NTT

Meet-in-the-Middle Attacks on Feistel Functions: Impact of Omitting the Last Network Twist

Yu Sasaki

NTT Corporation

ESC 2013 (14/Jan/2013@Luxembourg)

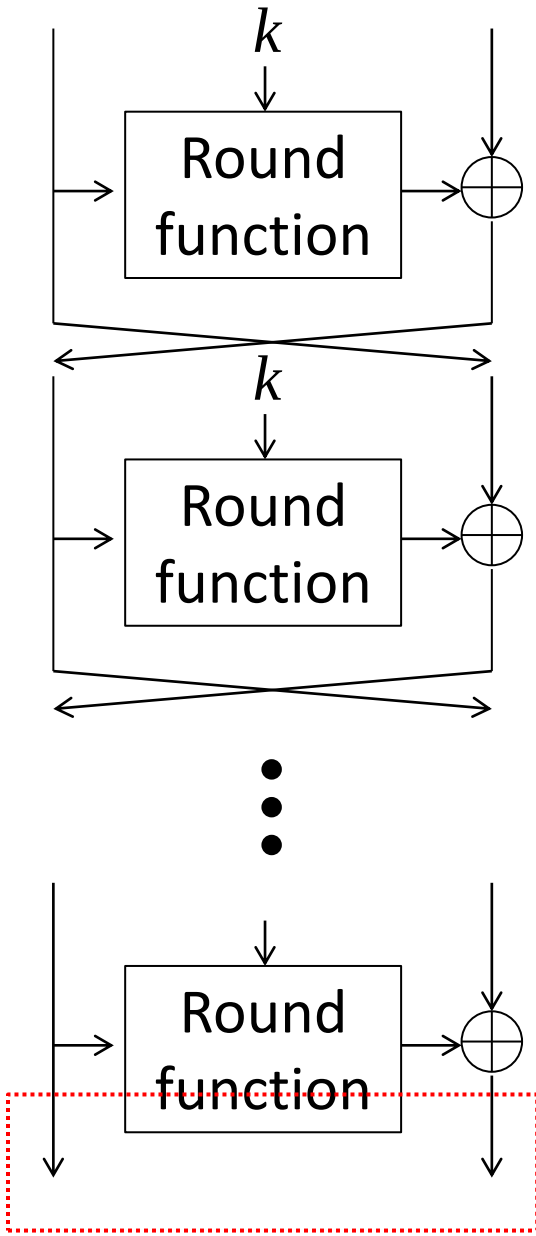
NTT

Contents

- Background
- Round shrink via feed-forward
- Analysis on generic Feistel-SP functions
- Applications to Camellia and CLEFIA
- Concluding remarks

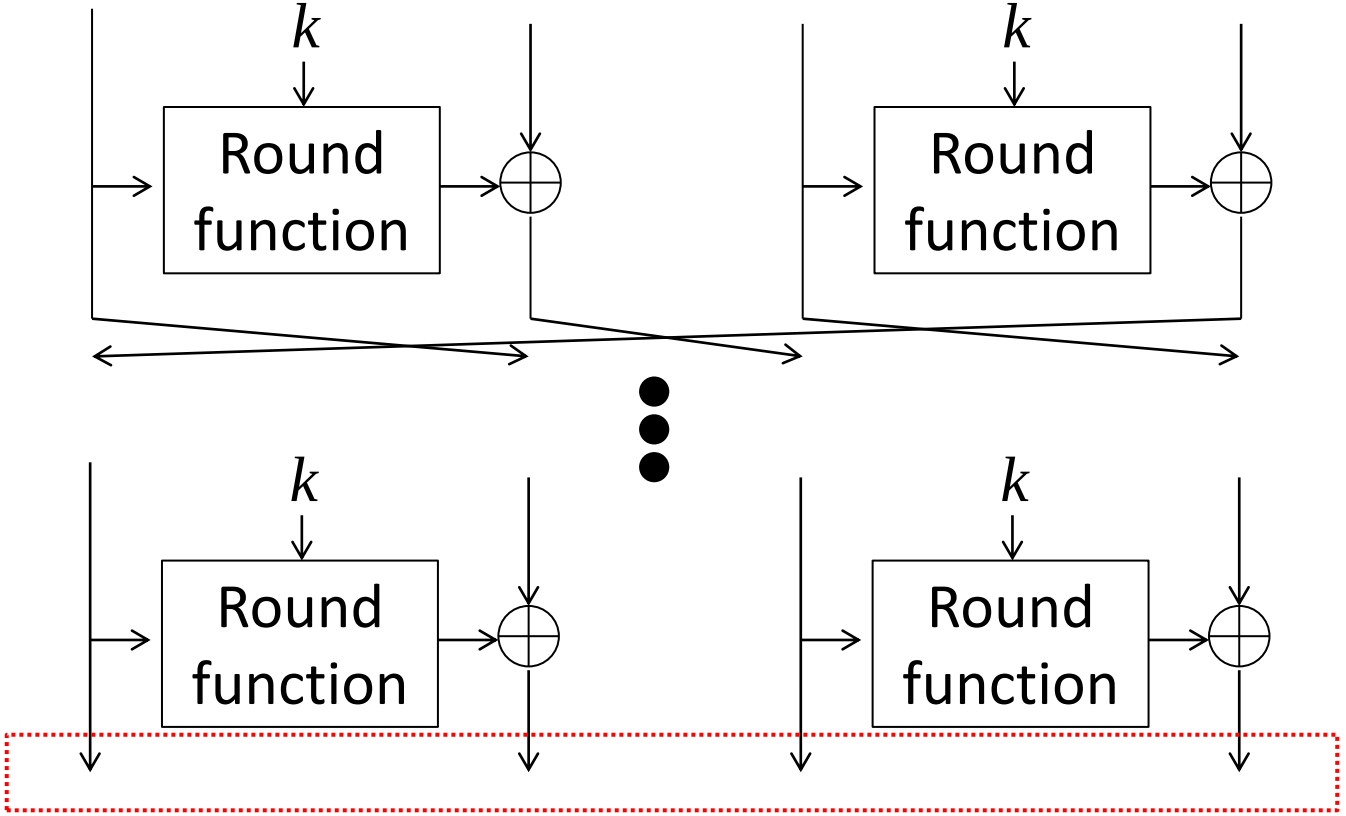
Feistel Structure

- Widely used since the design of DES
- Build a 2n-bit cipher from an n-bit round function.
- The network twist may be omitted in the last round



Generalized Feistel Structure

- Build a 2n-bit cipher from an n/2-bit round function
- suitable for compact implementations



NTT

Omission of the Last Network Twist

- In many designs, the network twist is omitted in the last round.

  Ex. ISO standard ciphers: Camellia, CLEFIA, HIGHT

- This makes the encryption and decryption algorithms symmetric.
- Then, it leads to some advantage in the implementation.
- The omission does not lower the security bound against differential and linear analyses.

NTT

Similar Design in AES

- AES also takes the same approach, which omits MixColumns in the last round.

- Impact of the omission
  - Several attack approaches other than DC and LC cleverly utilizes the omission [DK10].
  - In hashing modes, splice-and-cut technique for a preimage attack can work efficiently [S11].

