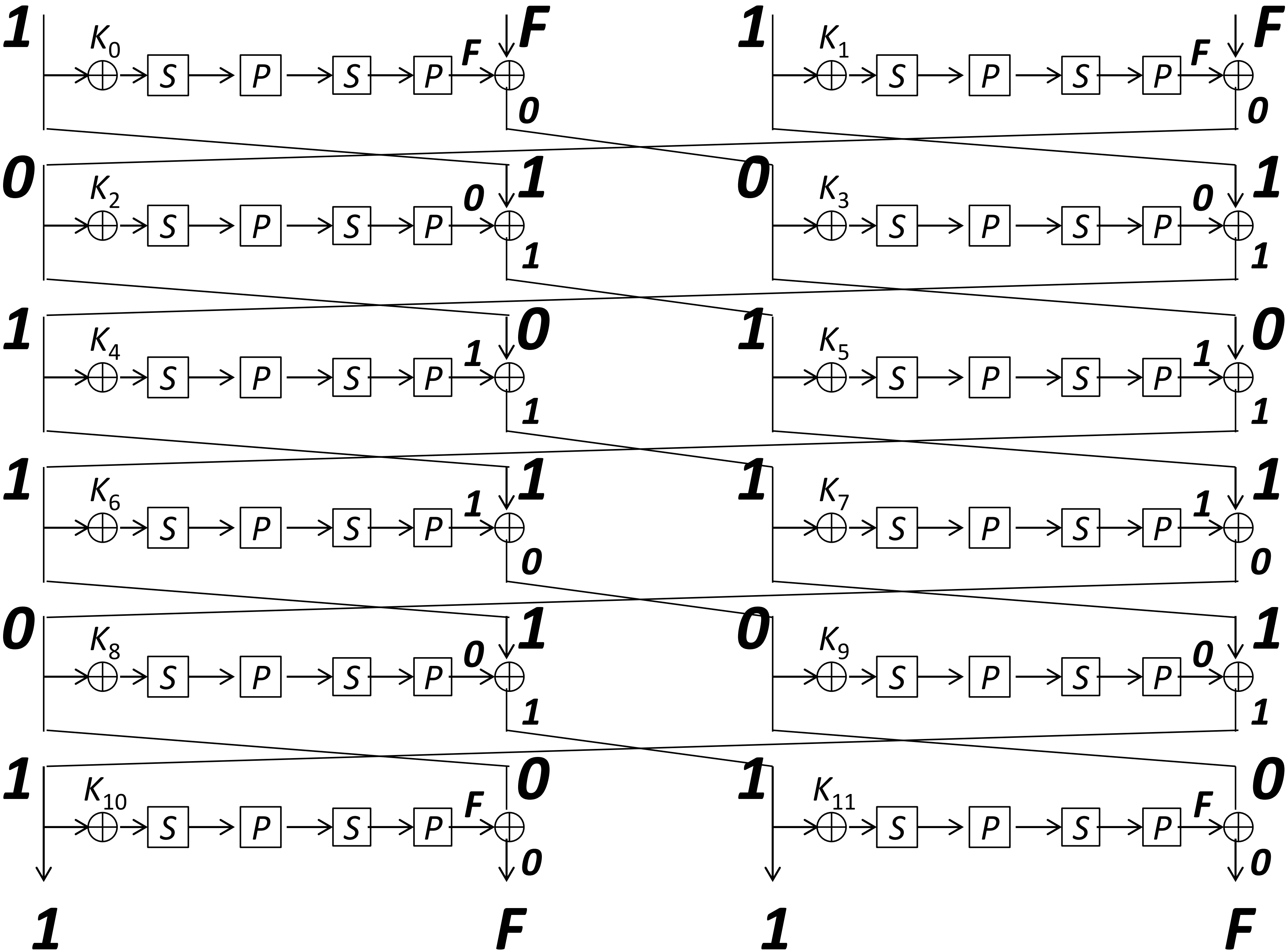
- #rounds that an attacker can control is finite.
- If a total #rounds is infinite, such an impact to a finite rounds are ignored.

