

# The Exact Multi-User Security of Key-Alternating Feistel Ciphers with a Single Permutation

Yusuke Naito

**Yu Sasaki**

Takeshi Sugawara

Mitsubishi Electric Corporation

NTT Social Informatics Laboratories, NIST Associate

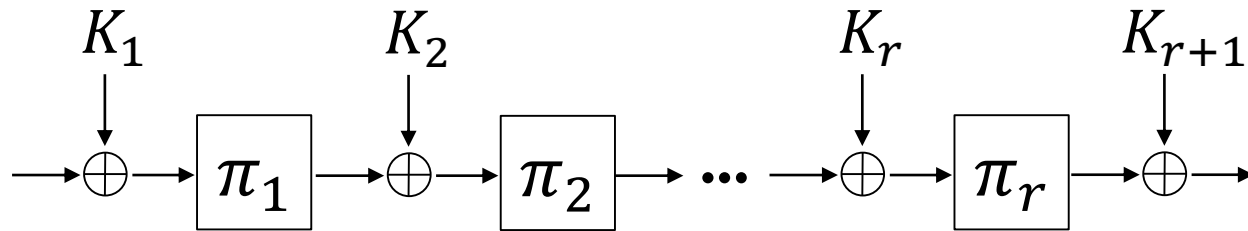
The University of Electro-Communications

08/18/2025 @CRYPTO 2025

# Security of Generic Block Cipher Construction **NTT**

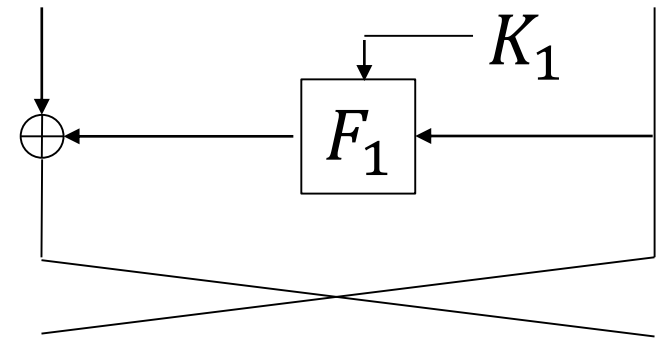
- It is popular to generalize constructions and study their security.  
➡ The results are **applied to many designs in general**.
- The goal is to drive the lower and upper bounds of the construction to be distinguished from ideal  $n$ -bit SPRP.

## Key Alternating Ciphers (KACs)



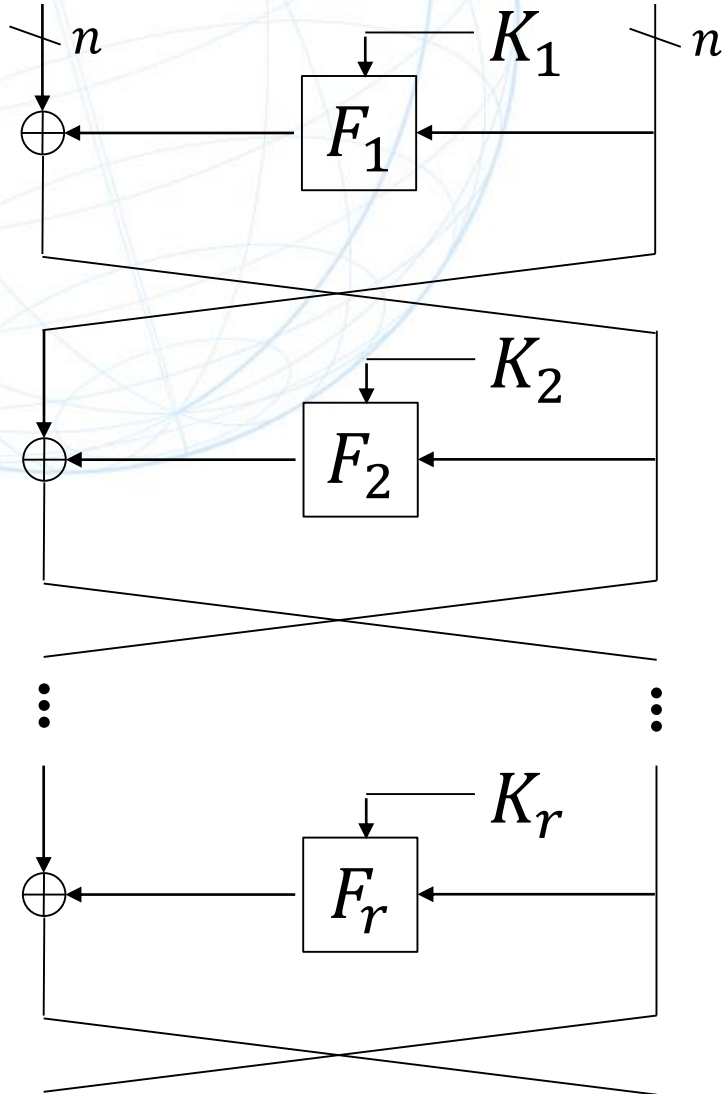
Studied at **Eurocrypt 2024** by Naito-Sasaki-Sugawara