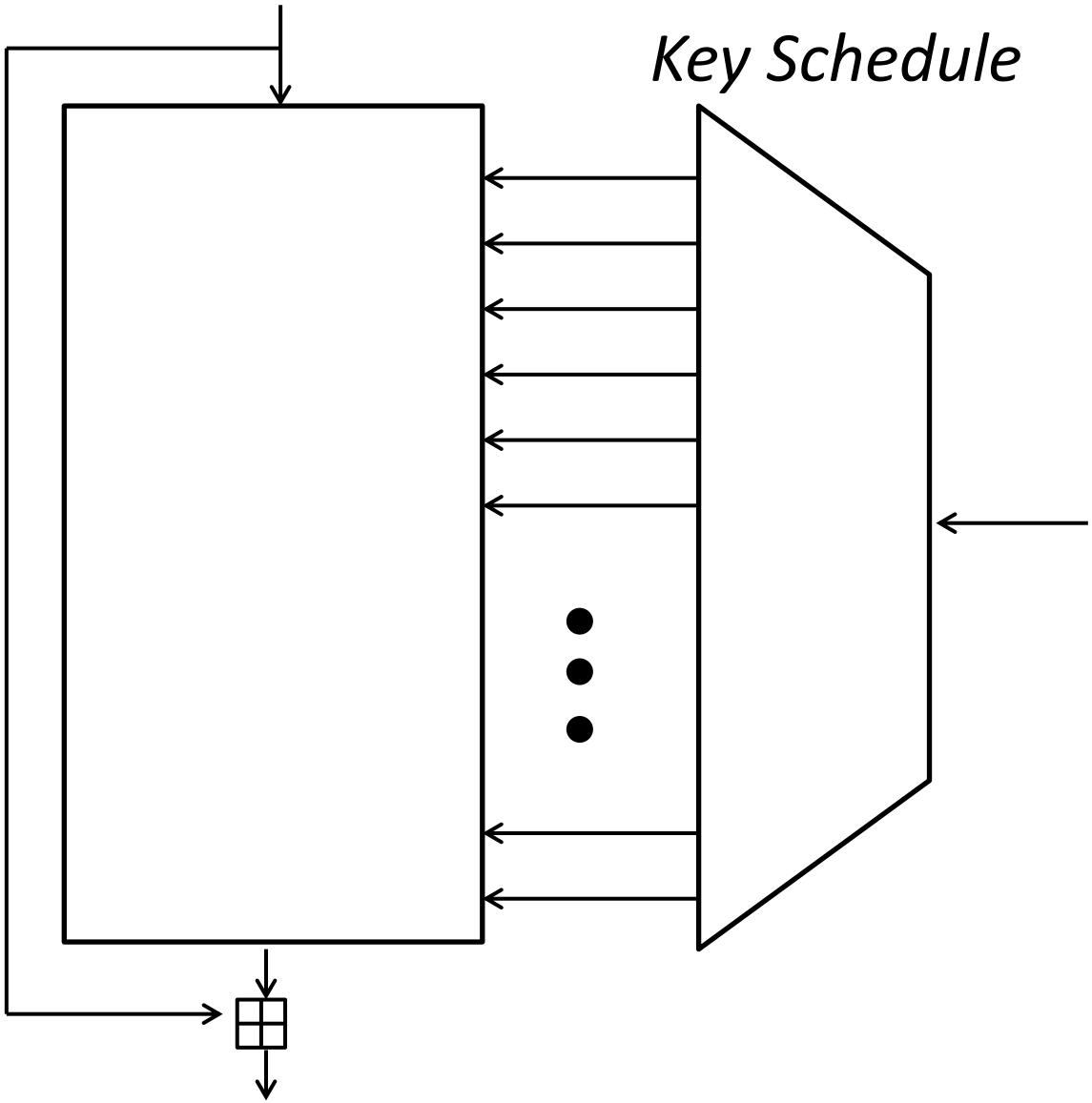
NTT

Research Summary

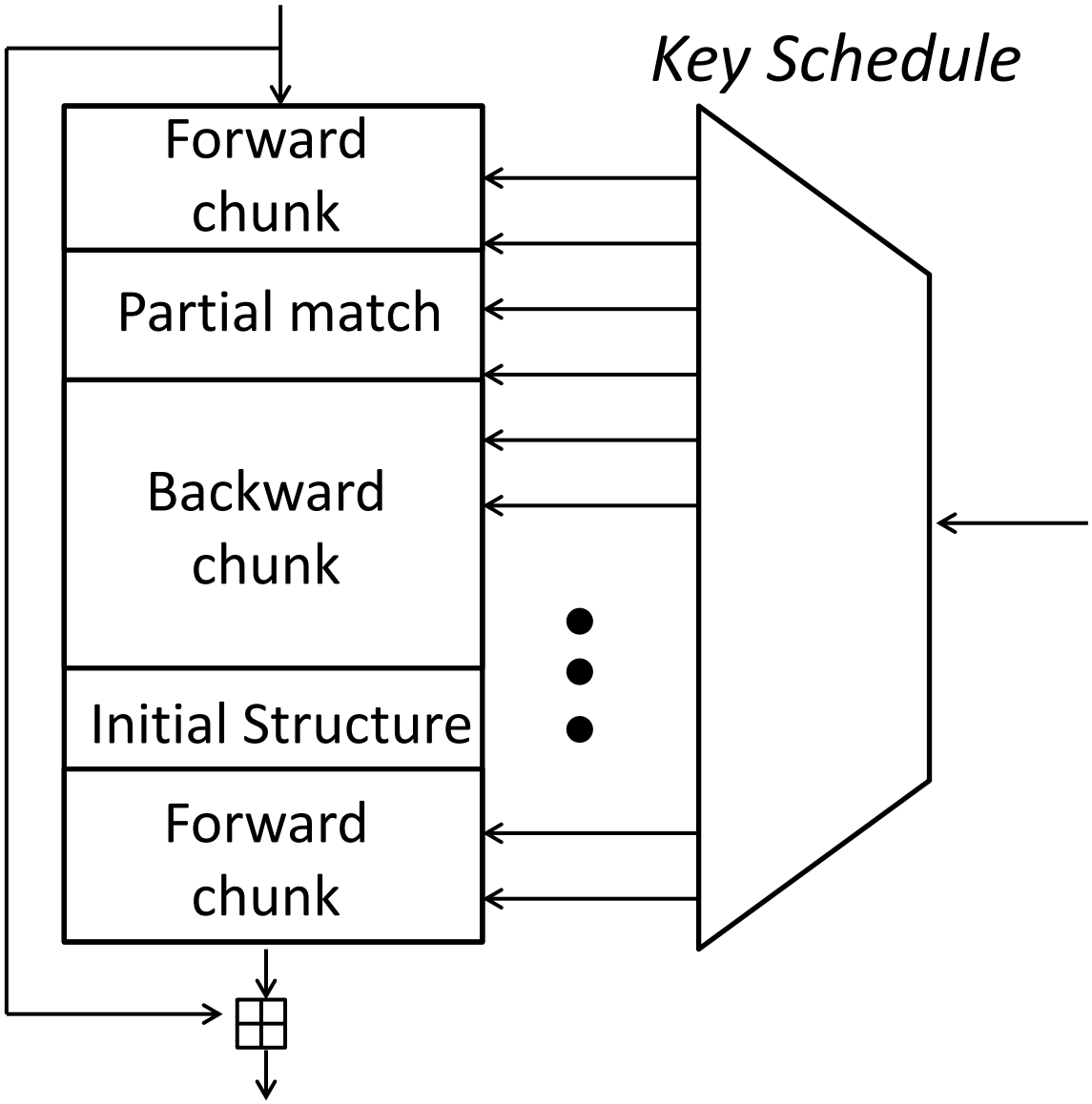
- This research shows that the omission of the last network twist can be a weakness against MitM preimage attacks in hashing modes.

- Application to generic Feistel-SP
  - 11 rounds can be attacked if key schedule is weak.
- Application to generic 4-branch Type-2 GFN
  - 15 rounds can be attacked for any key schedule.

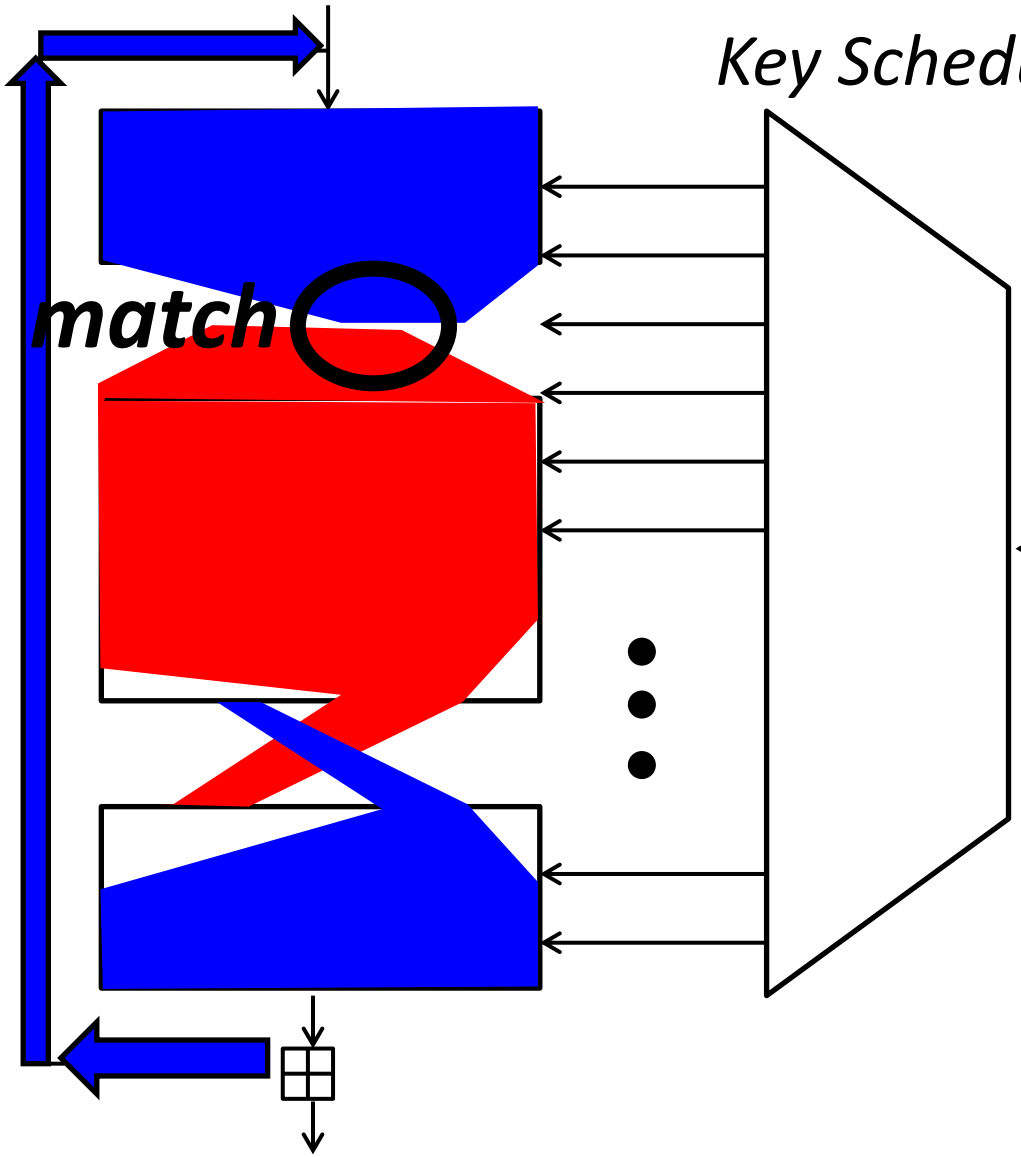
MitM Preimage Attacks



MitM Preimage Attacks



MitM Preimage Attacks

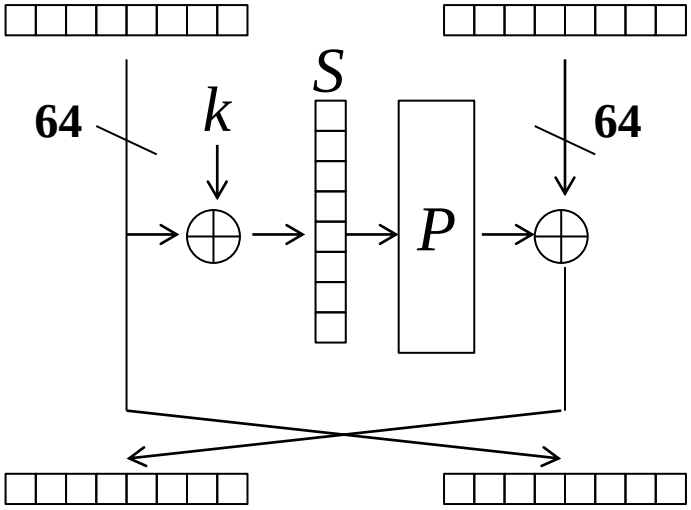


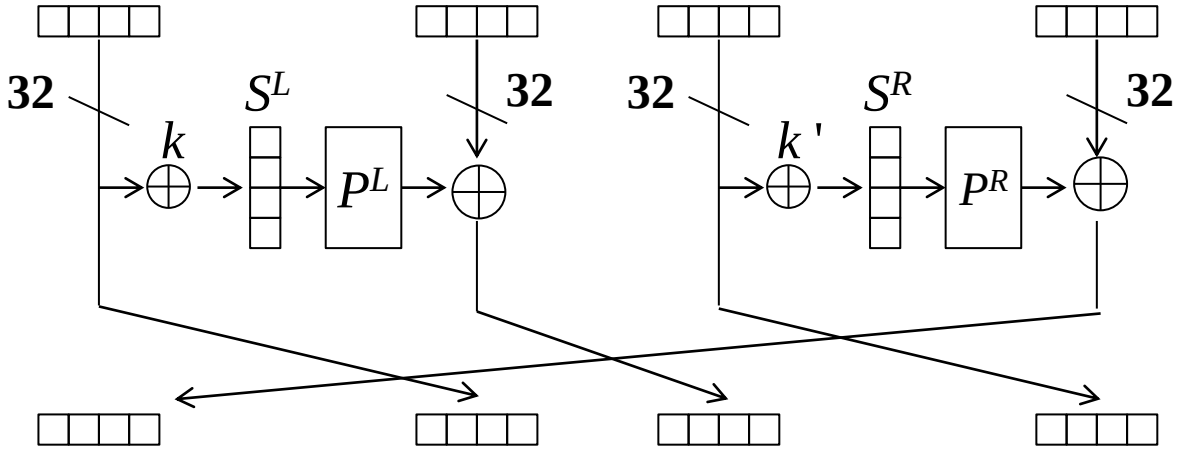
Key value is constant.

Free bits are in the state.