What we can learn:

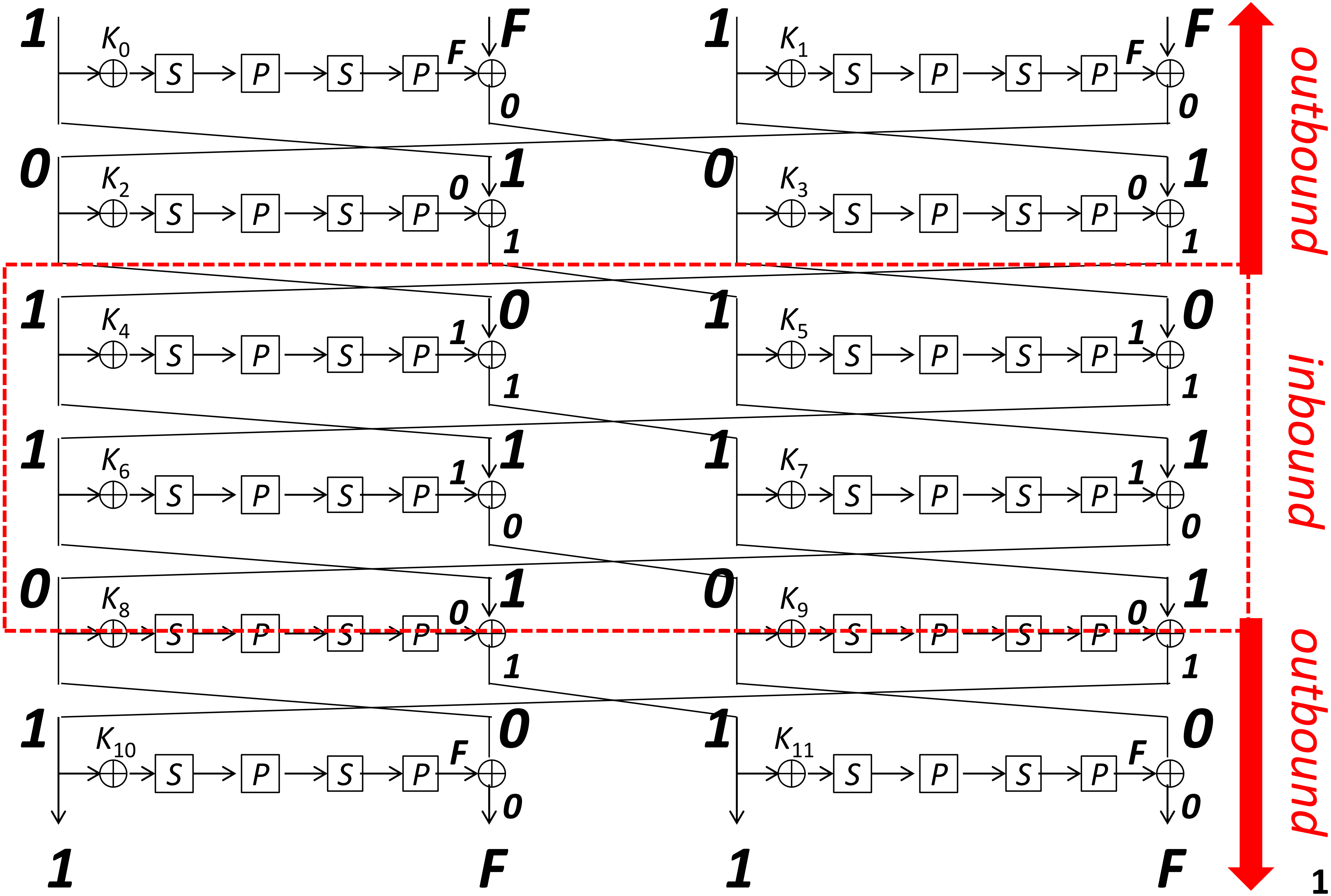
- for a small number of rounds, the attacker’s ability is not negligible.
- We may need to compare the ratio of #controlled active S-boxes by the attacker.

