Meet-in-the-Middle Attacks on Generic Feistel Constructions

Jian Guo[1], Jérémy Jean,[1] Ivica Nikolić[1] and Yu Sasaki[2]

1: Nanyang Technological University Singapore
2: NTT Secure Platform Laboratories, Japan

9/December/2014 @ Asiacrypt 2014

Copyright©2014 NTT corp. All Rights Reserved.

Contents

- Block-ciphers with Feistel
- Meet-in-the-Middle Attacks (Collision Attacks)
- Key Recovery Attacks against Feistel-2
- Key Recovery Attacks against Feistel-3
- Concluding Remarks

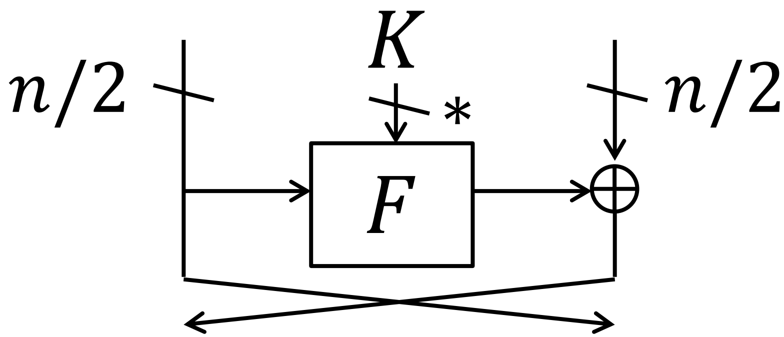
Copyright©2014 NTT corp. All Rights Reserved.

Research Background

Copyright©2014 NTT corp. All Rights Reserved.

Feistel Network

- Build n-bit permutation from $n/2$-bit function

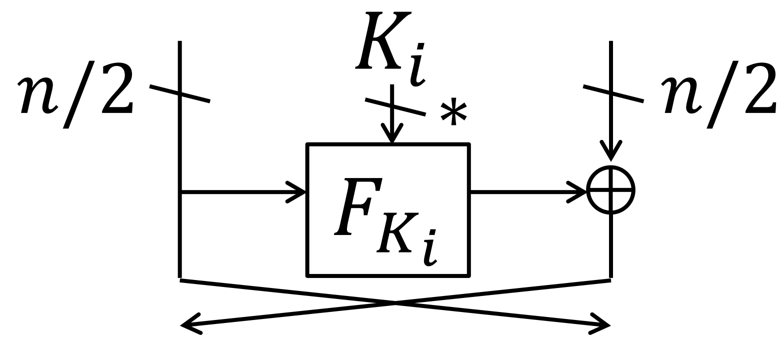


- Advantages
  - Enc and Dec can share the same network
  - function → permutation
  - small component → large permutation
- Useful design choice even now: Simon and LAC

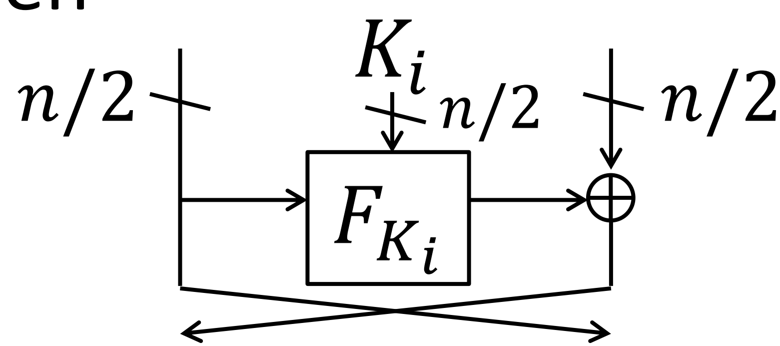
Copyright©2014 NTT corp. All Rights Reserved.

Generic Constructions (1/2)

- Luby-Rackoff
  - regarded as $|K| = \frac{n}{2} \cdot 2^{\frac{n}{2}}$ bits
  - provable security
  - hard to implement



- Feistel-1, analyzed by Knudsen
  - regarded as $|K| = \frac{n}{2}$ bits
  - cryptanalysis makes sense
  - still hard to implement

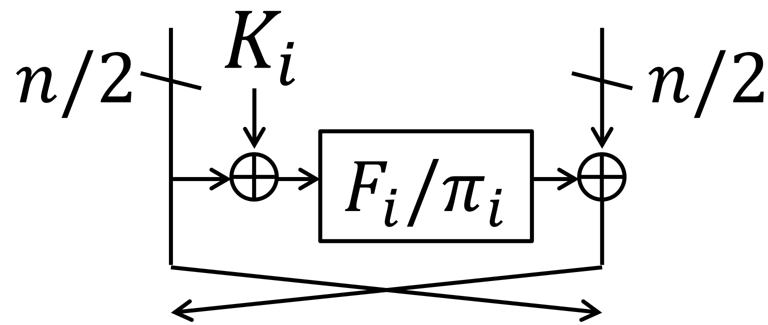


NTT

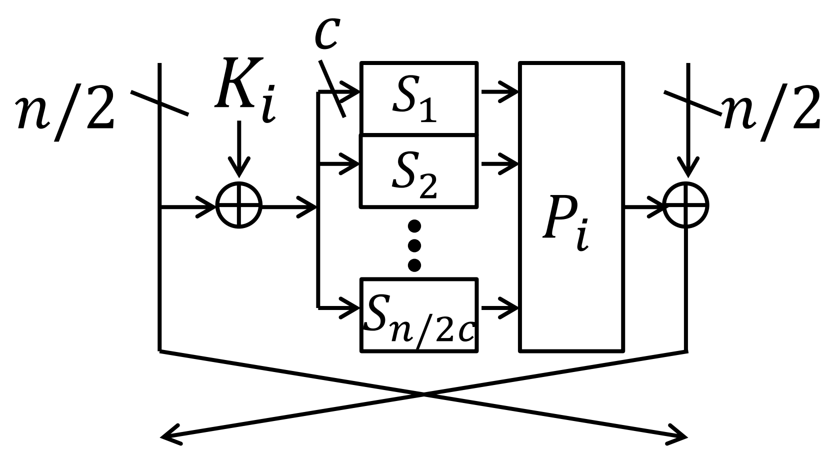
Copyright©2014 NTT corp. All Rights Reserved.