Target Structure

- SP round function:
  - Subkey addition
  - S-box transformation for *r* bytes.
  - Linear transformation with branch number *r*+1.
- Analyze the same size as Camellia and CLEFIA.



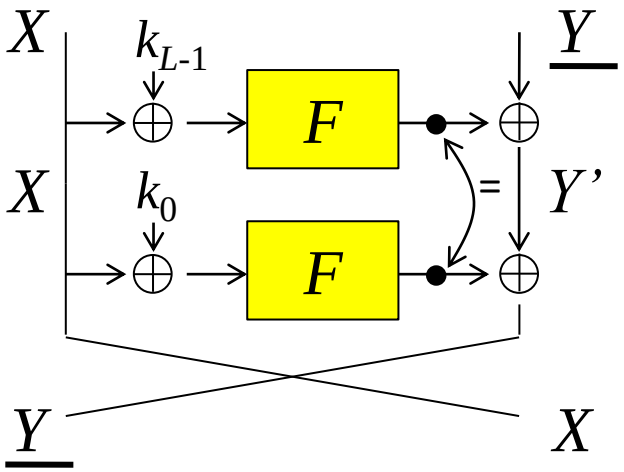


Key Idea (Round Shrink)

- Thanks to the Splice-and-Cut, MitM attack can start from the last round (without the network twist).

Last round

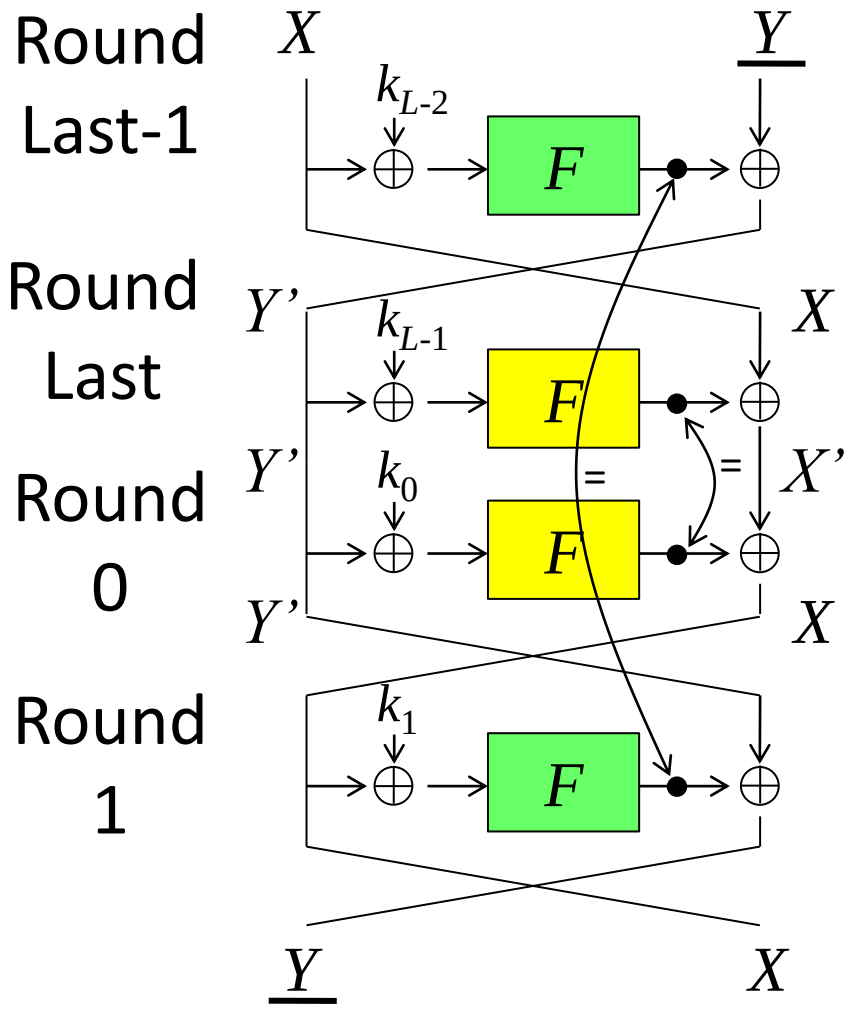
First round



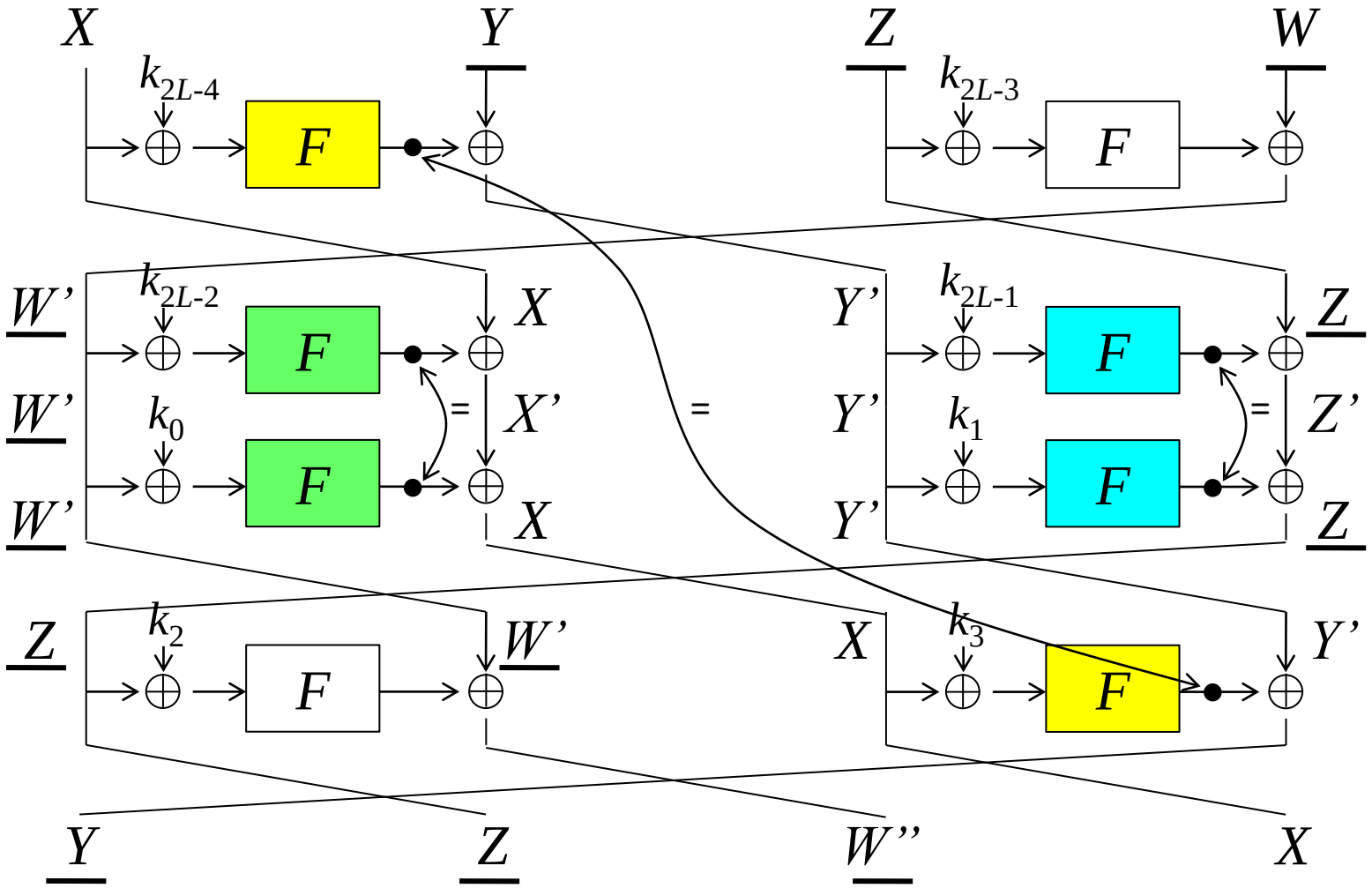
- If input to F in two rounds are identical, the output are cancelled.
- In hashing modes, key values are chosen by attackers.

4-Round Shrink on Feistel

- Start from the second last round.
- Round shrink twice
- *n*-bit relation among subkeys → requires 2^n costs in generic.
- Attack is valid only if such subkeys can be obtained through KSF.