## Feistel Ciphers



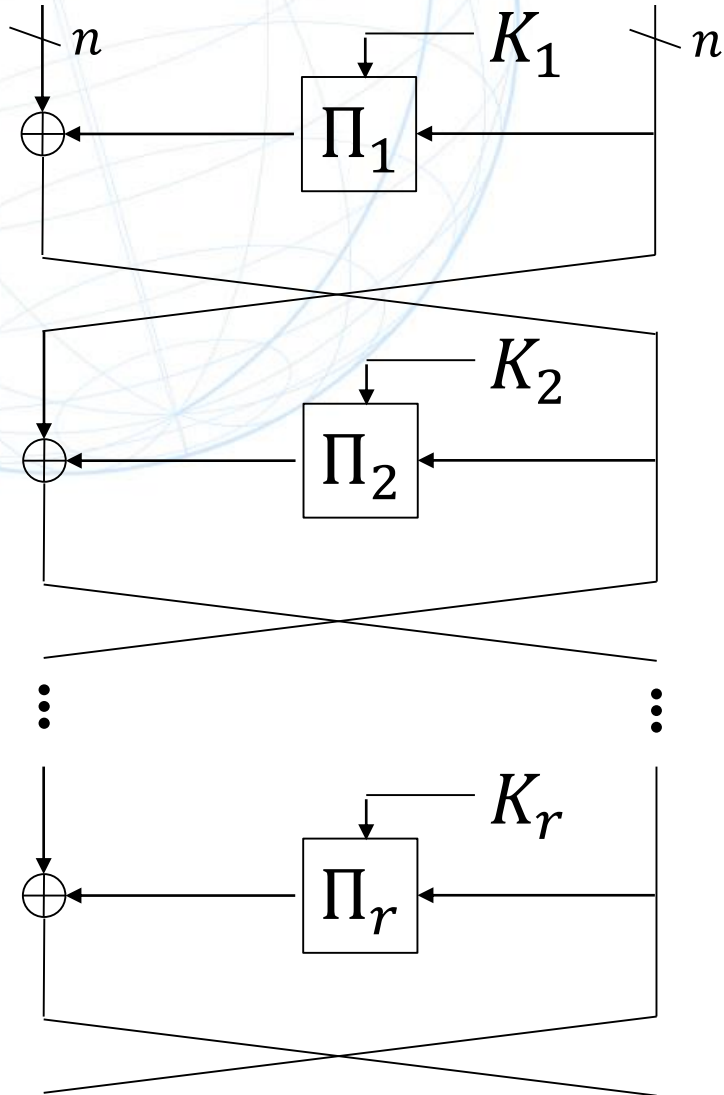
**This paper !!**

# Luby-Rackoff



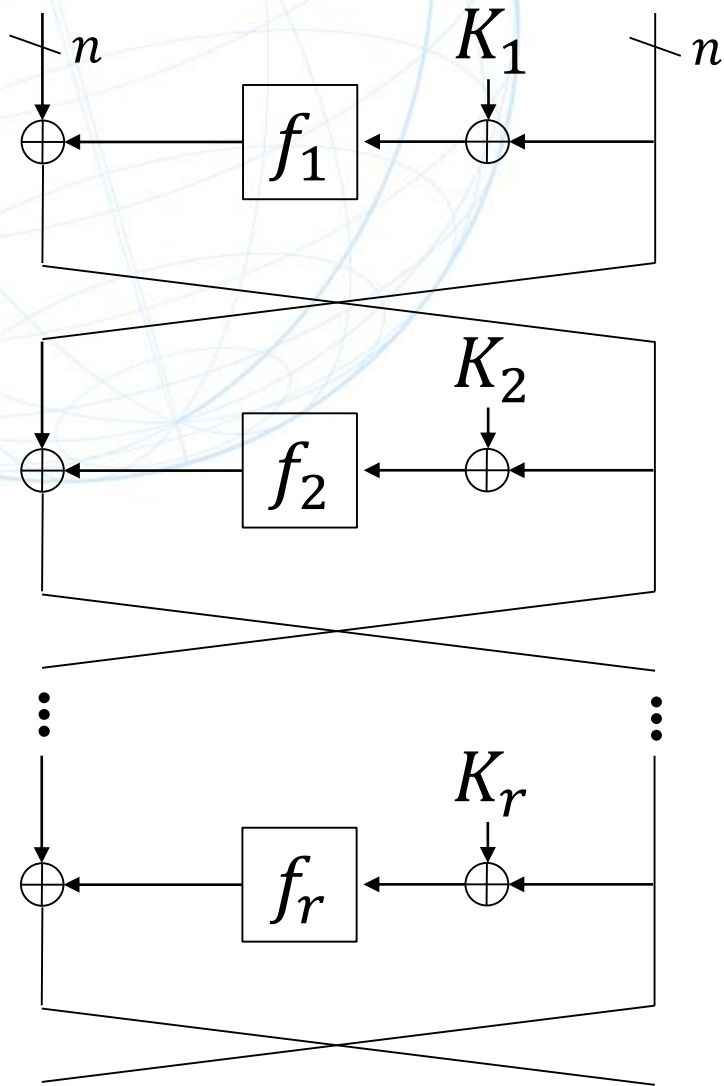
- It was proposed by Luby and Rackoff in 1986.
- The size of each branch is  $n$  bits.
- Round functions are secret and independent in each round.
- Patarin proved that 4 rounds are SPRP up to  $O(2^{\frac{1}{2}n})$  queries.
- Many other results are known ...

# Luby-Rackoff with Permutation



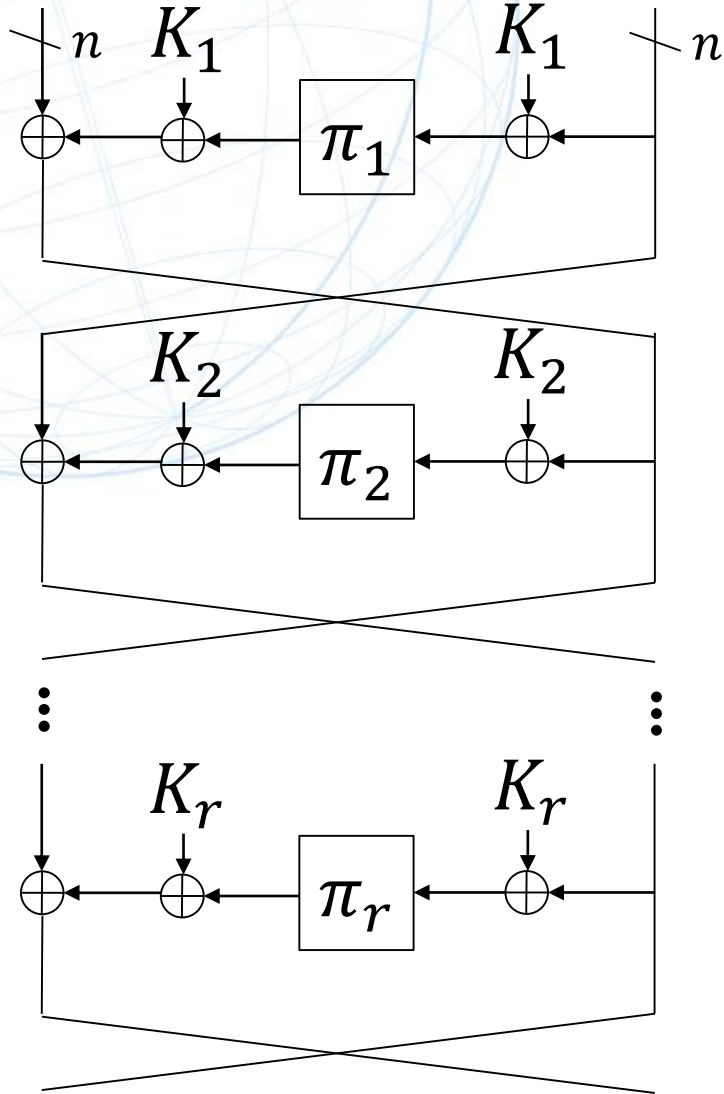
- First analyzed by Piret in 2006.
- Motivated by the fact that practical designs mostly adopt permutations as round functions.
- This direction was subsequently continued by Guo and Zhang [17] in 2021.

# KAF-F: Feistel with Key Alternating Function



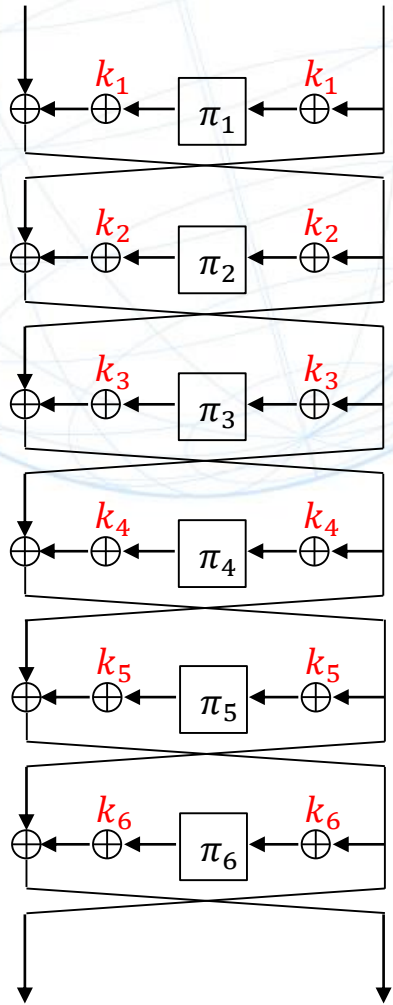
- First studied by Lampe and Seurin in 2014.
- Motivated by the fact that practical designs mostly adopt round functions applying the key addition followed by a public function.
- Big change in security analysis since adversaries now can make primitive queries besides construction queries.
- proved that  $6t$  rounds are SPRP up to  $O(2^{\frac{t}{t+1}n})$  queries.

# KAF-P: Feistel with Even-Mansour

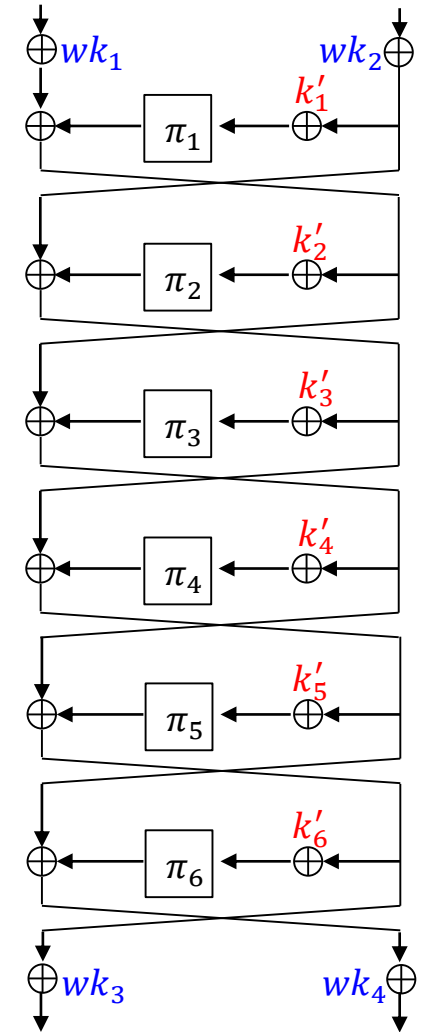


- First studied by Bhattacharjee et al. in 2024.
- Motivated by the fact that practical designs mostly adopt a public permutation.
- It was proved that 5 rounds are SPRP up to  $O(2^{\frac{2}{3}n})$  queries.
- We further show that if KAF-P is secure, so is **whitening + key +  $\pi$** .