Generic Constructions (2/2)

- Feistel-2
  - still captures many designs
  - F-function can be function or permutation. They may differ in different rounds.



- Feistel-3
  - F-function consists of c-bit S-boxes and a linear map P_i.



(Classification of Feistel-x is from Isobe-Shibutani Asiacrypt2013)

Copyright©2014 NTT corp. All Rights Reserved.

Attack Results on Feistel-2

F-function	#rounds for $\|K\| =$ n	$3n/2$	$2n$	Method	Ref.
any	5	6	7	imp. diff.	[Knu02]
any	5	7	9	MitM(ASR)	[IS13]
bij., ident.	6	–	–	Integ.-like	[Tod13]
any	**6**	**8**	**10**	**MitM**	**Ours**

- No assumption on F, e.g. F can be one-way func.
- For $k = (s+1)n/2$, #rounds is $4s + 2$.
- Complexity is higher than previous work.

Copyright©2014 NTT corp. All Rights Reserved.

Attack Results on Feistel-3

F-function	#rounds for $\lvert K\rvert =$ n	$3n/2$	$2n$	Method	Ref.
any	7	9	11	MitM(ASR)	[IS13]
any	**9**	**11**	**13**	**MitM**	**Ours**
identical	**10**	**12**	**14**	**MitM**	**Ours**

- Attack complexity depends on the S-box size, c.
- Our attacks work for practical choices of c e.g. $n = 128, c = 8$. (128-bit block, 8-bit S-boxes)

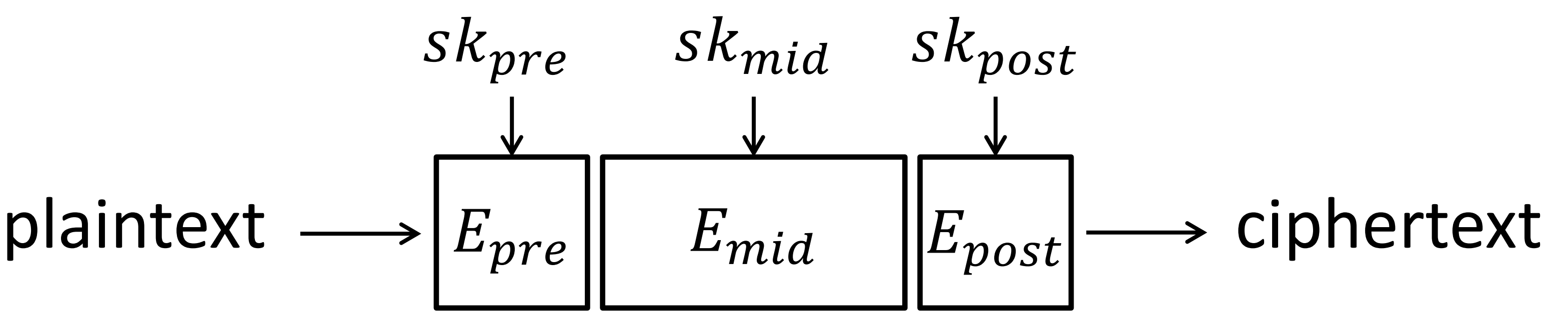
Copyright©2014 NTT corp. All Rights Reserved.

Framework of Meet-in-the-Middle Attacks

Copyright©2014 NTT corp. All Rights Reserved.

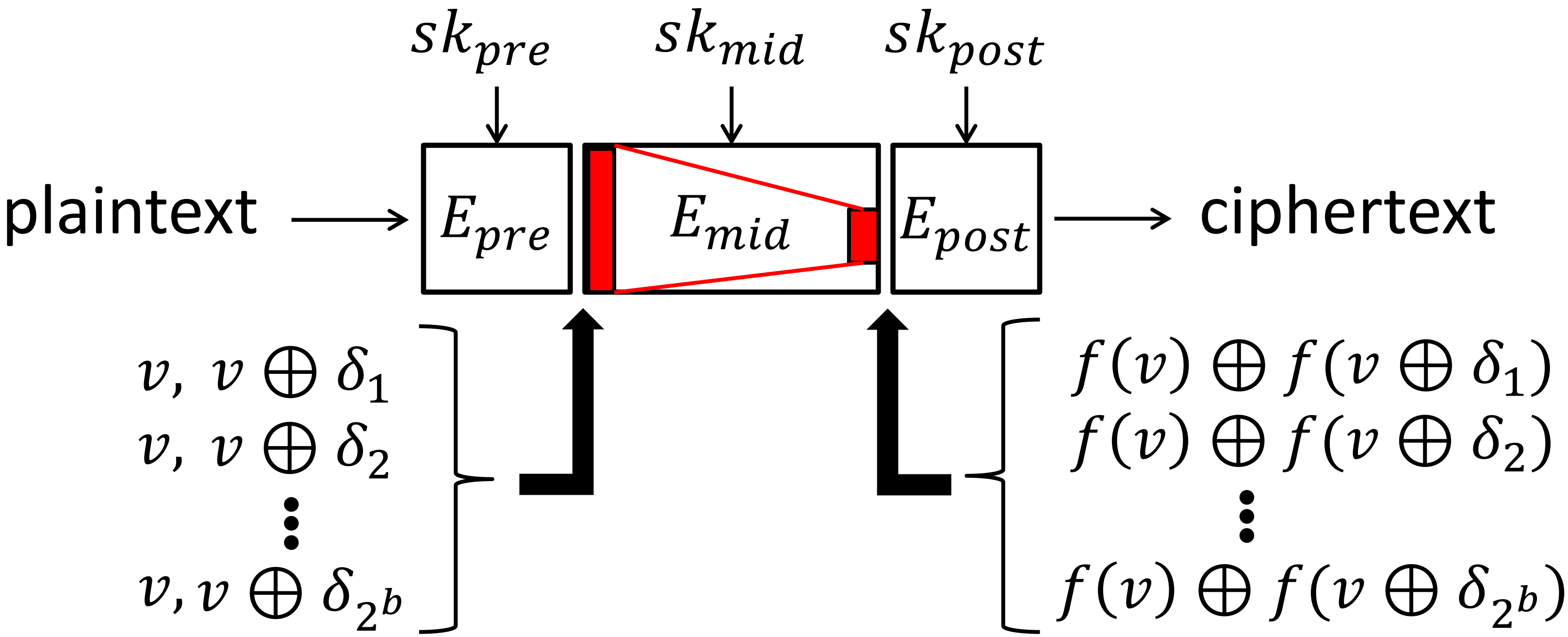
General Framework

- Divide the cipher into three parts.
- [Offline] Construct a distinguisher in E_{mid}, which works for any choice of sk_{mid}.
- [Online] Guess sk_{pre} and sk_{post}. The correct subkey guess leads to an internal state value consistent with the distinguisher.