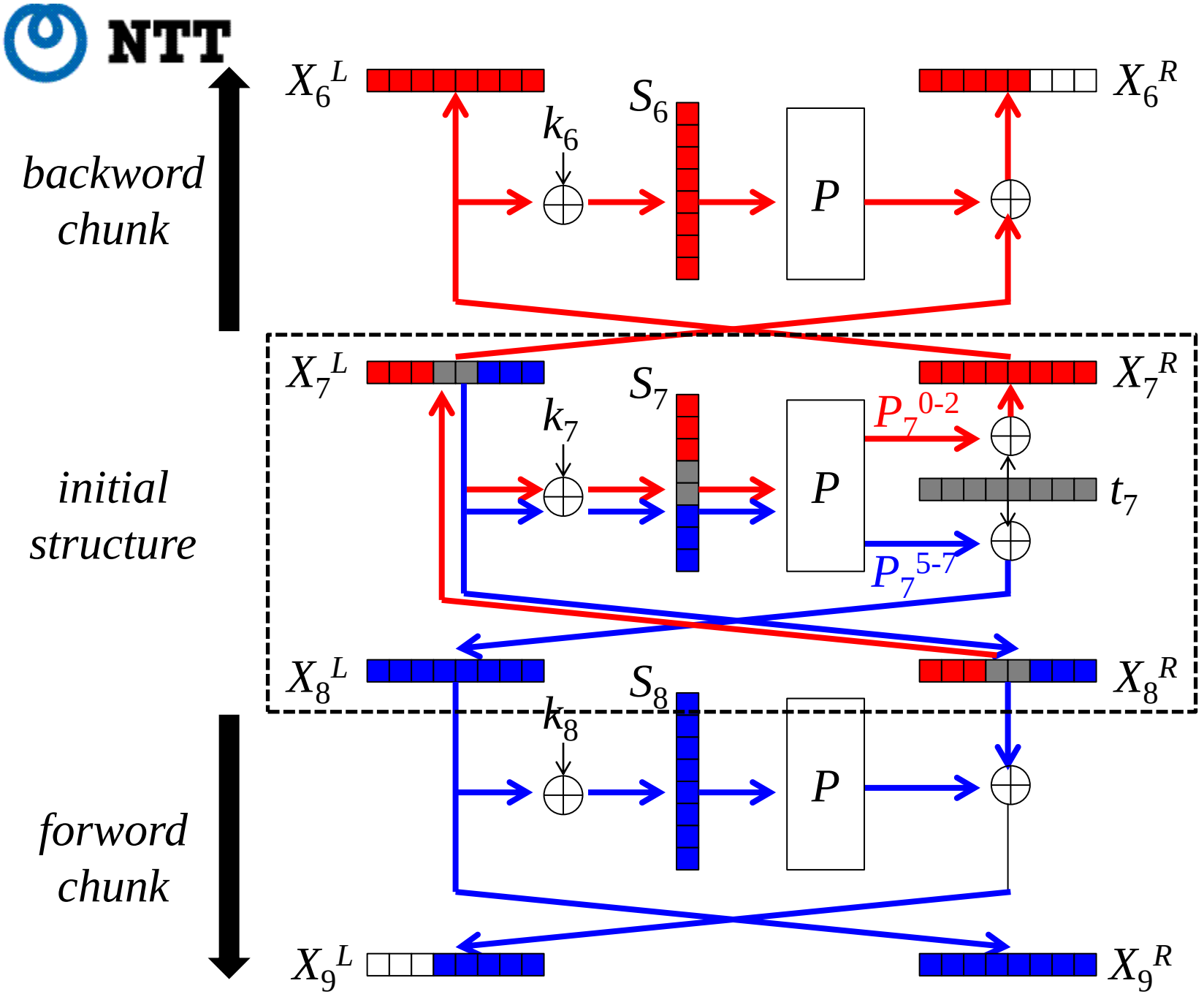
4-Round Shrink on 4-branch Type-2 GFN

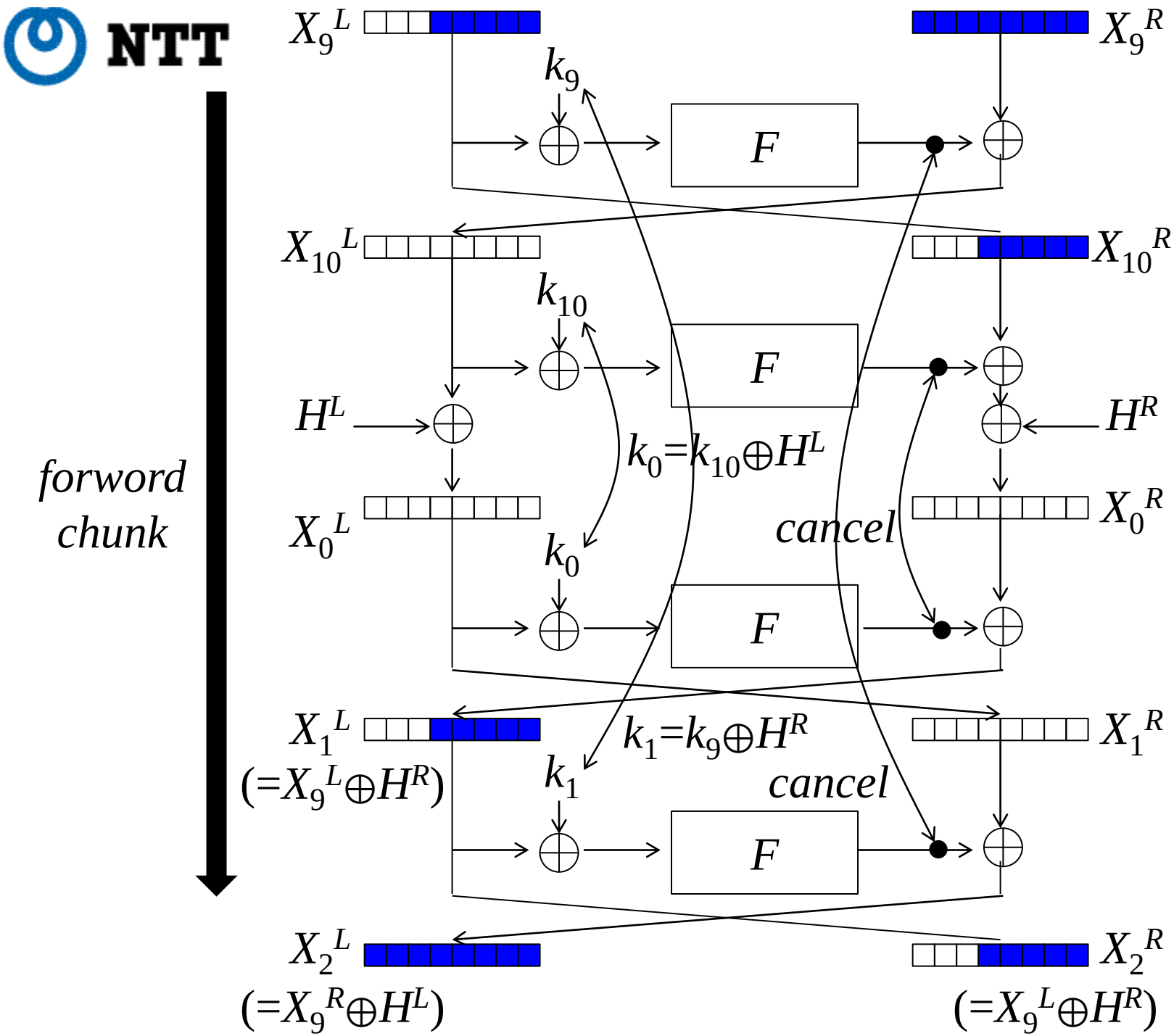


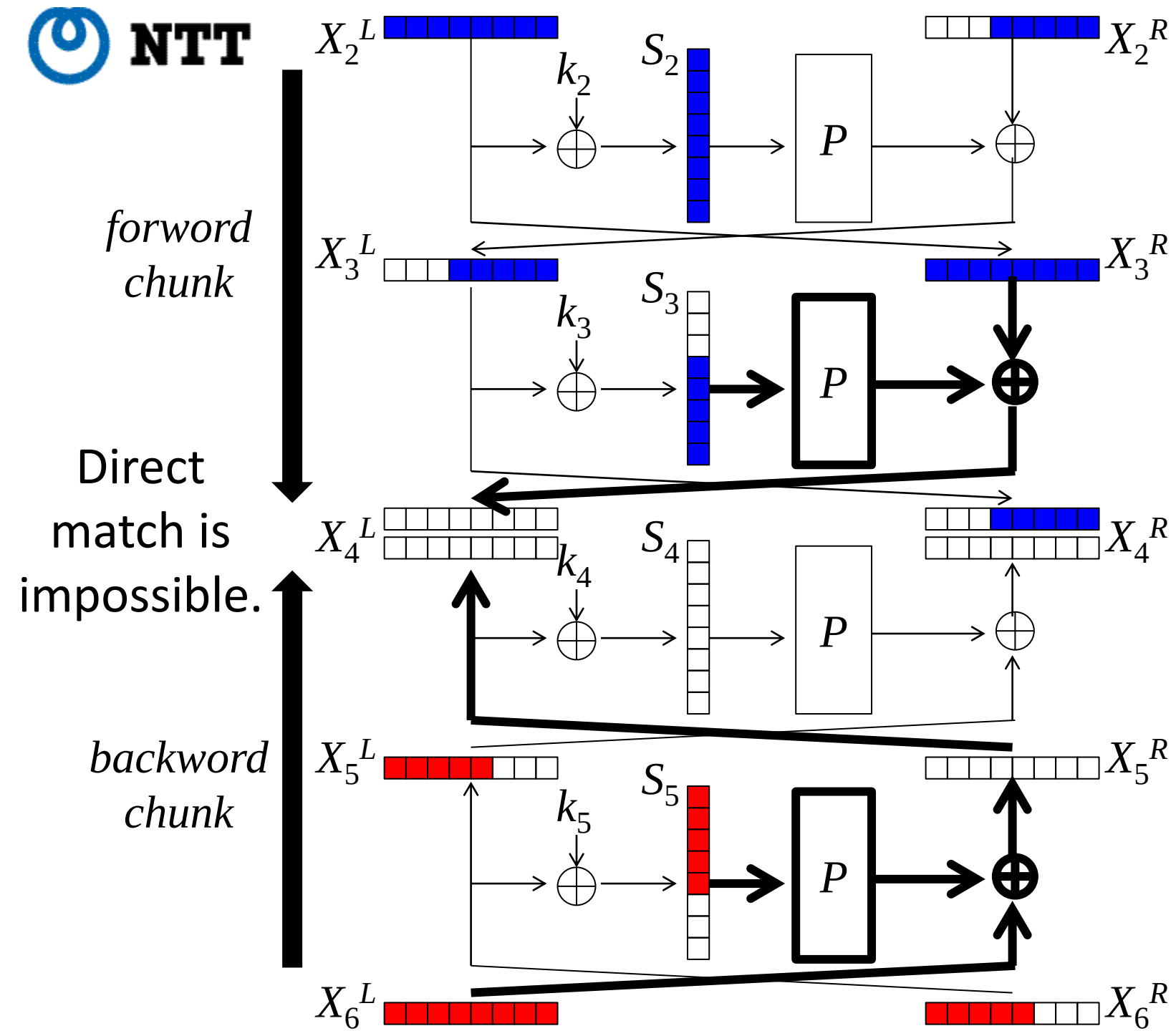
3n/2-bit relation among subkeys. With $2^{3n/2}$ cost, such keys can be found for any key schedule.

NTT

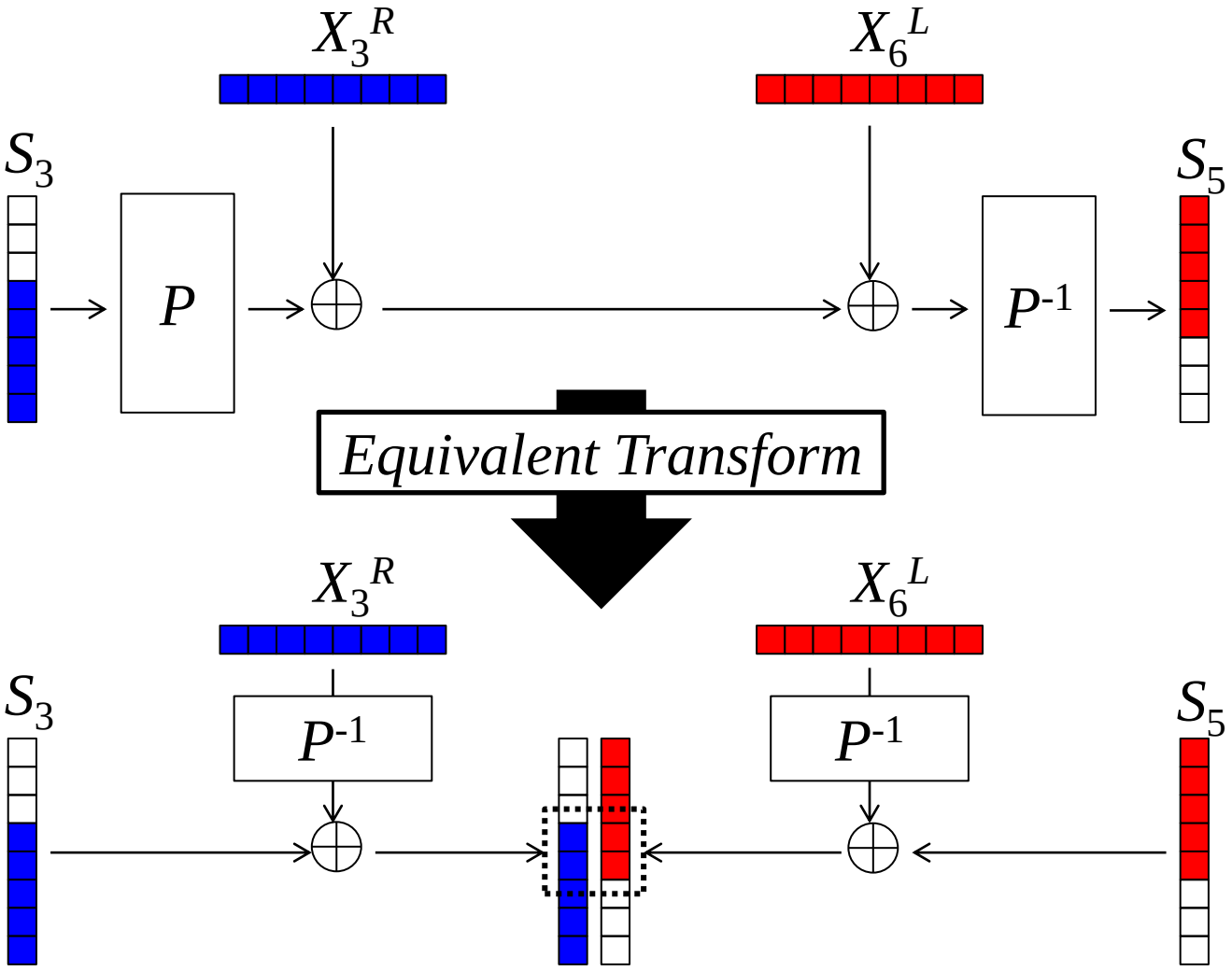
11 Round Preimage Attack on Generic Feistel-SP