# KAF-P is Secure $\Rightarrow$ Practical Designs are Secure **NTT**

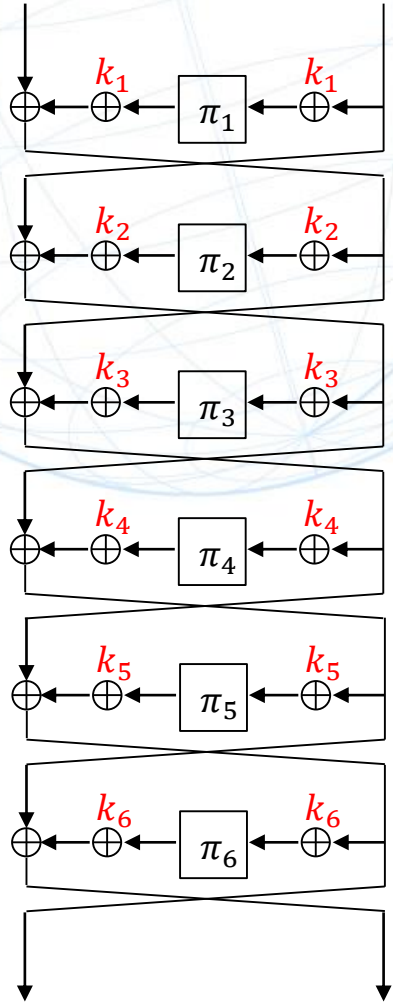


(a): KAF-P

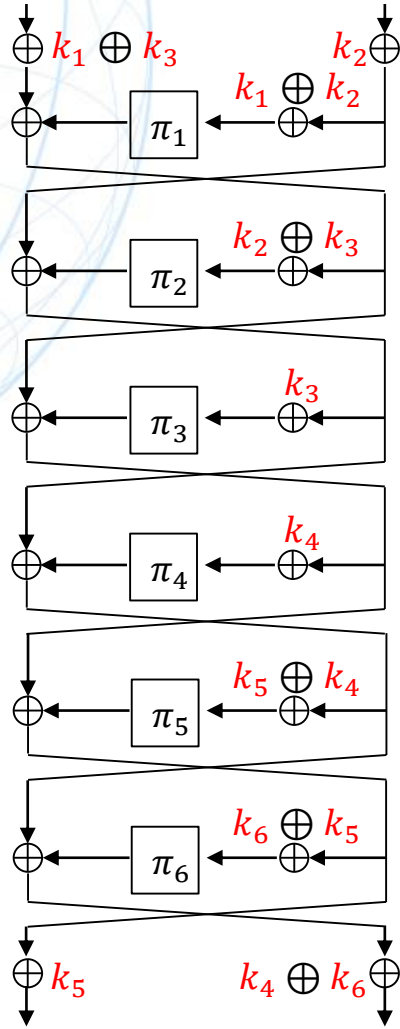


(e): practical structure

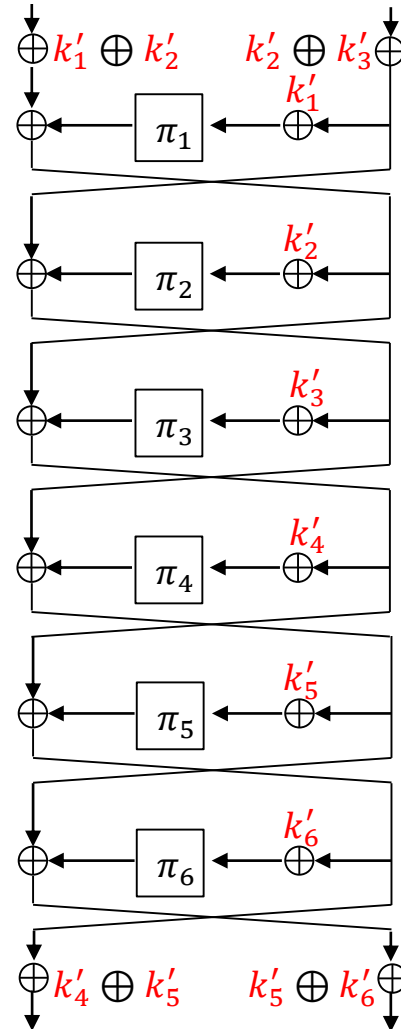
# KAF-P is Secure $\Rightarrow$ Practical Designs are Secure **NTT**



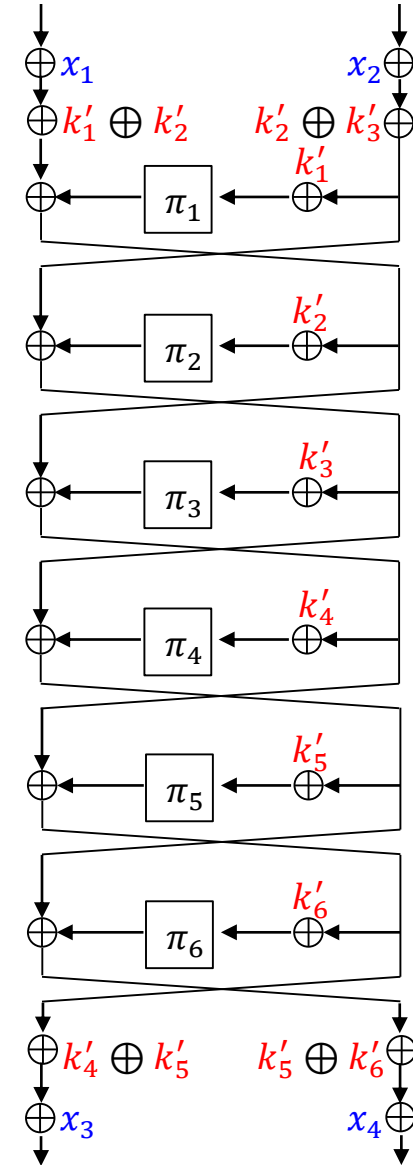
(a): KAF-P



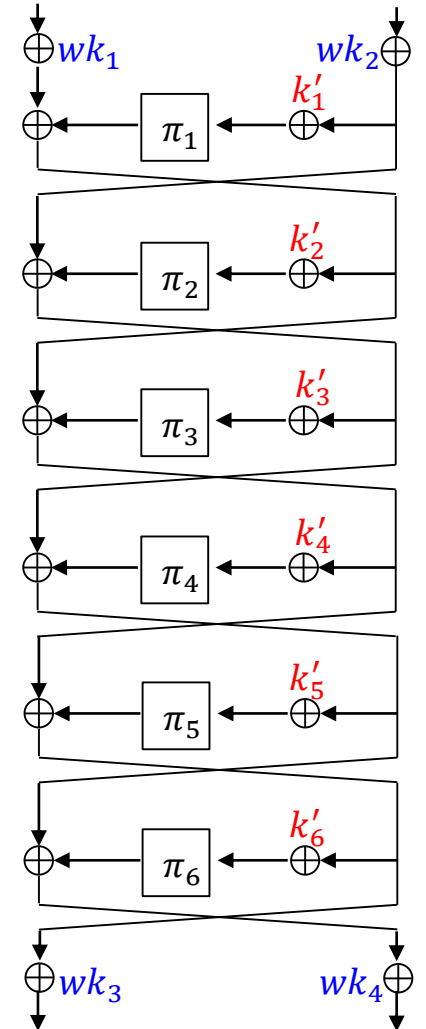
(b): linear key transformation



(c): rename variables



(d): add 4 keys  $x_1, x_2, x_3, x_4$  to strengthen the scheme



(e): practical structure



- **Tightness:** generic attacks matching the proven upper bound should be provided.
- **Multi-user security:** Adversaries make queries to multiple users having independently generated keys. This model captures more realistic cases.
- **Single-primitive:** Proofs are simpler if primitives are independently chosen in every round, while practical designs usually use only a single primitive for efficiency.
- **Correlated Subkeys:** Proofs are simpler if all the subkeys are independent, while practical designs usually generate all the subkeys from a master key.