Copyright©2014 NTT corp. All Rights Reserved.

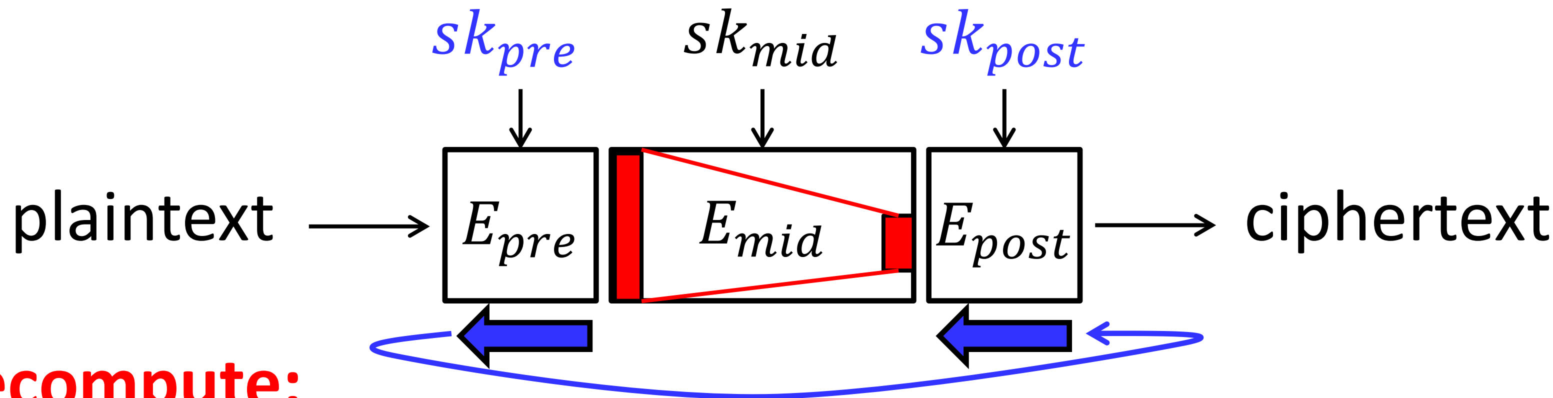
Distinguisher in MitM Attacks



- Determine a set of 2^b differences $\{\delta_1, \delta_2, \cdots, \delta_{2^b}\}$.
- ***b*-*δ*-set**: a set of 2^b paired values $(v, v \oplus \delta_j)$.
- The num of (ordered) set of 2^b partial differences after E_{mid} can be smaller than all the possibilities.

Copyright©2014 NTT corp. All Rights Reserved.

Key Recovery Procedure



Precompute:

Compute possible sets of partial differences from b-δ-set. They are stored in a pre-computation table T_δ.

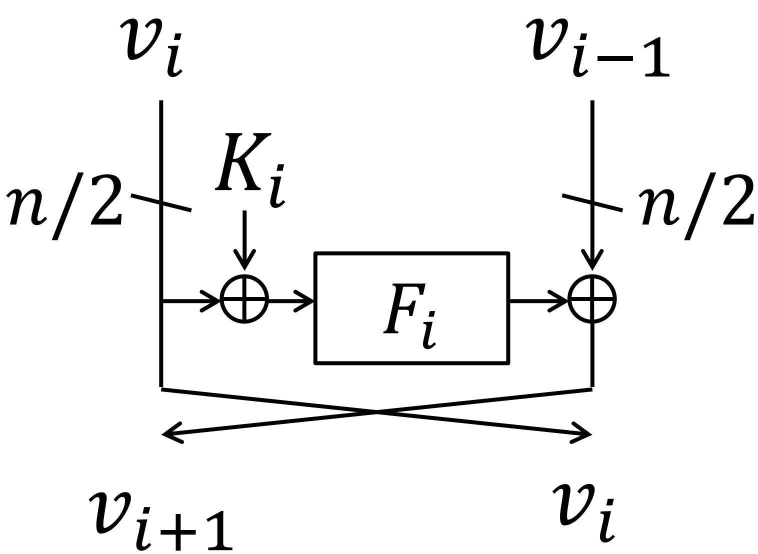
Online:

- Collect (P, P') and (C, C'). Guess sk_{pre} and sk_{post}.
- Build a b-δ-set at the beginning of E_{mid} and obtain P.
- Obtain C and compute the diff at the end of E_{mid}.
- Check if the result matches one of T_δ.

NTT

Copyright©2014 NTT corp. All Rights Reserved.

Key Recovery Attacks against Feistel-2



Copyright©2014 NTT corp. All Rights Reserved.

Approach of Constructing Distinguisher

1. Find a truncated differential characteristic satisfying the following condition:
   - Given a pair of input and output differences, the number of possible internal state values is small.

   Lemma 1

2. For each internal state value, differential propagation from the beginning to the end of E_{mid} is uniquely computed.