6-Round Attack

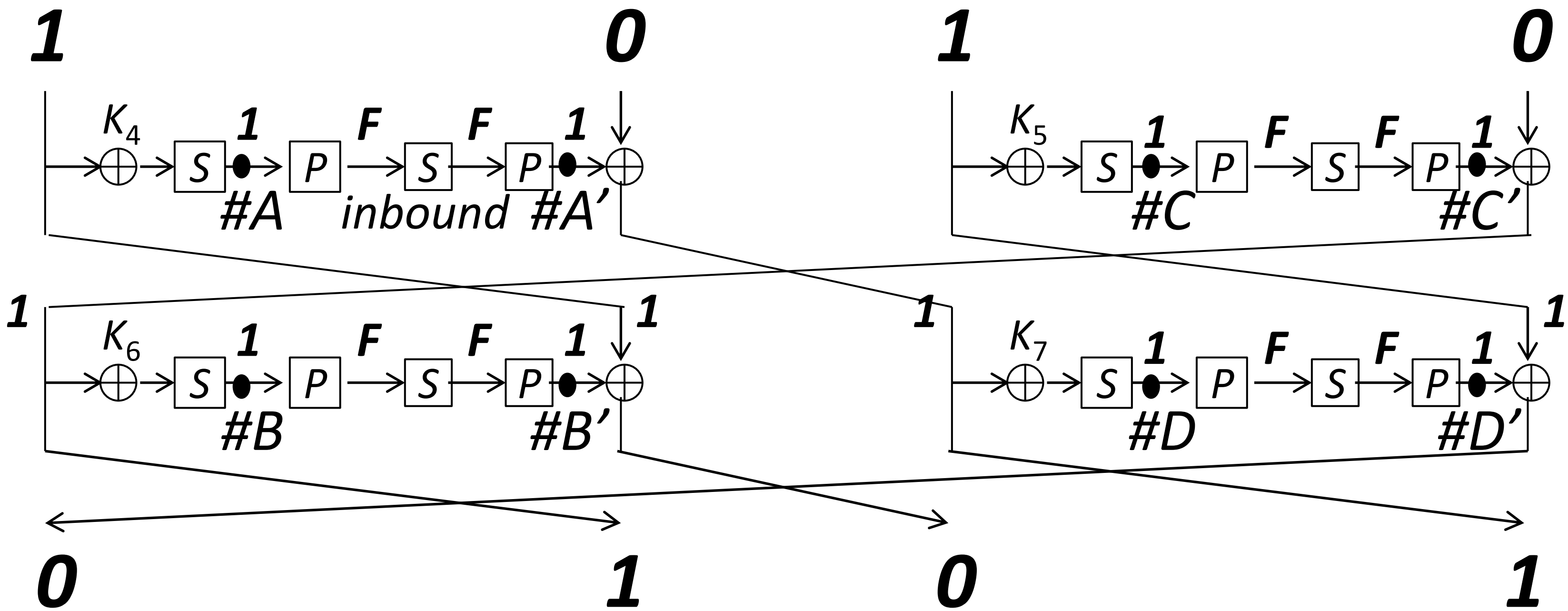
Differential Path



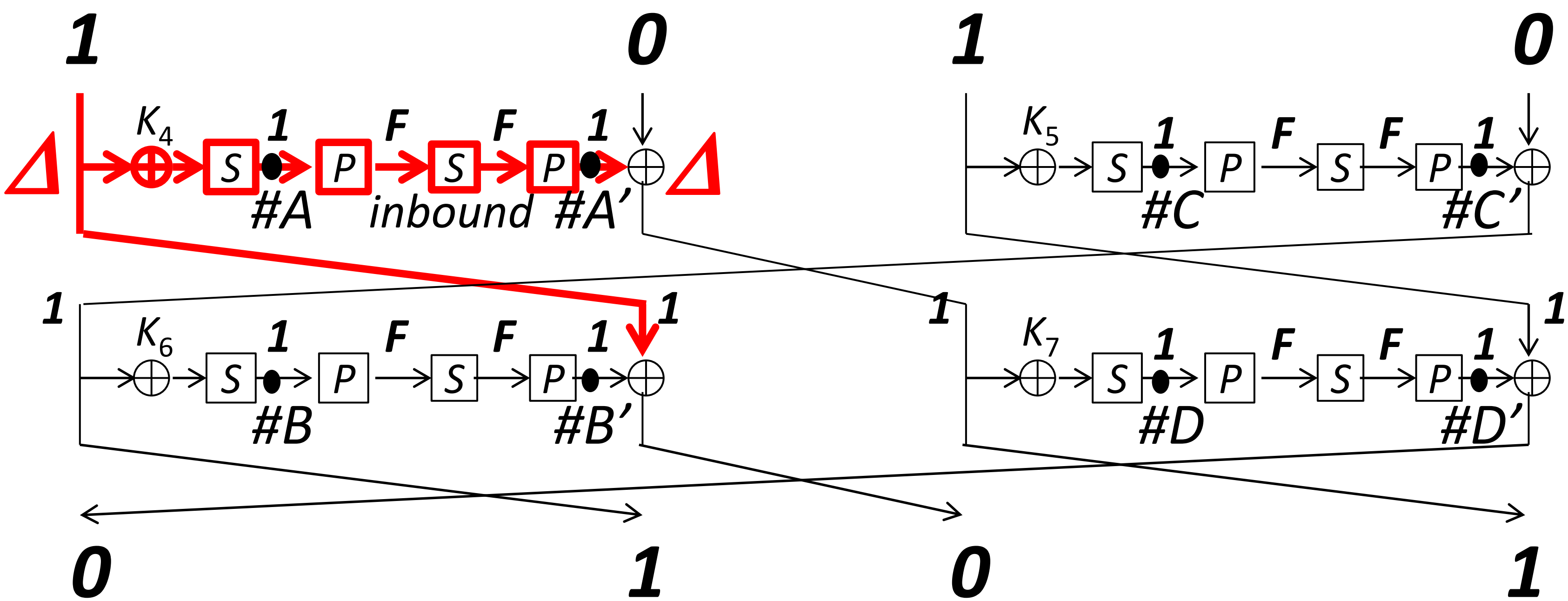