# Comparison of Results

- We prove that  $r$  rounds of KAF-P is secure up to  $O(2^{\frac{r-2}{r-1}n})$  queries.  
**tight, multi-user, single primitive,  $r - 2$  independent keys**

Table 1. Provable security bounds of Feistel ciphers with public primitives.

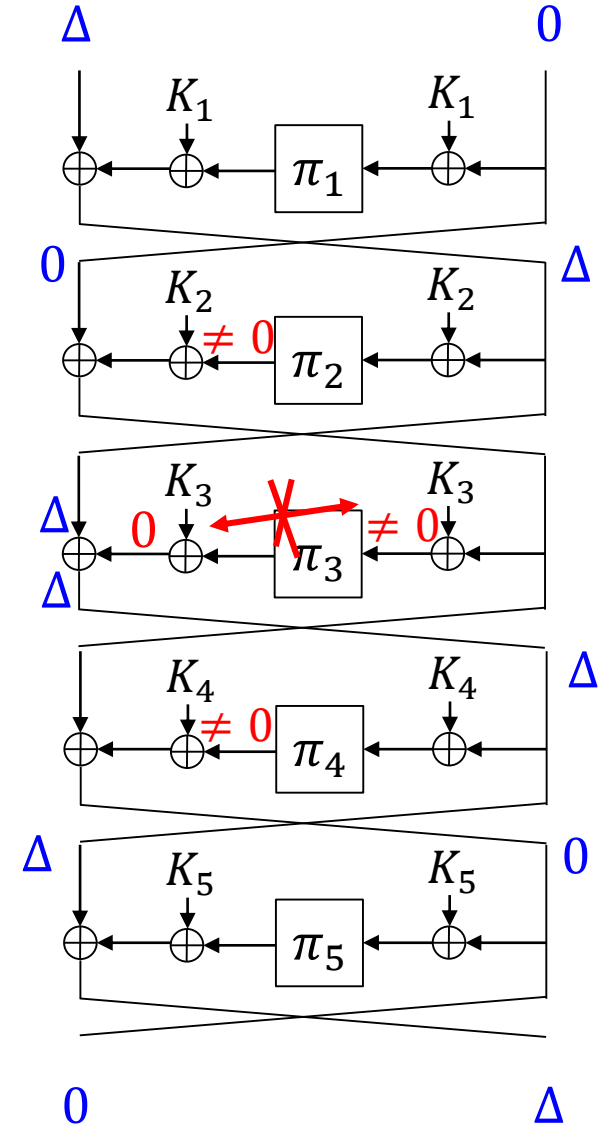
Reference	Type	Round	Bound (bits)	Tight- ness	Model	Single Primitive	Indep. Subkeys <sup>†</sup>
Lampe–Seurin [26]	KAF-F	12	$\frac{2}{3}n$	—	su	—	All
Lampe–Seurin [26]	KAF-F	$6t$	$\frac{t}{t+1}n$	—	su	—	All
Guo–Wang [16]	KAF-F	4	$\frac{1}{2}n$	✓	mu	✓	1
Guo–Wang [16]	KAF-F	6	$\frac{2}{3}n$	—	mu	—	2
Bhattacharjee et al. [4]	KAF-P	5	$\frac{2}{3}n$	—	su	—	All
<b>Ours</b>	KAF-P <sup>†</sup>	$r$	$\frac{r-2}{r-1}n$	✓	mu	✓	$r - 2$

<sup>†</sup>Our attack is also applicable to KAF-F.

# Best Generic Attacks for 5 Rounds

## Impossible Differential Attacks

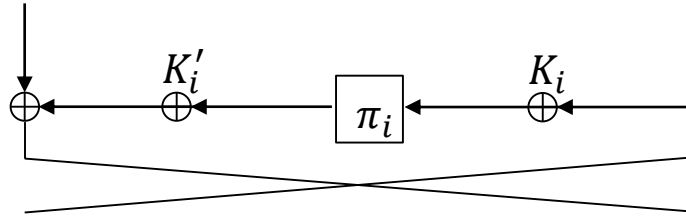
- The difference  $(\Delta, 0)$  never propagates to difference  $(0, \Delta)$  after 5 rounds.
- This property allows to distinguish 5 rounds with  $O(2^n)$  queries.
- This type of attacks will be inapplicable when  $r$  becomes large, since any differential propagation will be possible for a large  $r$ .



# Target Constructions in our Attacks / Proofs

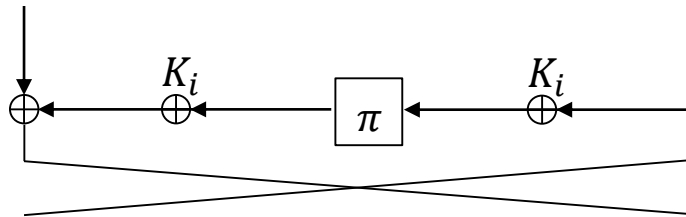
## Attacks

- Attacks are better if it works even if all rounds use independent permutation and independent subkeys, moreover different keys for Even-Mansour construction.



## Proofs

- Proofs are better if it works even if all rounds use the same permutation and the same key for the Even-Mansour construction.