   Proposition 1

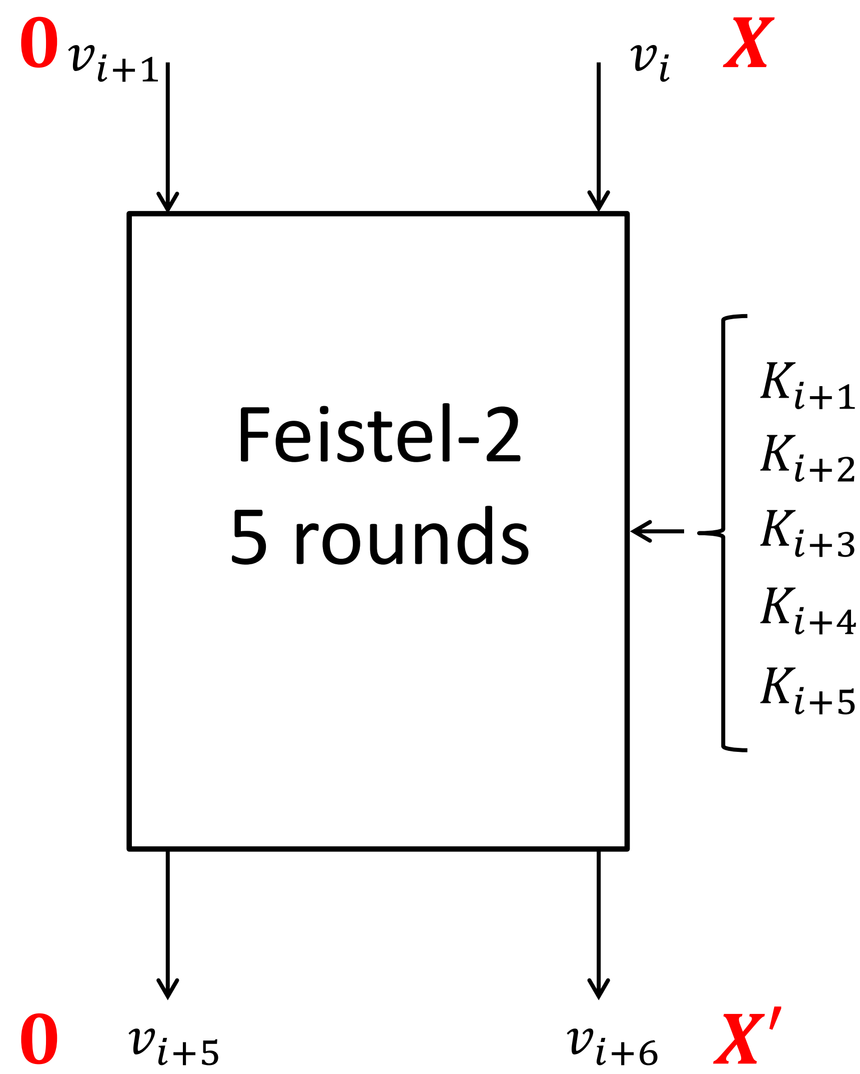
NTT

Copyright©2014 NTT corp. All Rights Reserved.

5-Round Distinguisher (Lemma 1)

Let $\boldsymbol{X}, \boldsymbol{X}'$ be two non-zero differences s.t. $\boldsymbol{X} \neq \boldsymbol{X}'$.

The number of internal state values for the middle 3-rounds satisfying the differential propagation $(\mathbf{0}, \boldsymbol{X}) \rightarrow (\mathbf{0}, \boldsymbol{X}')$ in 5 rounds is only $2^{n/2}$.

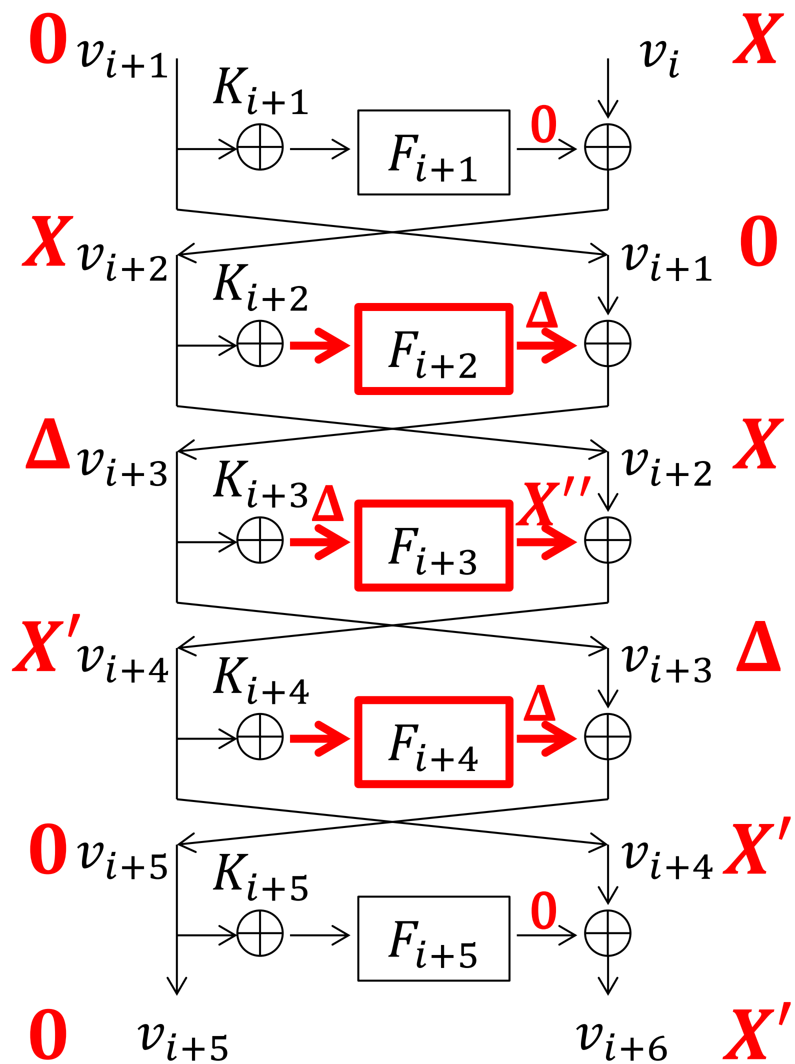


Copyright©2014 NTT corp. All Rights Reserved.

Proof of Lemma 1 (1/2)

Input difference $(\mathbf{0}, \boldsymbol{X})$ and output difference $(\mathbf{0}, \boldsymbol{X}')$ are propagated.