Differential Path



2-round Inbound Phase (1/3)

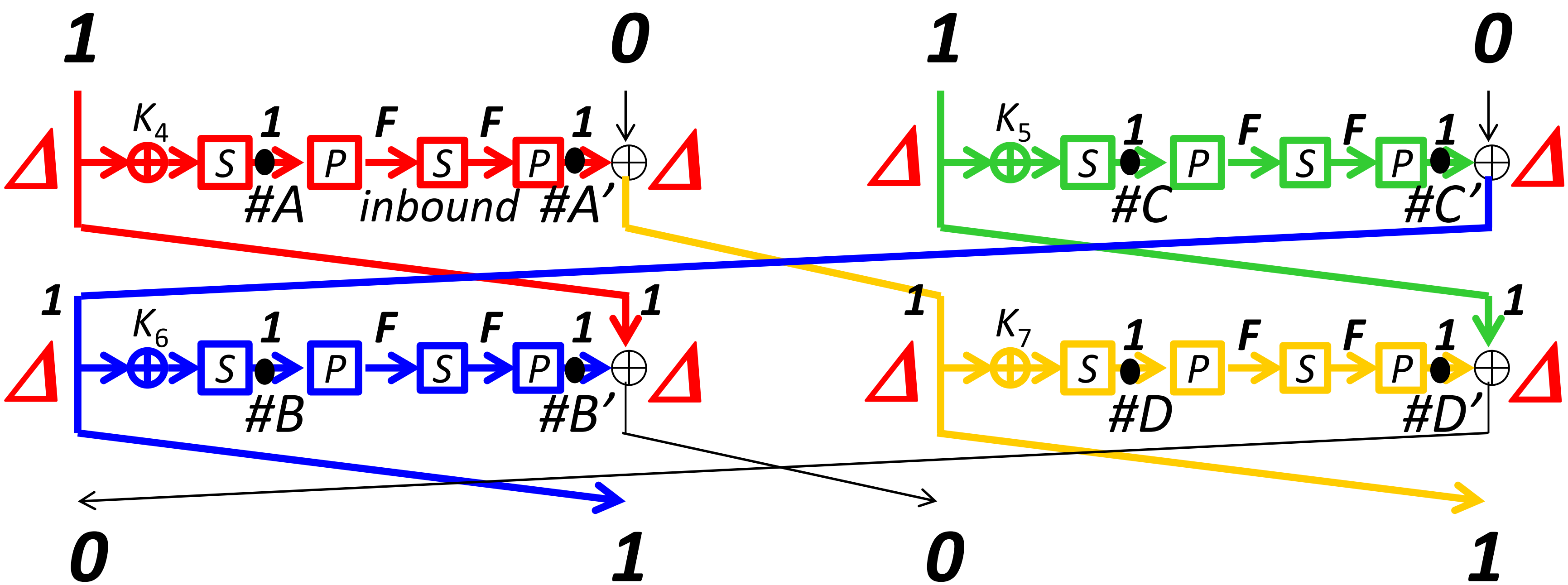


2-round Inbound Phase (2/3)