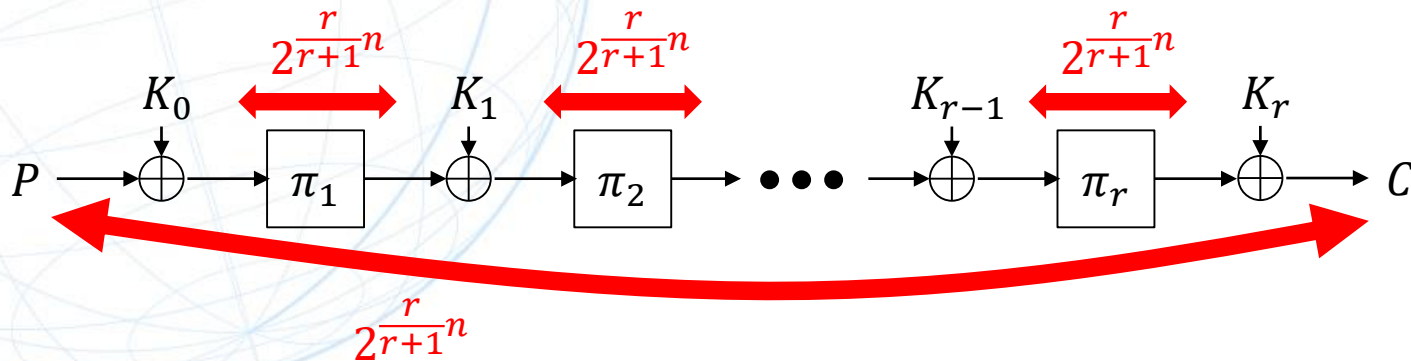




# New Attacks

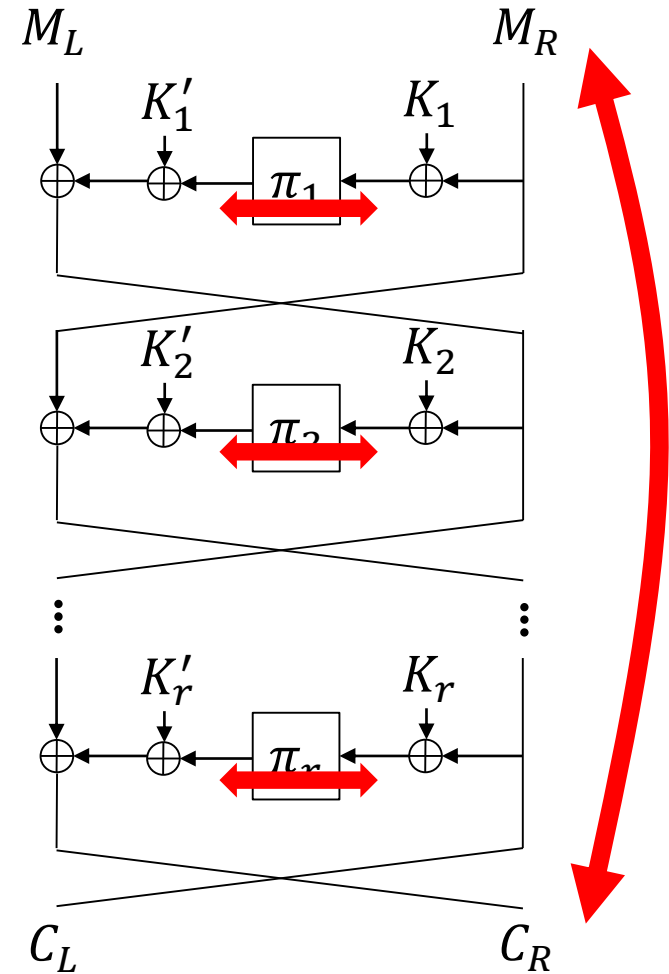
# Inapplicability of Related Works 1

## Generic Attacks on $r$ -round KAC



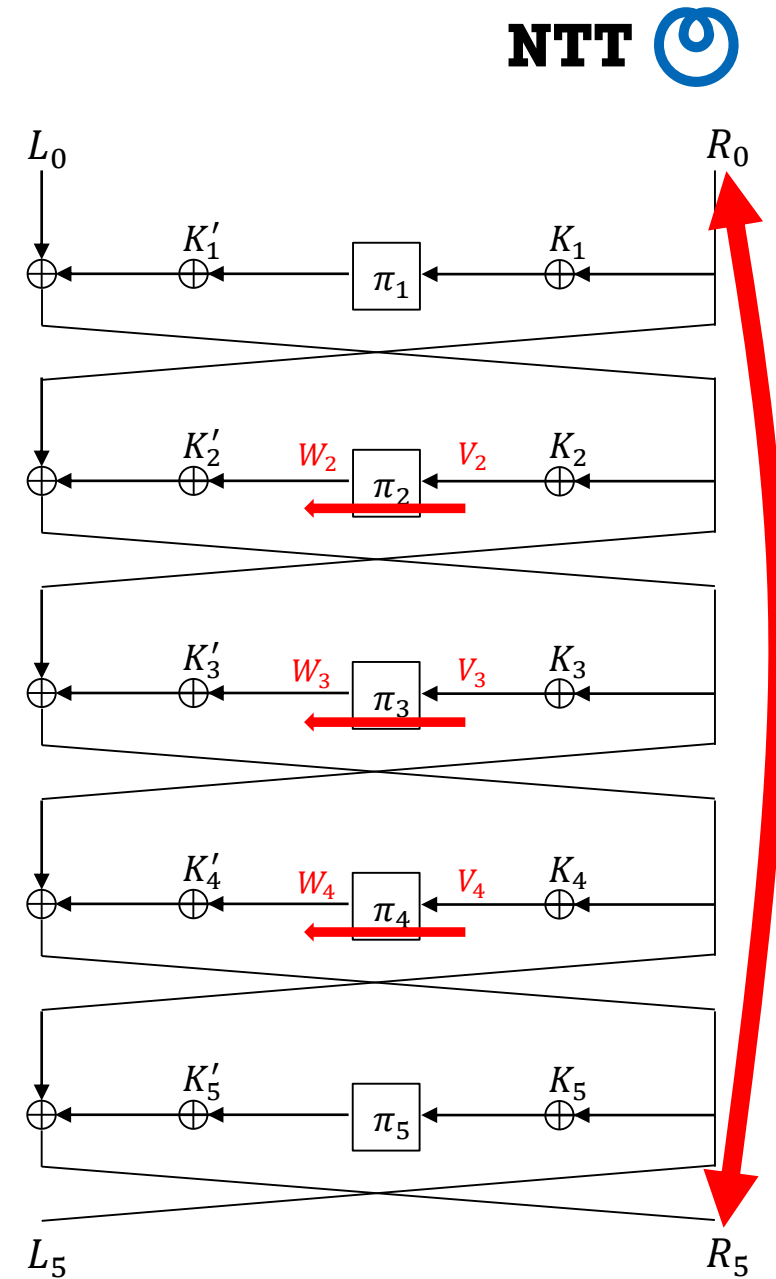
- Make  $O(2^{\frac{r}{2r+1}n})$  construction queries.
- Make  $O(2^{\frac{r}{2r+1}n})$  primitive queries for each  $\pi_i$ .
- There should exist consistent queries.
- Subkeys are derived just computing XORs.

However, for Feistel, even if both queries match, XOR of Feistel construction protects subkeys.



# Our Approach: Meet-in-the-Middle

- We first find a match between construction and primitive queries for all but the first and the last rounds; i.e. a consistent tuple  $L_0 || R_0, (V_2, W_2), (V_3, W_3), \dots, (V_{r-1}, W_{r-1}), L_r || R_r$
- To recover subkeys, we make it a pair with another construction query, and to trace differential propagation rather than values. (propagate with prob.1 over subkey XOR)
- Values after  $\pi_i$  for the query that is chosen to be a pair can be looked up by reusing primitive queries.



Figures are for 5 rounds.

# Query Strategy

- Definition of Set  $S_1$ :

MSB:  $n - \frac{r-2}{r-1}n$  bits are constant ( $c_i$ )

LSB:  $\frac{r-2}{r-1}n$  bits take all values

- Definition of Set  $S_2$ :

MSB:  $\frac{r-2}{r-1}n$  bits take all values

LSB:  $n - \frac{r-2}{r-1}n$  bits are constant ( $c$ )

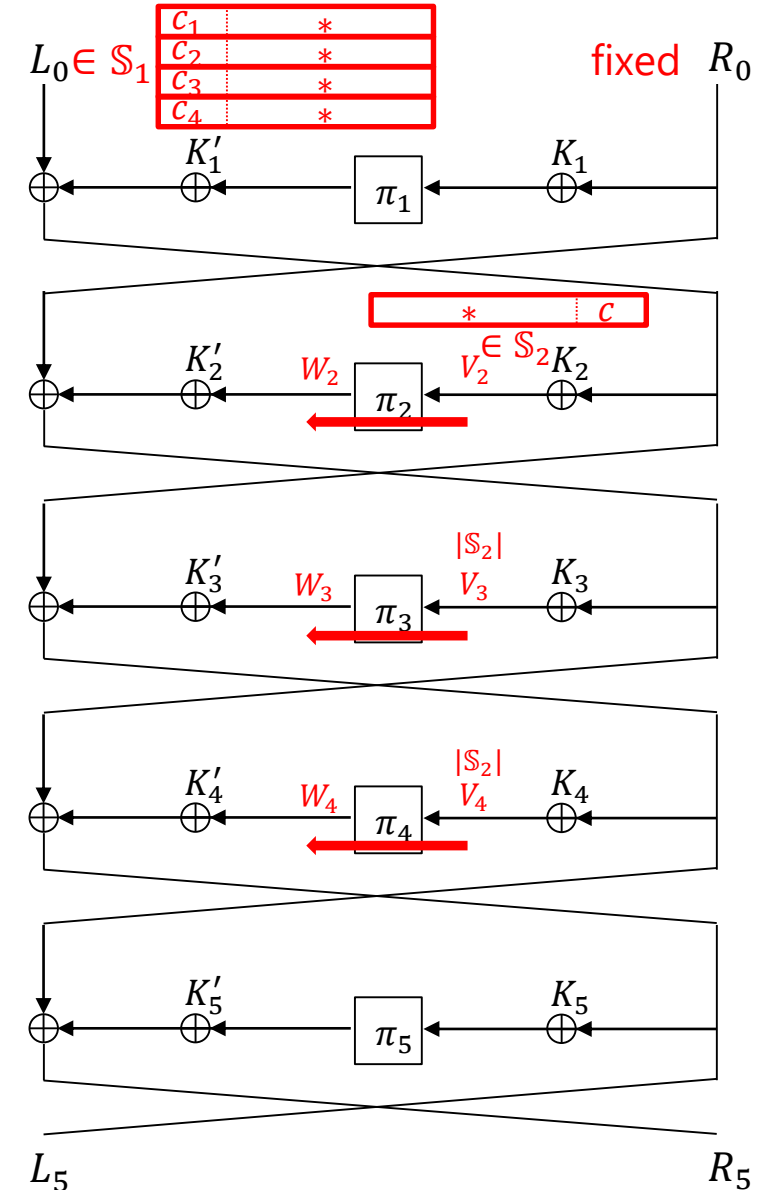
- Construction Queries

- Query  $r - 2$  sets of  $S_1$

- Primitive Queries

- Query  $S_2$  for all but the first and the last rounds.