The num of differential characteristics is $2^{n/2}$. $\boldsymbol{X}, \boldsymbol{X}', \boldsymbol{X}''$ are fixed, and if $\boldsymbol{\Delta}$ is fixed, all the differences are fixed.



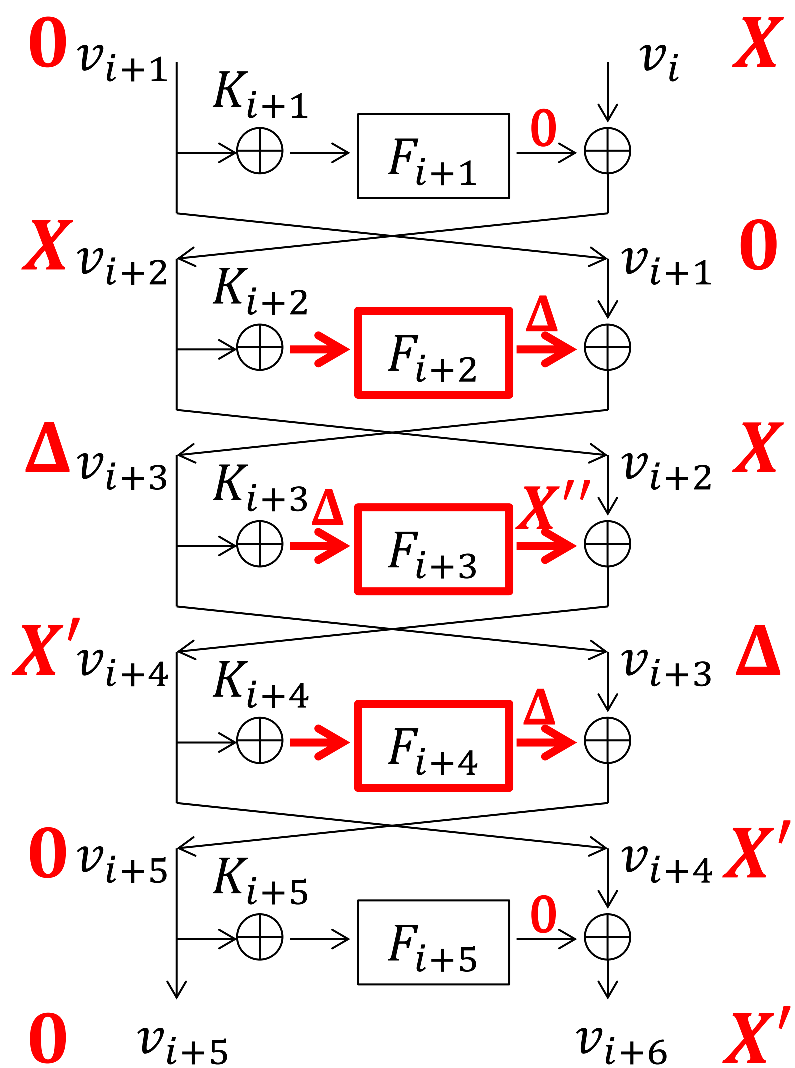
Copyright©2014 NTT corp. All Rights Reserved.

Proof of Lemma 1 (2/2)

For each $\boldsymbol{\Delta}$, input and output differences are fixed for F functions in the 3 middle rounds.

If both of input and output differences are fixed, only 1 state value is obtained on average.

The num of internal state values satisfying the diff propagation is $2^{n/2}$.



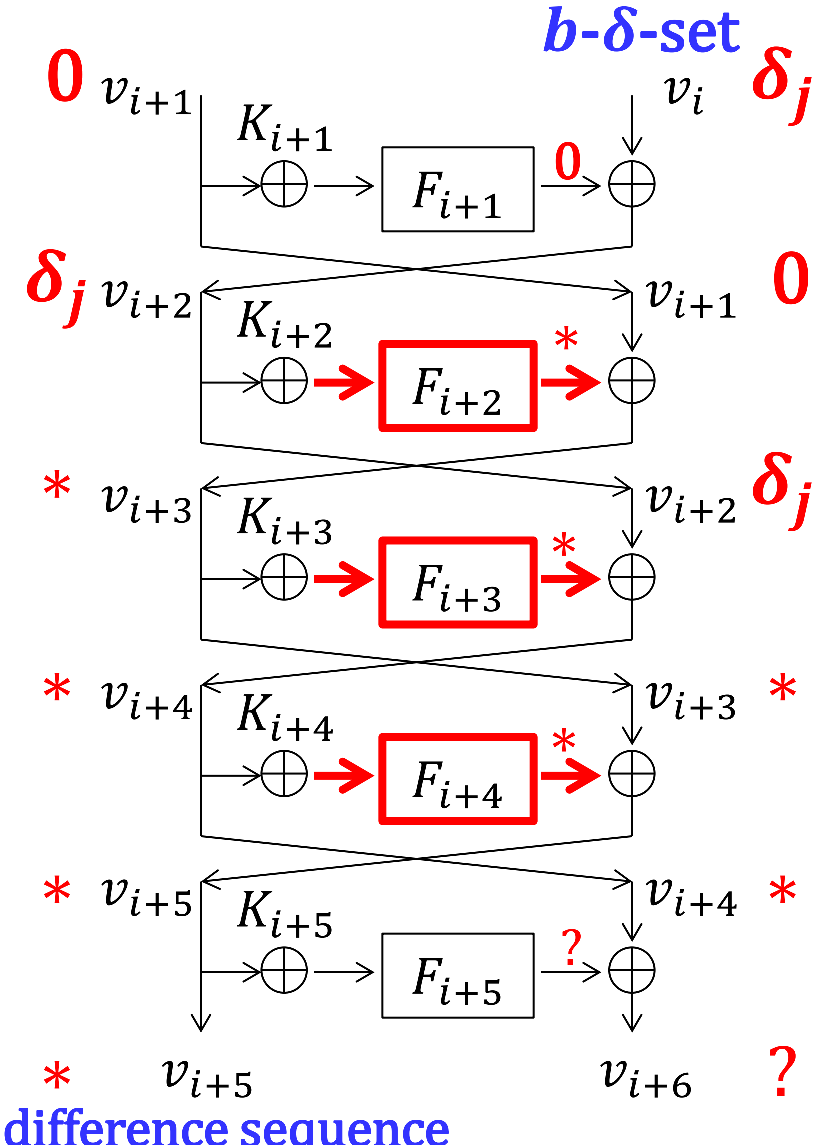
Copyright©2014 NTT corp. All Rights Reserved.