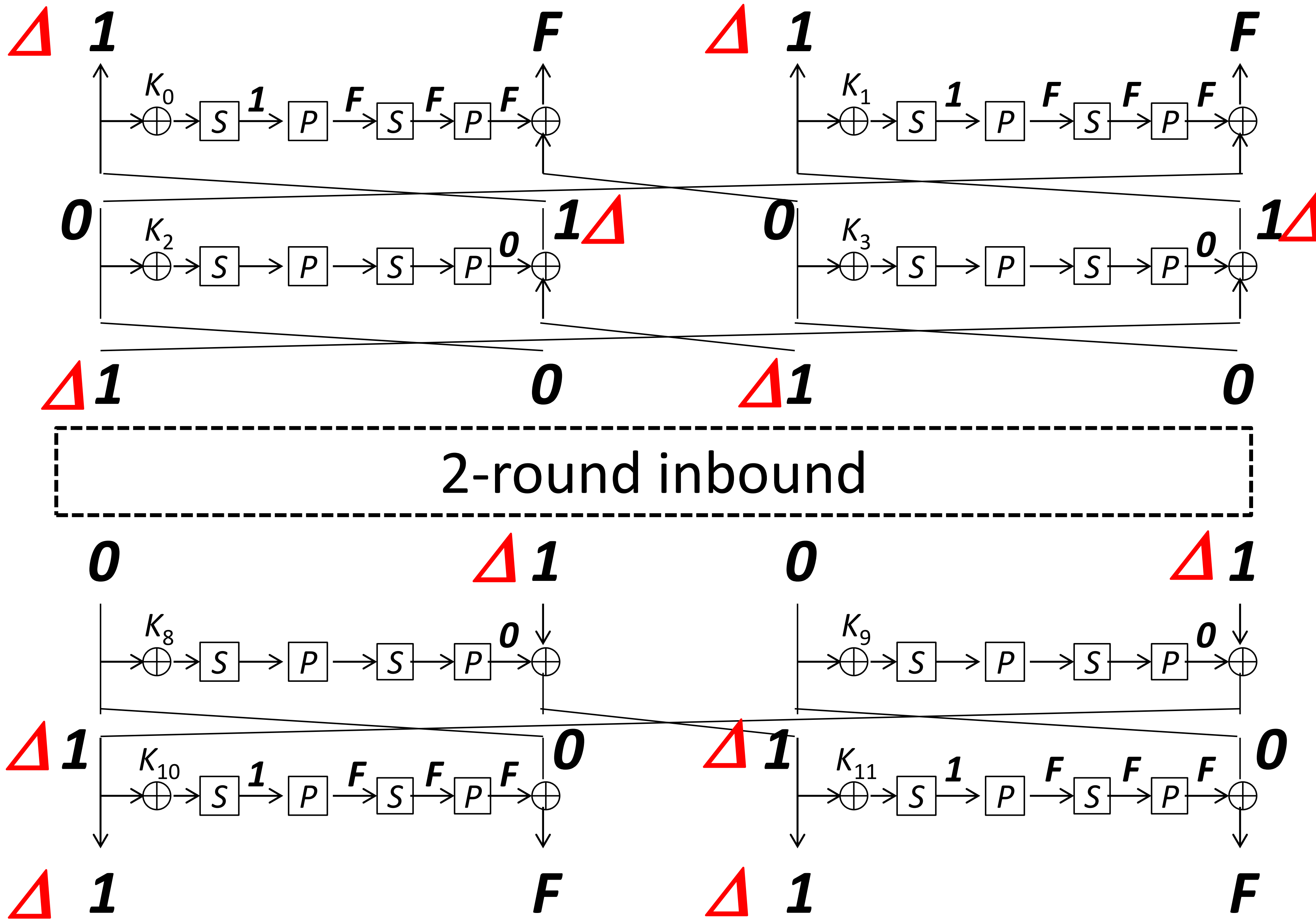
- For the red part, find a paired value such that input and output Δ are identical.
- This requires 2^8 round func computations.

2-round Inbound Phase (3/3)



- Copy the paired values of #*A* and #*A*' for the other parts.
- This requires 2^8 round func computations.

Outbound with Pr.=1



Summary of 6-round Attack

- 2-round backword outbound with Pr.=1.
- 2-round inbound with complexity 2^8.
- 2-round forward outbound with Pr.=1.

- If the compression function is build by the MMO mode, a half of the state will collide.
- The attacker controls 6*4=24 SP-layers. This is more than the current best attack (22 SP-layers) on single-SP functions.

Summary of 7-round Attack

- 2-round backword outbound with Pr.=1.
- 2-round inbound with complexity 2^{20}.
- 2-round forward outbound with Pr.=1.

- An artificial distinguisher for the MMO mode, where ideal function requires 2^{24} to find it.
- Need more techniques than the 6-round attack. If you are interested in the rebound attack, please refer to the paper.

Concluding Remarks

- For a small number of rounds, the attack can control more active S-boxes in a double-SP than in a single-SP function.
  - Single-SP: 22 SP-layers for a half-state collision
  - Double-SP: 24 SP-layers for a half-state collision or 28 SP-layers for an artificial distinguisher.
- We man need to compare #controlled active S-boxes rather than #total active S-boxes.

Thanks for your attention !!