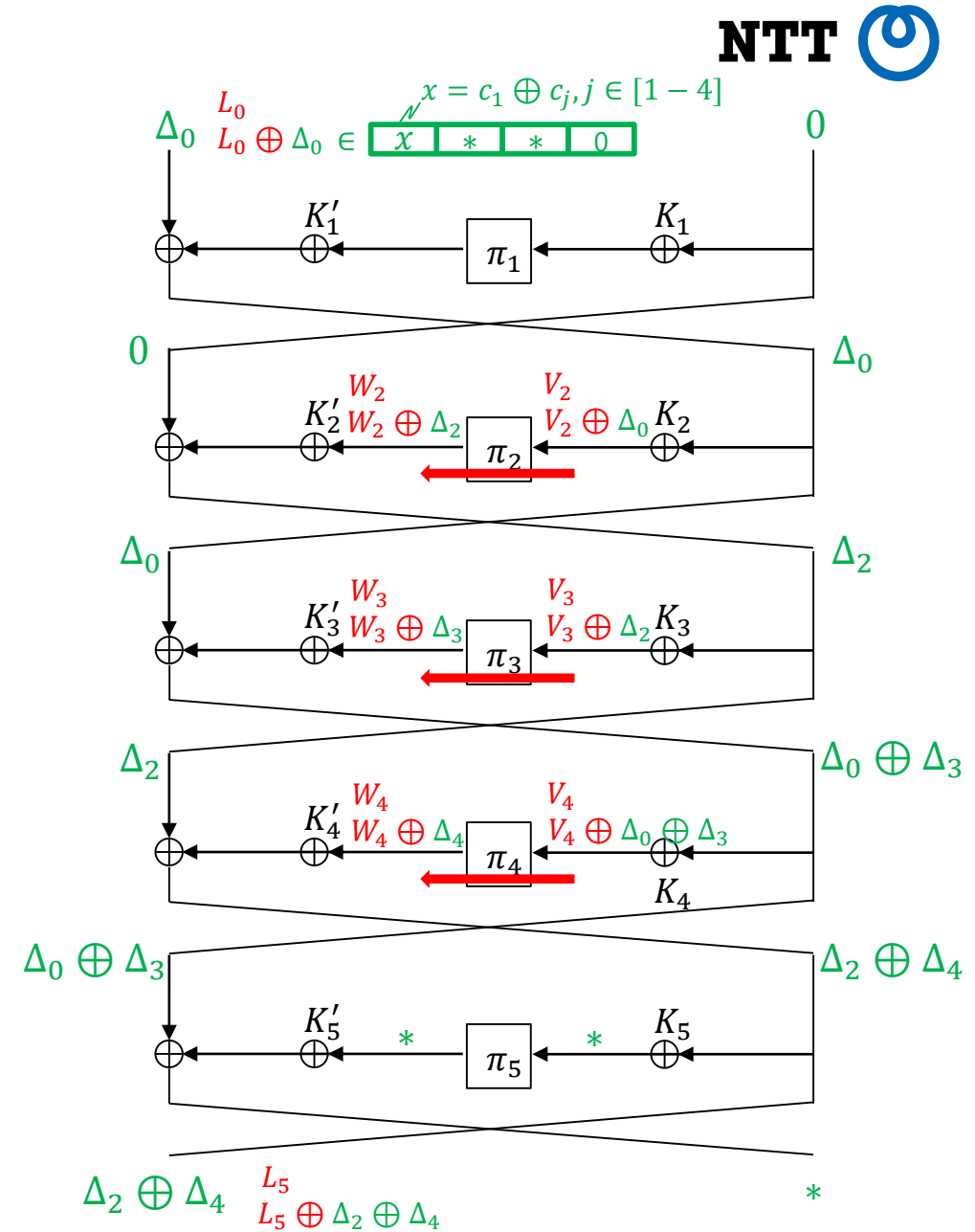
By taking any combination of construction and primitive queries, a match is expected.





# Distinguished Procedure

- For all  $L_0 || R_0, (V_2, W_2), \dots, (V_{r-1}, W_{r-1}), L_r || R_r$ , make a pair with  $L'_0 || R'_0, L'_r || R'_r$ .
- 1<sup>st</sup> Round:  $\Delta_0$  is simply computed.
  - 2<sup>nd</sup> Round:  $V'_2$  is computed  $V_2 \oplus \Delta_0$ .  $V'_2$  exists in primitive queries, so it's possible to look up  $W'_2$ . Then,  $\Delta_2 = W_2 \oplus W'_2$  can be computed.
  - 3<sup>rd</sup> to  $r-1$  rounds:  $V'_i$  is computed  $V_i \oplus \Delta_{i-1}$ . If  $V'_i$  exists in primitive queries, then look up  $W'_i$  and compute  $\Delta_i = W_i \oplus W'_i$ .
  - Last round: Check the correctness of the pair by matching the left-half of the ciphertext.

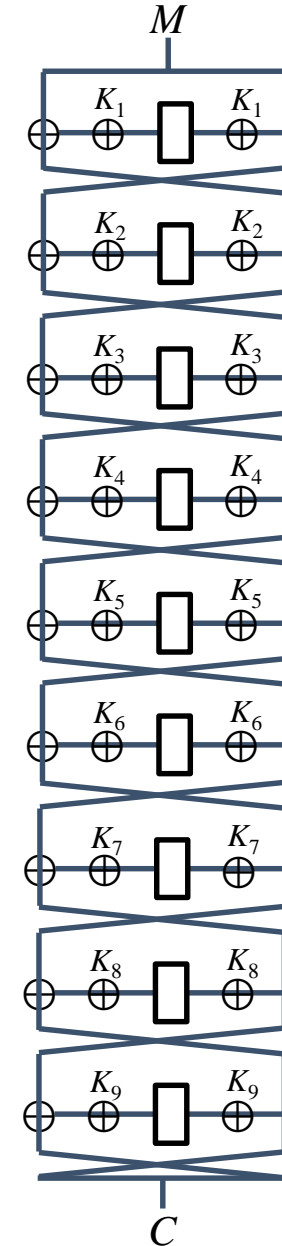




# New Proofs

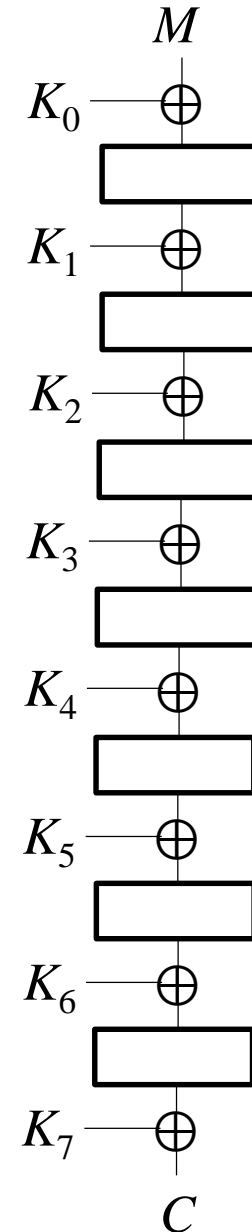
# Proof with Resampling Method

- Tight mu-bound:  $\frac{r-2}{r-1}n$  bits for KAF-P with a single permutation.
- Proof Methods:
  - Patarin's coefficient-H technique.
  - Resampling method with new procedures for KAF-P.
- Resampling method for any  $r$ 
  - Introduced for Key Alternating Cipher at EUROCRYPT2024.
  - Define dummy internal values for each  $(M, C)$  by forward and backward sampling steps in the ideal word.
    1. Perform a forward sampling.
    2. Perform an inverse sampling if a collision occurs for some internal value.