backword chunk
initial structure
forword chunk
X_6^L
X_6^R
k_6
S_6
P
X_7^L
X_7^R
k_7
S_7
P
P_7^{0-2}
t_7
P_7^{5-7}
X_8^L
X_8^R
k_8
S_8
P
X_9^L
X_9^R


X_9^L
X_9^R
k_9
F
X_{10}^L
X_{10}^R
k_{10}
F
H^L
H^R
$k_0=k_{10}\oplus H^L$
X_0^L
X_0^R
cancel
k_0
F
X_1^L
X_1^R
$k_1=k_9\oplus H^R$
$(=X_9^L\oplus H^R)$
k_1
cancel
F
X_2^L
X_2^R
$(=X_9^R\oplus H^L)$
$(=X_9^L\oplus H^R)$
forword
chunk


NTT
X_2^L
X_2^R
k_2
S_2
P
forword chunk
X_3^L
X_3^R
k_3
S_3
P
Direct match is impossible.
X_4^L
X_4^R
k_4
S_4
P
backword chunk
X_5^L
X_5^R
k_5
S_5
P
X_6^L
X_6^R

Equivalent Linear Transformation



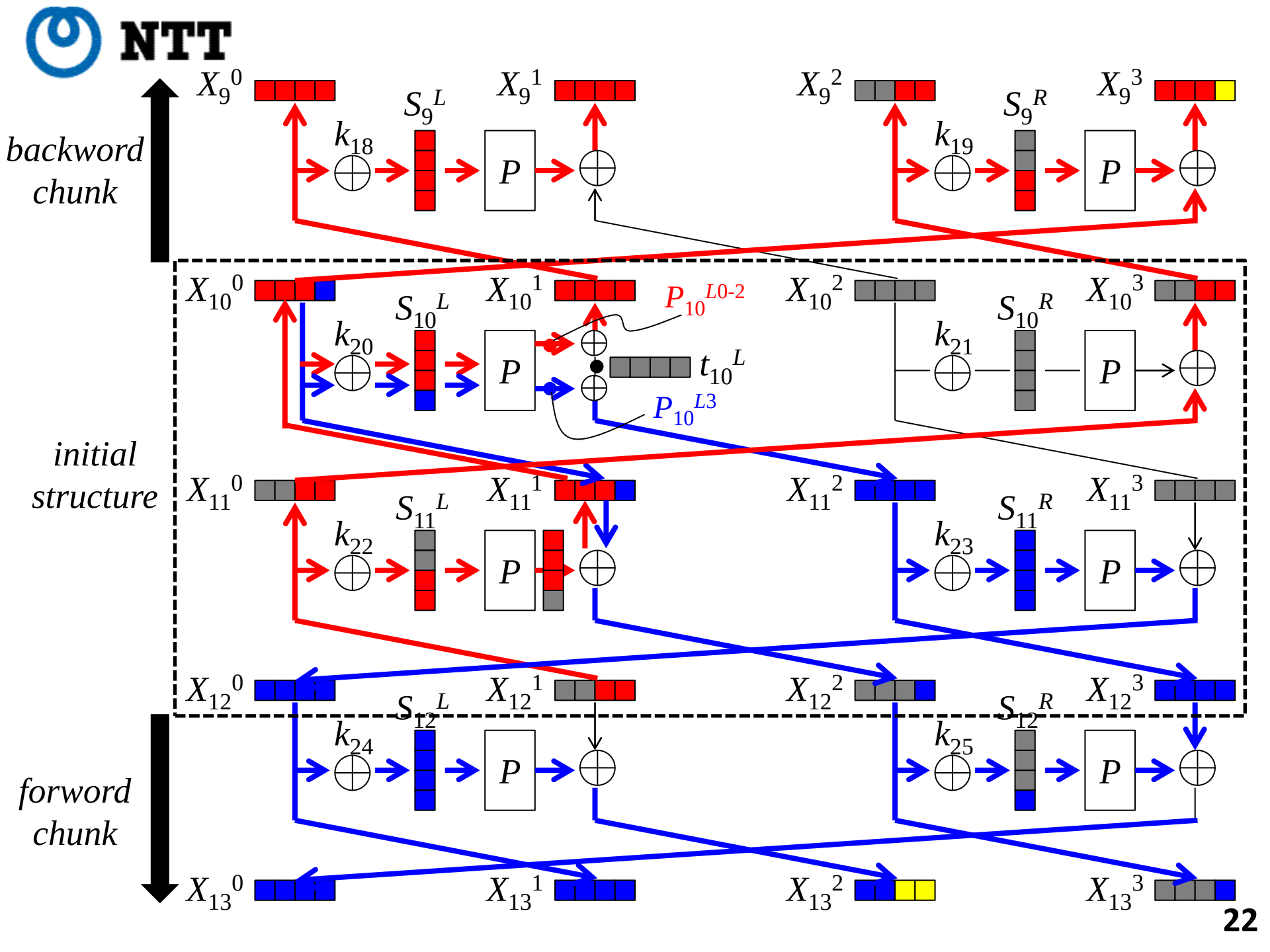
2-byte match

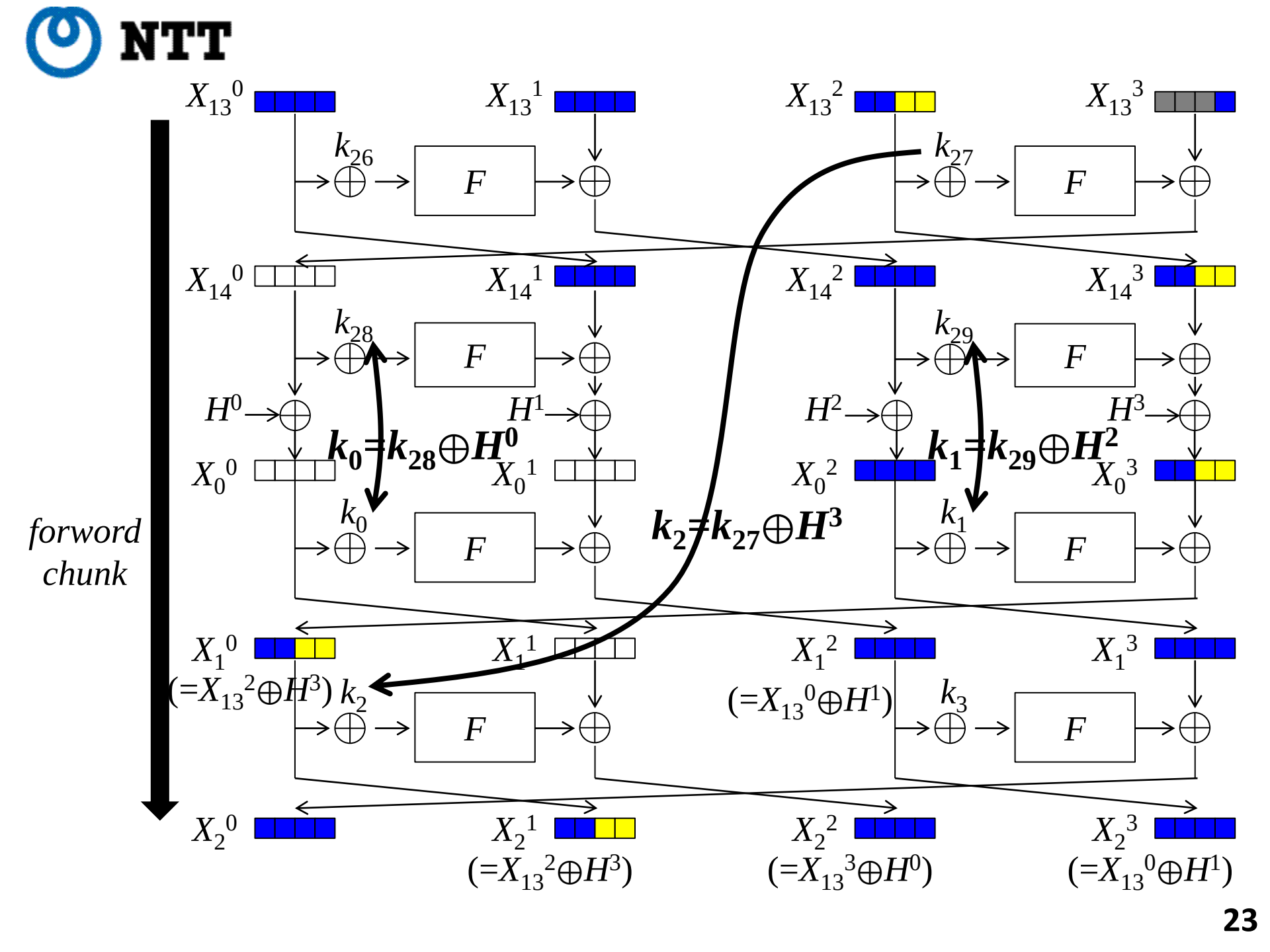
NTT

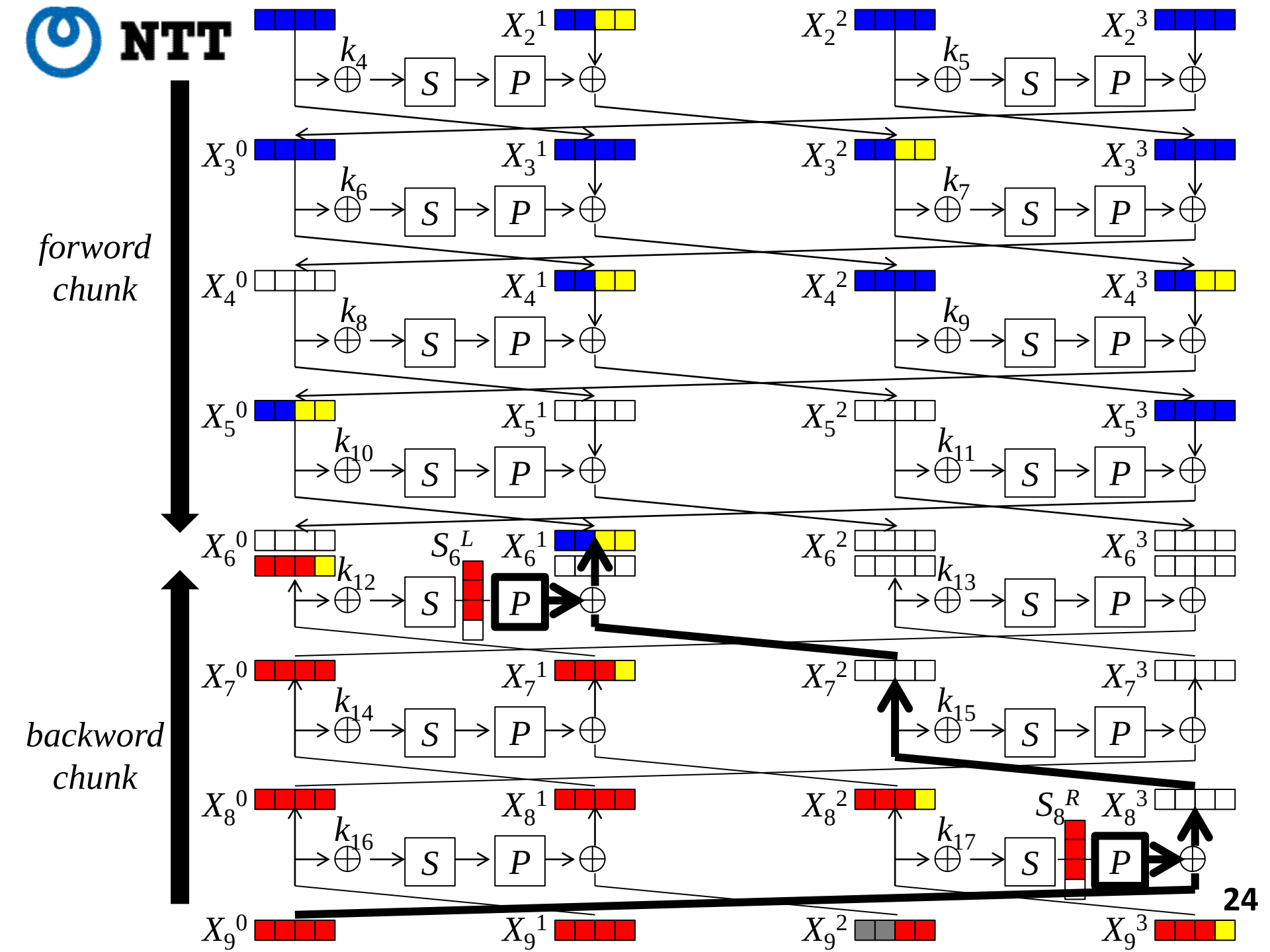
Attack Summary

- 11 Rounds are attacked on generic Feistel-SP. (3-round IS, 4-round shrink, 4-round match)
- For the same parameter as Camellia, 3-byte freedom degrees and 2-byte match. The attack is improved by a factor of 2^{16}.
- Needs to satisfy *n*-bit subkey relations. The attack is valid only if KSF is weak.

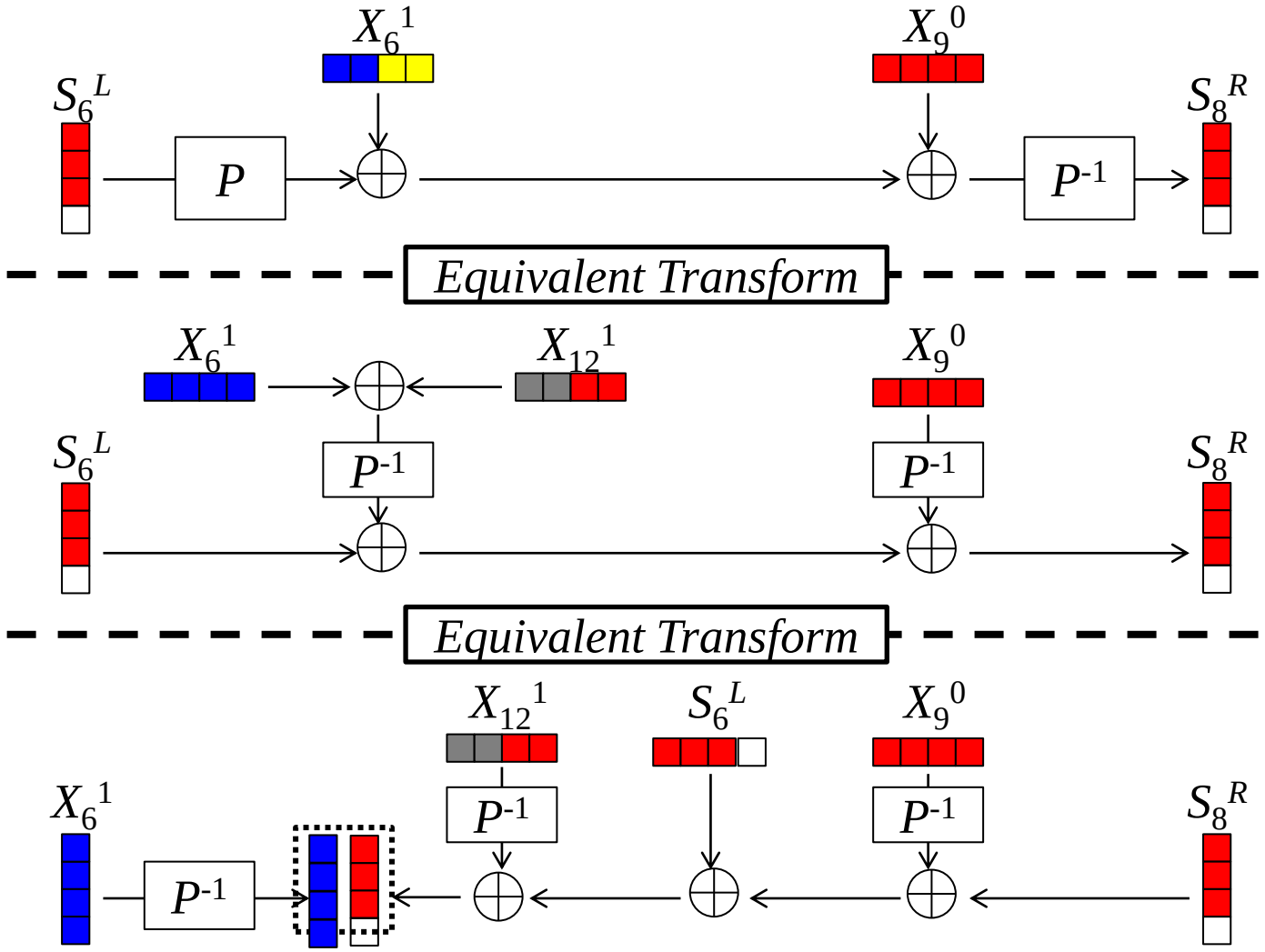
15 Round Preimage Attack on Generic 4-branch Type-2 GFN