5-Round Distinguisher (Proposition 1)

Set $\mathfrak{D} = (\delta_1, \delta_2, \cdots, \delta_{2^b})$ to ones produced by b LSBs of v_i.

Let $(m, m \oplus \delta), \delta \in \mathfrak{D}$ be a pair of state values satisfying the 5-round diff. propagation.

Make b-δ-set $(m, m \oplus \delta_j)$, and construct a set of Δv_{i+5} for each δ_j. The num of such sets is limited to $2^{n/2}$.



Copyright©2014 NTT corp. All Rights Reserved.

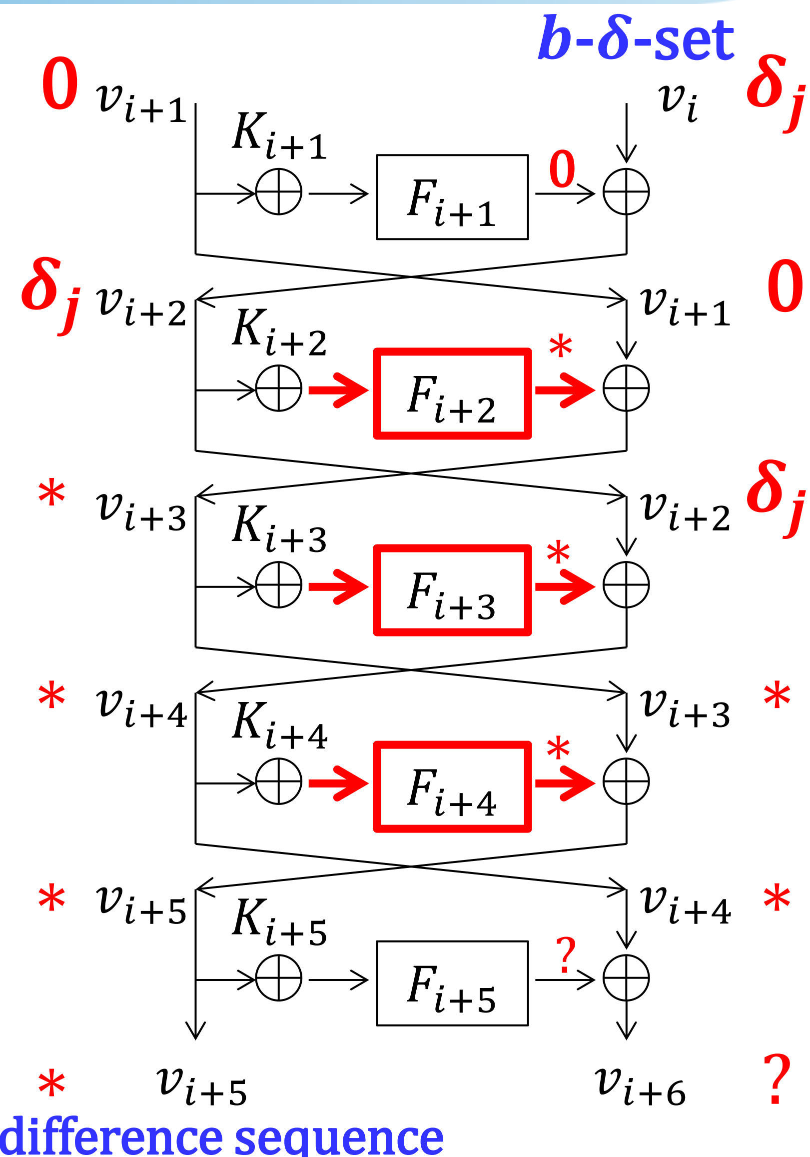
Intuition for Proof of Proposition 1

Approach:

For each of $2^{n/2}$ internal state values, any $\boldsymbol{\delta_j}$ at Δv_i can be mapped to Δv_{i+5} without the value of v_i, v_{i+1}, and subkeys.

Intuition:

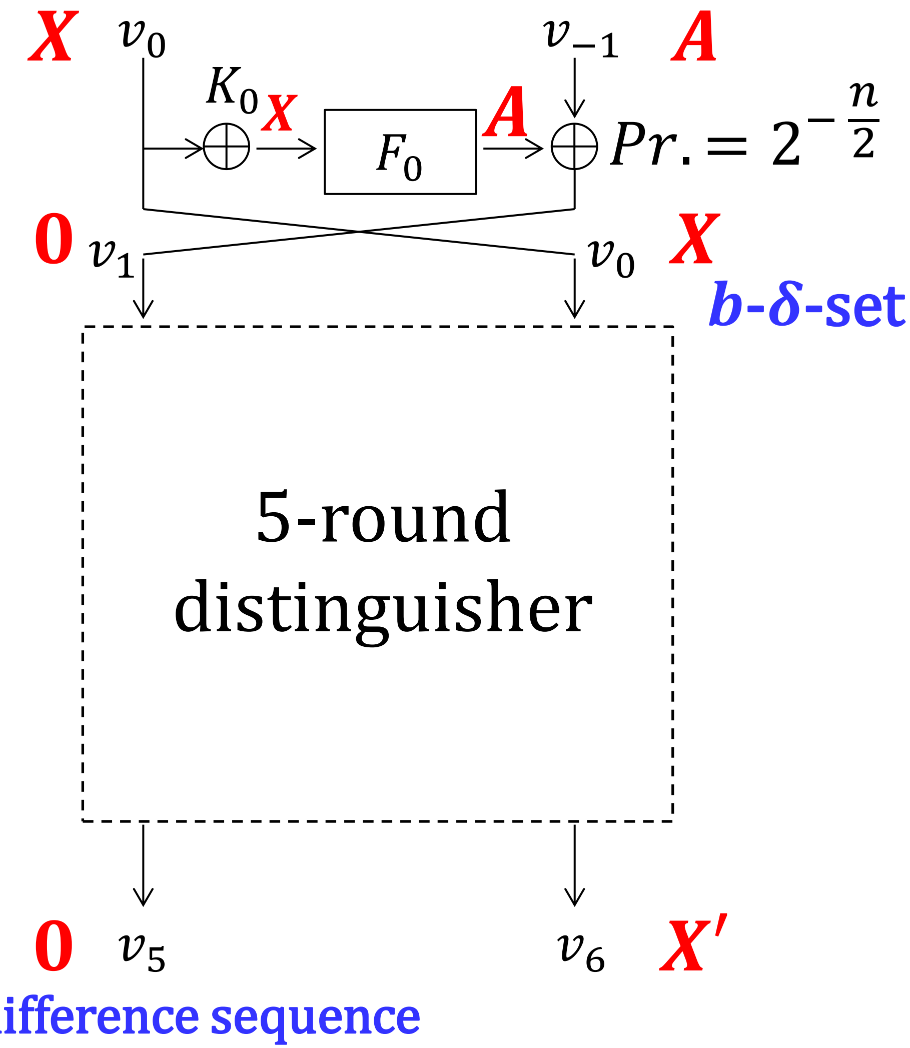
For each round, the state value and new input diff can yield new output diff. Then, Δv_{i+5} is computed.