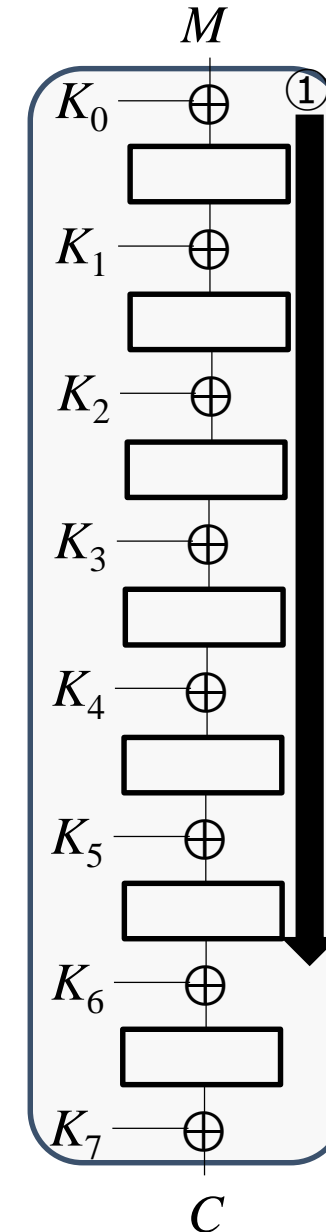
# Proof with Resampling Method

- Tight mu-bound:  $\frac{r-2}{r-1}n$  bits  
for KAF-P with a single permutation.
- Proof Methods:
  - Patarin's coefficient-H technique.
  - Resampling method with new procedures for KAF-P.
- Resampling method for any  $r$ 
  - Introduced for Key Alternating Cipher at EUROCRYPT2024.
  - Define dummy internal values for each  $(M, C)$   
by forward and backward sampling steps in the ideal word.
    1. Perform a forward sampling.
    2. Perform an inverse sampling  
if a collision occurs for some internal value.



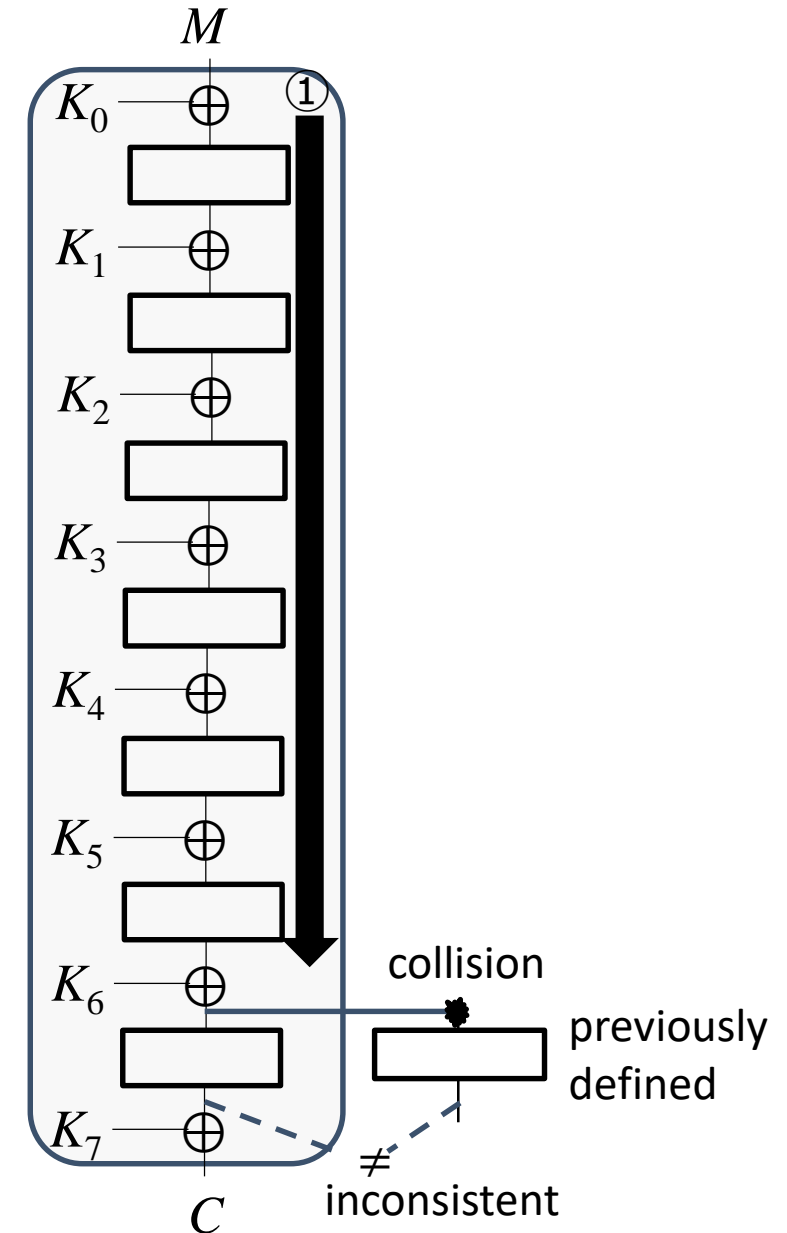
# Proof with Resampling Method

- Tight mu-bound:  $\frac{r-2}{r-1}n$  bits for KAF-P with a single permutation.
- Proof Methods:
  - Patarin's coefficient-H technique.
  - Resampling method with new procedures for KAF-P.
- Resampling method for any  $r$ 
  - Introduced for Key Alternating Cipher at EUROCRYPT2024.
  - Define dummy internal values for each  $(M, C)$  by forward and backward sampling steps in the ideal word.
    1. Perform a forward sampling.
    2. Perform an inverse sampling if a collision occurs for some internal value.



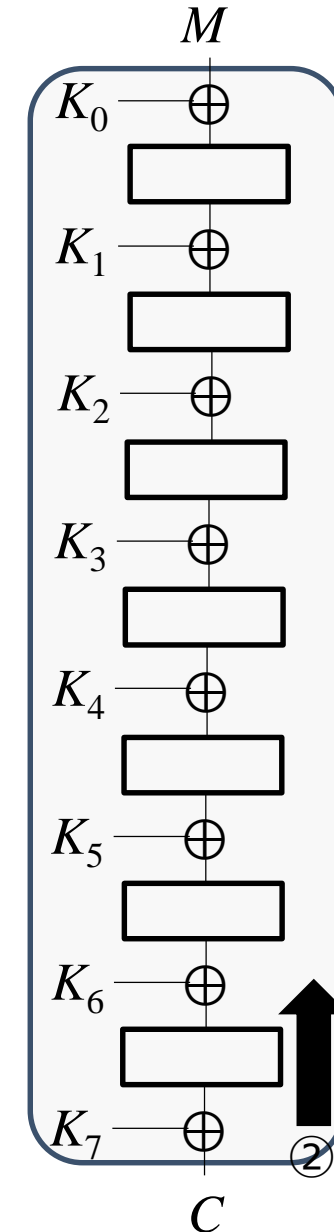
# Proof with Resampling Method

- Tight mu-bound:  $\frac{r-2}{r-1}n$  bits for KAF-P with a single permutation.
- Proof Methods:
  - Patarin's coefficient-H technique.
  - Resampling method with new procedures for KAF-P.
- Resampling method for any  $r$ 
  - Introduced for Key Alternating Cipher at EUROCRYPT2024.
  - Define dummy internal values for each  $(M, C)$  by forward and backward sampling steps in the ideal word.
    1. Perform a forward sampling.
    2. Perform an inverse sampling if a collision occurs for some internal value.