NTT
backword chunk
initial structure
forword chunk
X_9^0
X_9^1
X_9^2
X_9^3
S_9^L
S_9^R
k_{18}
k_{19}
P
X_{10}^0
X_{10}^1
X_{10}^2
X_{10}^3
S_{10}^L
S_{10}^R
k_{20}
k_{21}
$P_{10}^{L0\text{-}2}$
t_{10}^L
P_{10}^{L3}
X_{11}^0
X_{11}^1
X_{11}^2
X_{11}^3
S_{11}^L
S_{11}^R
k_{22}
k_{23}
X_{12}^0
X_{12}^1
X_{12}^2
X_{12}^3
S_{12}^L
S_{12}^R
k_{24}
k_{25}
X_{13}^0
X_{13}^1
X_{13}^2
X_{13}^3


X_{13}^0
X_{13}^1
X_{13}^2
X_{13}^3
k_{26}
k_{27}
F
X_{14}^0
X_{14}^1
X_{14}^2
X_{14}^3
k_{28}
k_{29}
H^0
H^1
H^2
H^3
$k_0 = k_{28} \oplus H^0$
$k_1 = k_{29} \oplus H^2$
X_0^0
X_0^1
X_0^2
X_0^3
k_0
k_1
$k_2 = k_{27} \oplus H^3$
forword chunk
X_1^0
X_1^1
X_1^2
X_1^3
$(=X_{13}^2 \oplus H^3)$ k_2
$(=X_{13}^0 \oplus H^1)$
k_3
X_2^0
X_2^1
X_2^2
X_2^3
$(=X_{13}^2 \oplus H^3)$
$(=X_{13}^3 \oplus H^0)$
$(=X_{13}^0 \oplus H^1)$


NTT
forword chunk
backword chunk
X_2^1
X_2^2
X_2^3
k_4
k_5
X_3^0
X_3^1
X_3^2
X_3^3
k_6
k_7
X_4^0
X_4^1
X_4^2
X_4^3
k_8
k_9
X_5^0
X_5^1
X_5^2
X_5^3
k_{10}
k_{11}
X_6^0
S_6^L
X_6^1
X_6^2
X_6^3
k_{12}
k_{13}
X_7^0
X_7^1
X_7^2
X_7^3
k_{14}
k_{15}
X_8^0
X_8^1
X_8^2
S_8^R
X_8^3
k_{16}
k_{17}
X_9^0
X_9^1
X_9^2
X_9^3
S
P