Copyright©2014 NTT corp. All Rights Reserved.

Key Recovery for $|K| = n$

- 1 round is added before the 5R distinguisher.
- The attacker's first goal is recovering K_0.



NTT

Copyright©2014 NTT corp. All Rights Reserved.

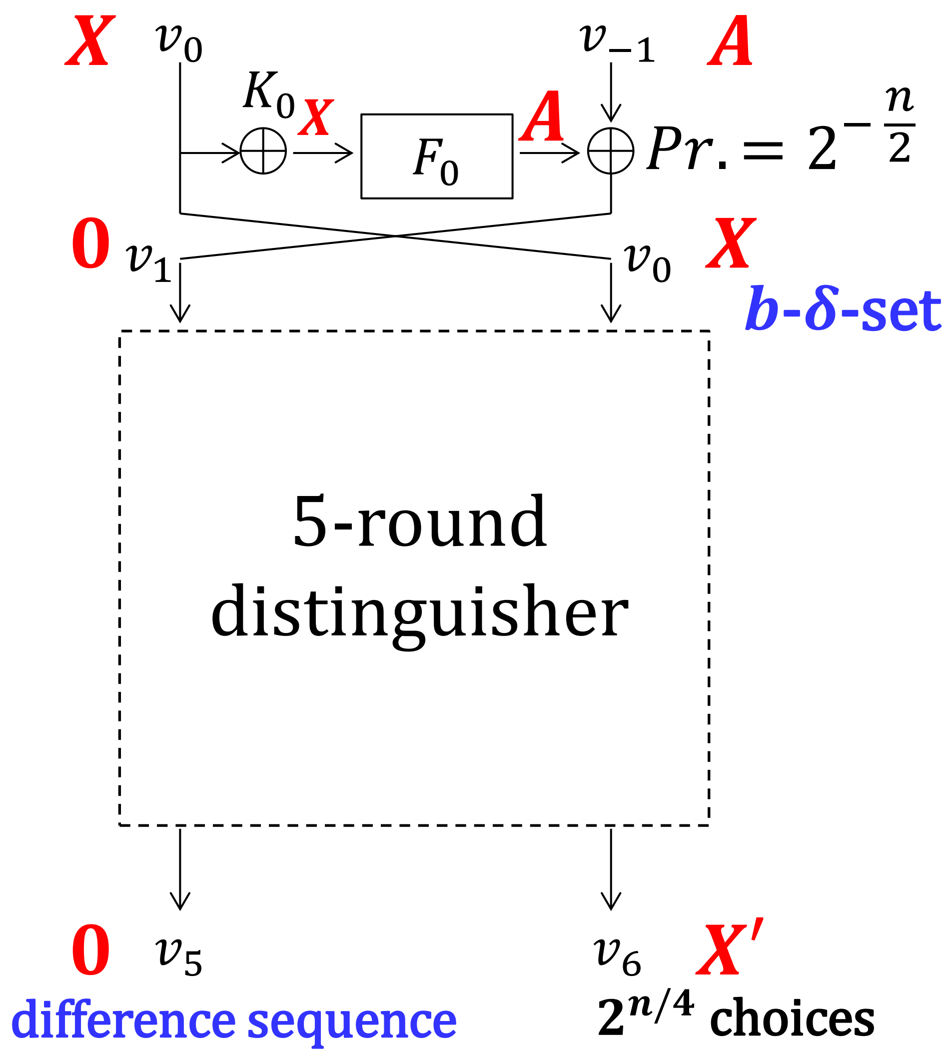
Precomputation Phase

Fix $(\boldsymbol{X}, \boldsymbol{X}')$ and compute $2^{n/2}$ possible difference sequences of Δv_{i+5}. Store the result in T_δ.

Complexity: $2^{n/2}$

Repeat the above by changing $\boldsymbol{X}'$ $2^{n/4}$ times. (change $n/4$ LSBs of $\boldsymbol{X}'$)