# Proof with Resampling Method

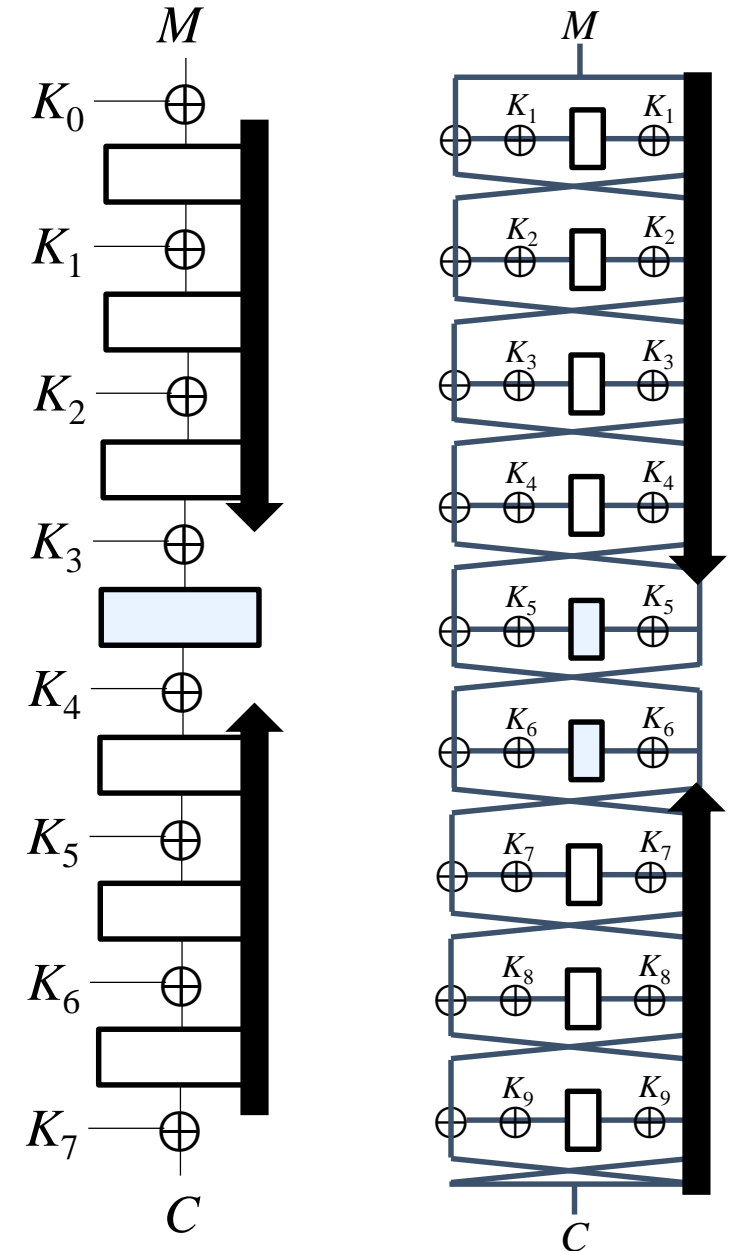
- Tight mu-bound:  $\frac{r-2}{r-1}n$  bits for KAF-P with a single permutation.
- Proof Methods:
  - Patarin's coefficient-H technique.
  - Resampling method with new procedures for KAF-P.
- Resampling method for any  $r$ 
  - Introduced for Key Alternating Cipher at EUROCRYPT2024.
  - Define dummy internal values for each  $(M, C)$  by forward and backward sampling steps in the ideal word.
    1. Perform a forward sampling.
    2. Perform an inverse sampling if a collision occurs for some internal value.





# Resampling Method for KAF-P

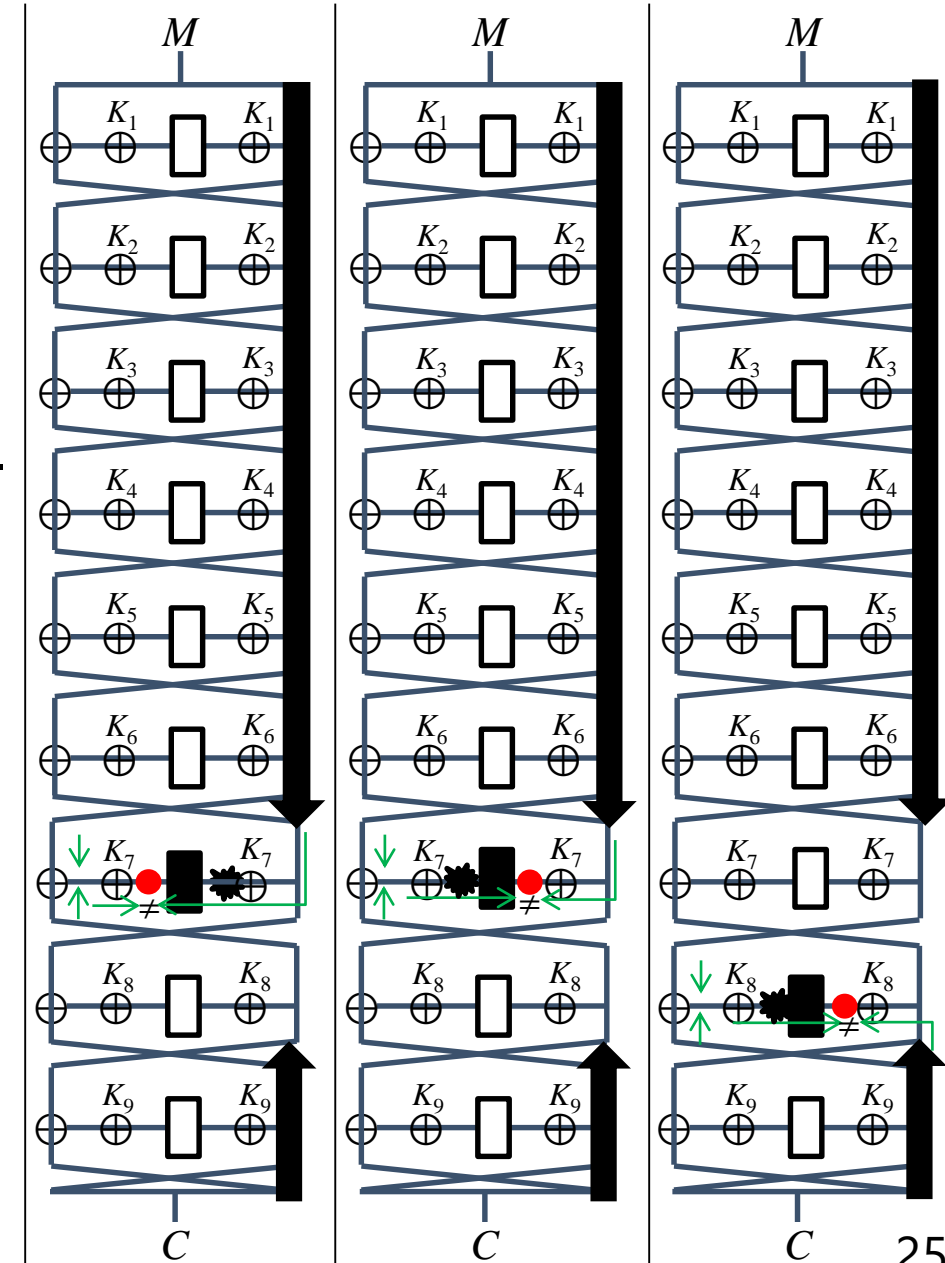
- Update the resampling method for KAF-P with a single permutation.
- Differences between KAC and KAF-P.
  - KAC:  $r - 1$  internal values define all internal values.
  - KAF-P:  $r - 2$  internal values define all internal values.
- Collision events for failures of the resampling method.
  - KAC: 1
  - KAF-P: 3
- We give a new resampling algorithm for KAF-P with the three collision events  
 $\Rightarrow$  Tight mu-bound for KAF-P:  $\frac{r-2}{r-1} n$  bits.





# Resampling Method for KAF-P

- Update the resampling method for KAF-P with a single permutation.
- Differences between KAC and KAF-P.
  - KAC:  $r - 1$  internal values define all internal values.
  - KAF-P:  $r - 2$  internal values define all internal values.
- Collision events for failures of the resampling method.
  - KAC: 1
  - KAF-P: 3
- We give a new resampling algorithm for KAF-P with the three collision events  
 $\Rightarrow$  Tight mu-bound for KAF-P:  $\frac{r-2}{r-1} n$  bits.



# Conclusion

- Provable tight security bound of Feistel KAF-P ciphers
  - in the multi-user (mu) setting
  - a single primitive across all rounds
  - $r - 2$  correlated subkeys for  $r$  rounds
- By applying the resampling method to Feistel KAF-P ciphers, security is proven to be  $O(2^{\frac{r-2}{r-1}n})$  for  $r$  rounds.
- We also provide a new matching attack by information-theoretic variant of the meet-in-the-middle attack.

*Thank you for your attention!!*