Equivalent Linear Transformation



3-byte match

Attack Summary

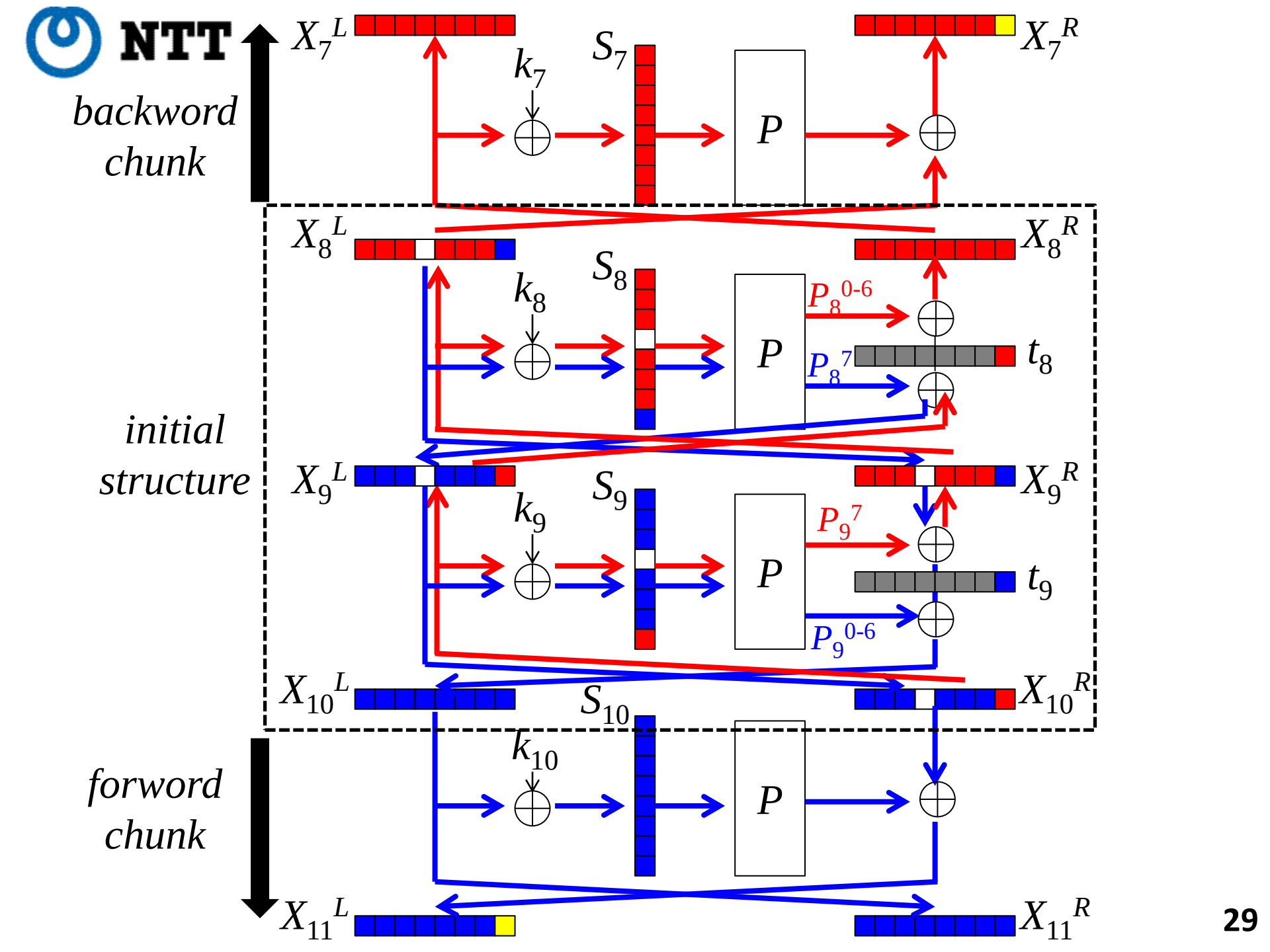
- 15 Rounds are attacked on generic 4-branch type-2 GFN. (4-round IS, 4-round shrink, 7-round match)
- For the same parameter as CLEFIA, 1-byte freedom degrees and 3-byte match. The attack is improved by a factor of 2^8.
- Analysis of KSF requires $2^{3n/2}$ cost. The attack works for any KSF.
- Linear relations with free bits for the other chunk is traced during the MitM attack.

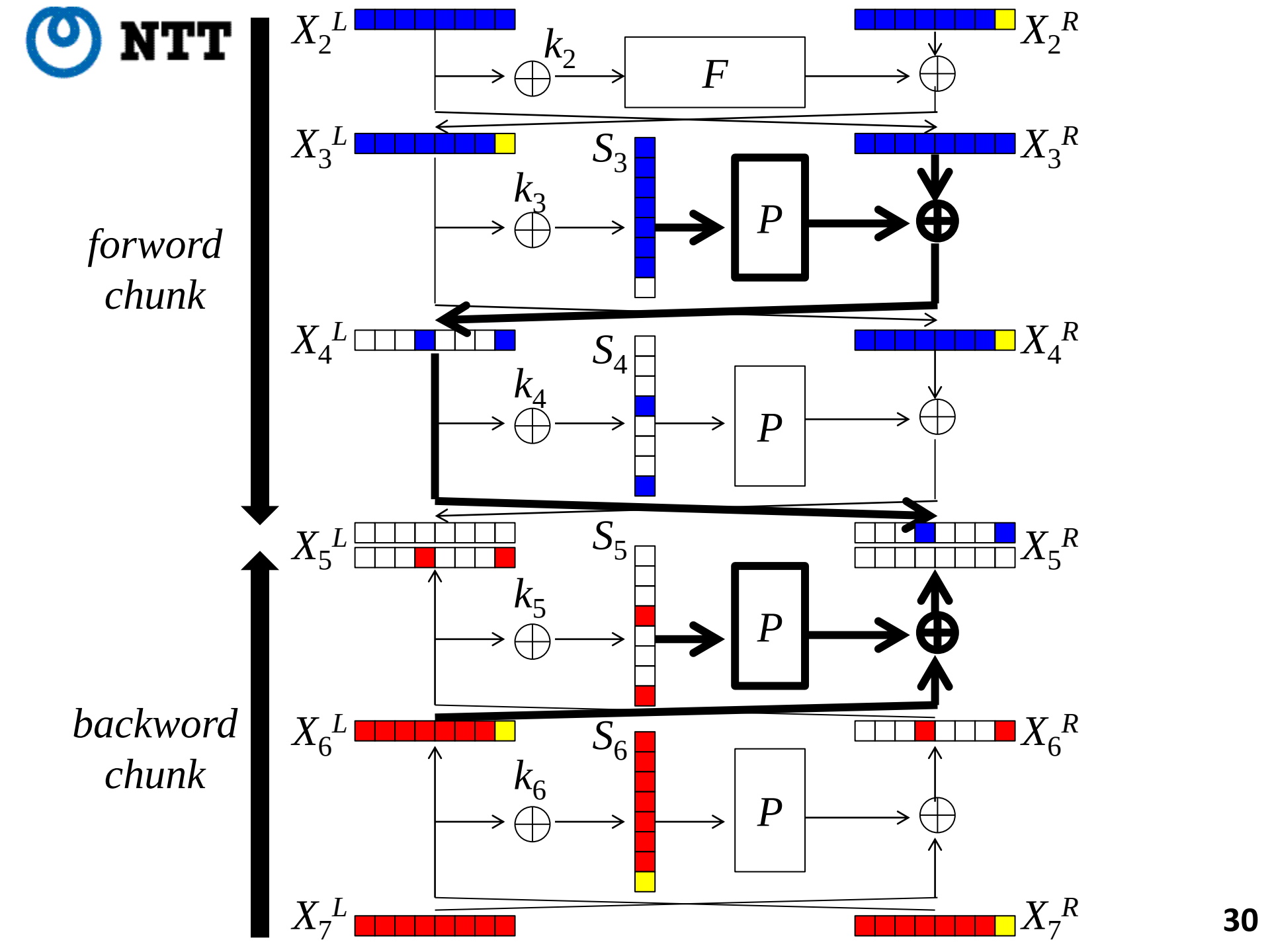
Applications to Camellia without FL and whitening layers

Camellia

- Jointly designed by Mitsubishi Electric Corporation and NTT.

- Standard Feistel with 64-bit round function, but the branch number of the linear computation is only 5 (rather than 9).


NTT
backword chunk
initial structure
forword chunk
X_7^L
X_7^R
k_7
S_7
P
X_8^L
X_8^R
k_8
S_8
P_8^{0-6}
P_8^7
t_8
X_9^L
X_9^R
k_9
S_9
P_9^7
t_9
P_9^{0-6}
X_{10}^L
X_{10}^R
S_{10}
k_{10}
X_{11}^L
X_{11}^R


NTT
forword chunk
backword chunk
X_2^L
X_2^R
k_2
F
X_3^L
X_3^R
S_3
k_3
P
X_4^L
X_4^R
S_4
k_4
P
X_5^L
X_5^R
S_5
k_5
P
X_6^L
X_6^R
S_6
k_6
P
X_7^L
X_7^R

Analysis of Key Schedule Function

- Two subkey relations must be satisfied.
  - $k_0 = k_{12} \oplus H^L, \quad k_1 = k_{11} \oplus H^R.$
- First relation is satisfied probabilistically.
- Need to satisfy second relation efficiently.
  - k_1 is right half of K_A,
  - k_{11} is right half of $K_A^{<<<60}$.
- Because the relation between K_1 and K_{11} is simple, they can be satisfied easily.

Attack Summary

- Due to the small branch number of *P*-layer:
  - Initial structure is extended by 1 round.
  - Matching phase is extended by 1 round.

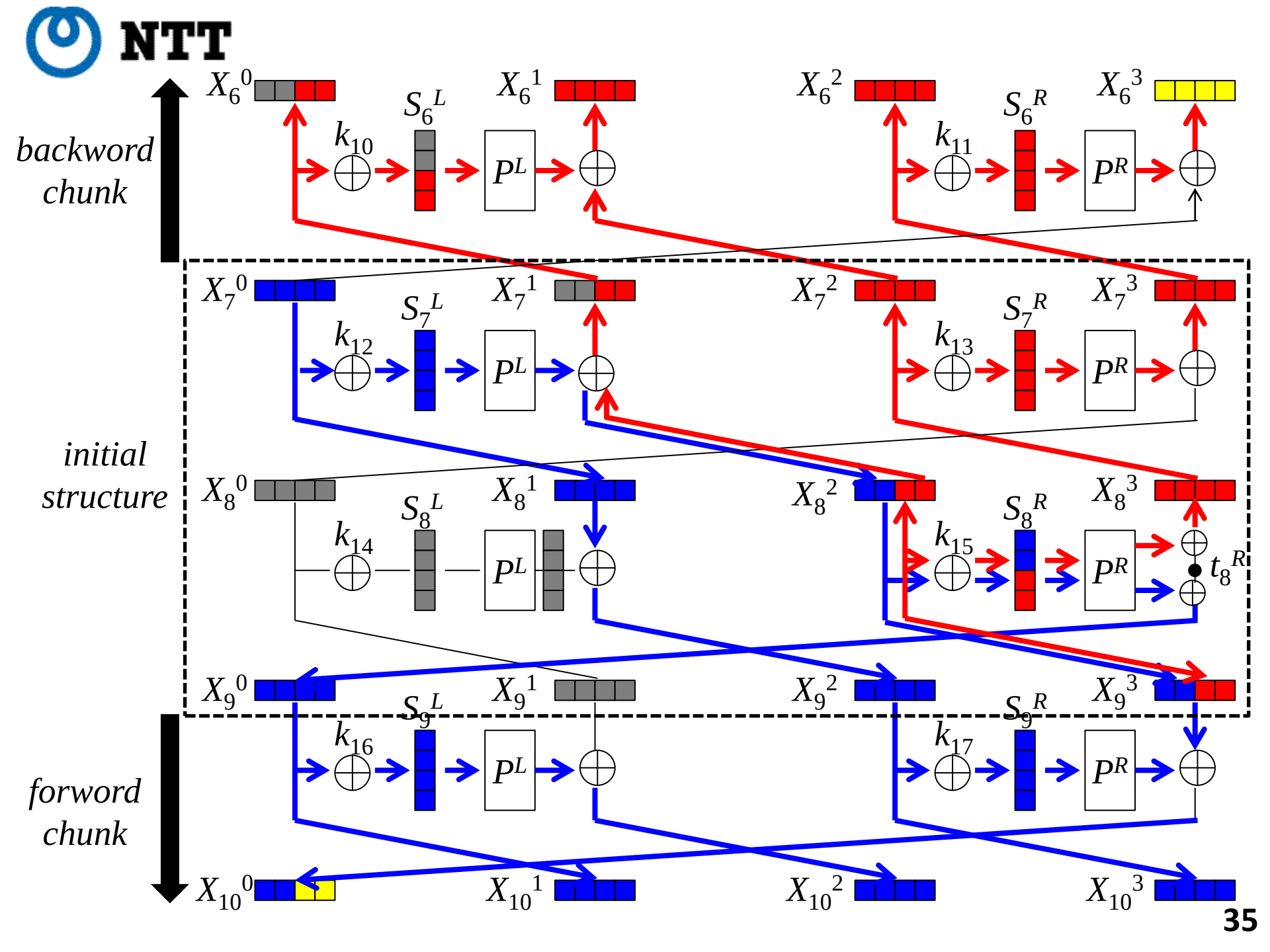
  In total, 11+1+1=13 rounds are attacked.
- Due to the simple key schedule, satisfying *n*-bit relation is possible.
- 1-byte freedom degrees and 2-byte match. The attack is improved by a factor of 2^8.

NTT

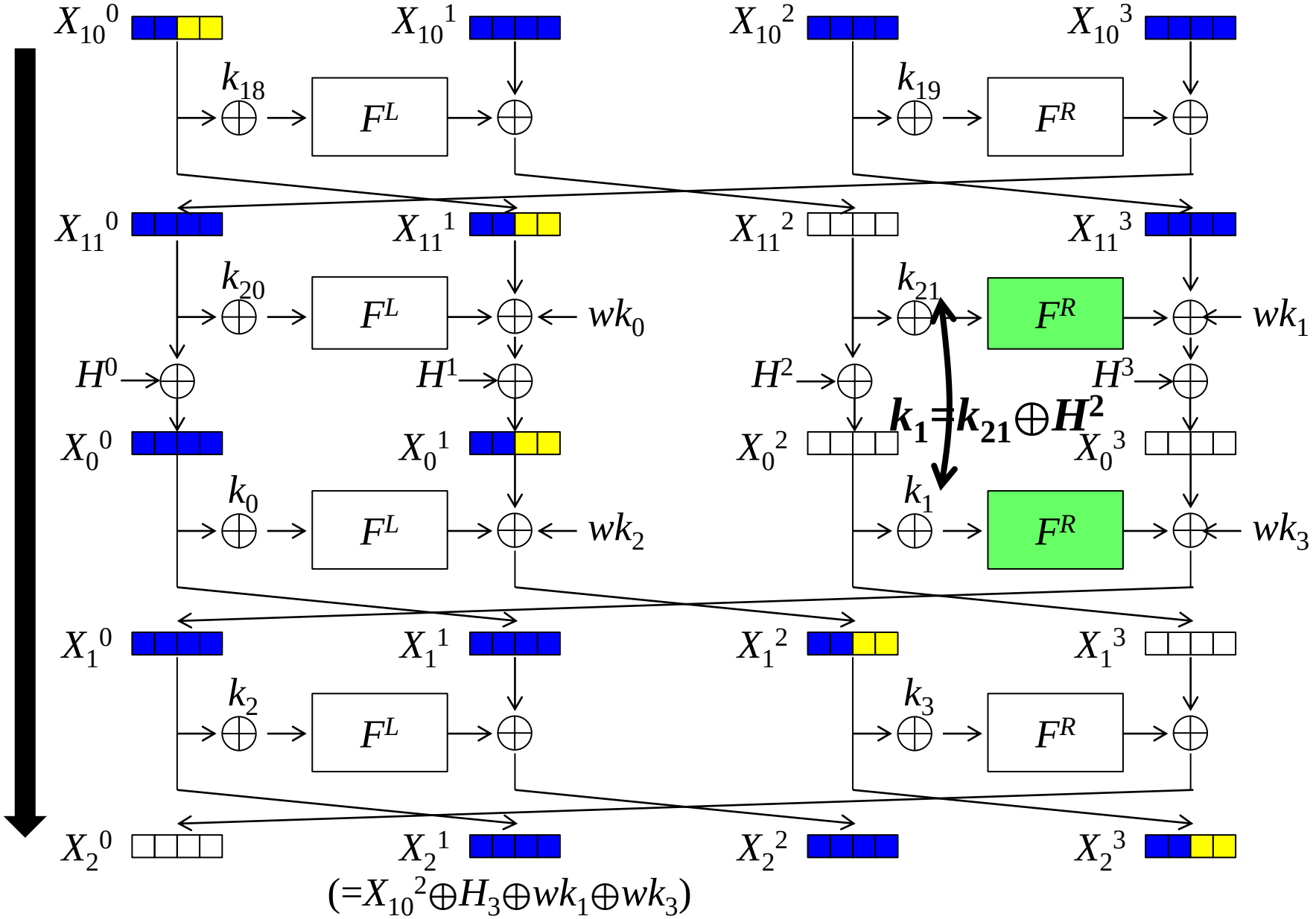
Applications to CLEFIA (with whitening layers)

CLEFIA

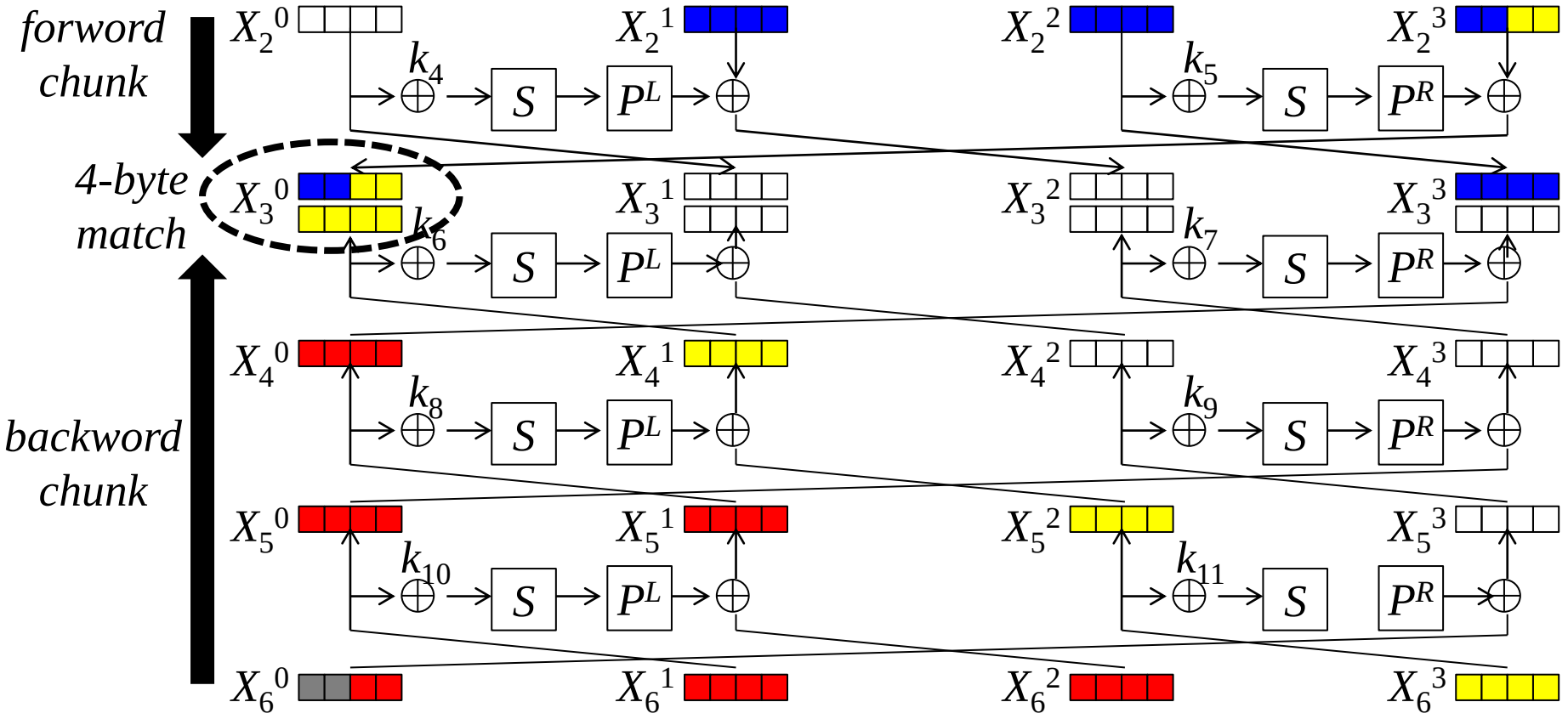
- CLEFIA is a block-cipher designed by SONY and Nagoya University.
- 4-branch type-2 GFN with pre- and post-whitening operations.
- Diffusion switching mechanism → Different MDX matrices in left and right functions.


NTT
backword chunk
initial structure
forword chunk
X_6^0
X_6^1
X_6^2
X_6^3
S_6^L
S_6^R
k_{10}
k_{11}
P^L
P^R
X_7^0
X_7^1
X_7^2
X_7^3
S_7^L
S_7^R
k_{12}
k_{13}
X_8^0
X_8^1
X_8^2
X_8^3
S_8^L
S_8^R
k_{14}
k_{15}
t_8^R
X_9^0
X_9^1
X_9^2
X_9^3
S_9^L
S_9^R
k_{16}
k_{17}
X_{10}^0
X_{10}^1
X_{10}^2
X_{10}^3

Cancelling the impact only once.



- DSM prevents 7-round match.
- If each branch consists of more than 4 bytes, 7-round match is possible.



NTT

Attack Summary

- Due to the DSM:
  - Round shrink becomes inefficient.
  - Matching phase is shortened by 3 rounds.

  In total, 15-3=12 rounds are attacked.
- 2-byte freedom degrees and 4-byte match. The attack is improved by a factor of 2^{16}.
- The whitening operation do not impact to the attack complexity.

NTT

Concluding Remarks

- Omission of the last network twist lowers the security in the hash function setting because the key value is chosen and rounds will shrink.
- Showed preimage attacks on generic structure.
  - 11-round attack for Feistel-SP
  - 15-round attack for 4-branch type-2 GFN
- Showed applications to dedicated designs.
  - 13-round attack for Camellia w/o FL and WH.
  - 12-round attack for CLEFIA.

Thanks for your attention !!