Complexity: $2^{3n/4}$

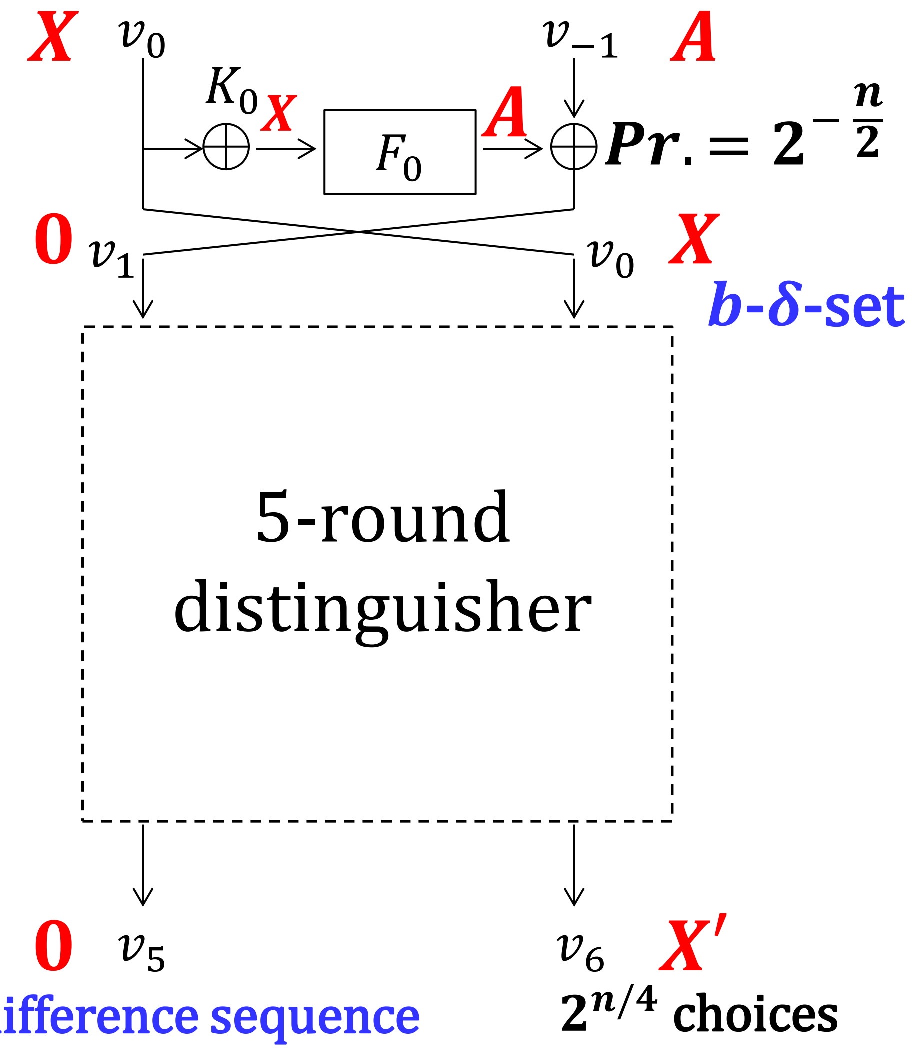


Copyright©2014 NTT corp. All Rights Reserved.

Online Phase (Collecting Pairs) 1/2

- Fix v_0.
- For all $2^{n/2}$ choices of v^{-1}, query $(v_0,*)$ and $(v_0 \oplus X,*)$. 2^n pairs are generated.
- Pick up pairs satisfying $2^{n/4}$ choices of $(0, X')$. $2^{n/4}$ pairs will be obtained.
- Iterate the above $2^{n/4}$ times by changing the value of v_0. $2^{n/2}$ pairs are expected.

Data Complexity: $2^{3n/4}$

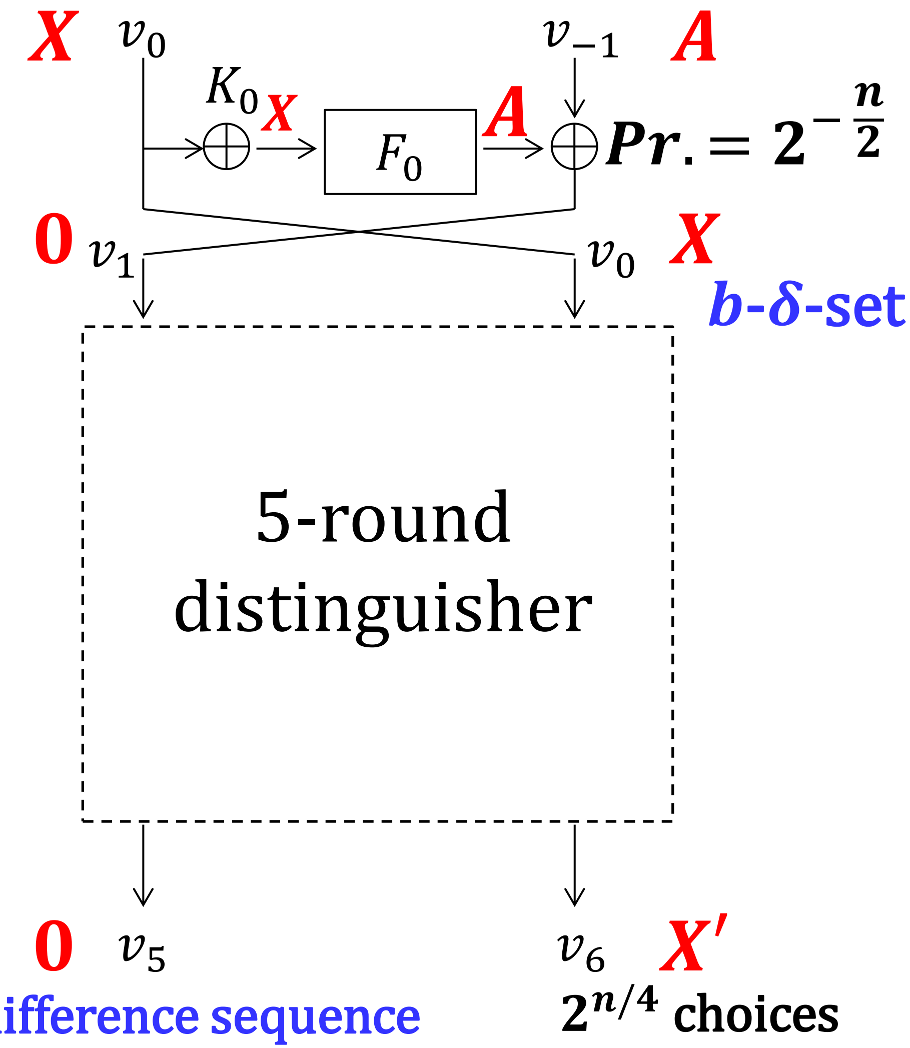


NTT
Copyright©2014 NTT corp. All Rights Reserved.

Online Phase (Collecting Pairs) 2/2

- Fix v_0.
- For all $2^{n/2}$ choices of v^{-1}, query $(v_0,*)$ and $(v_0 \oplus X,*)$. 2^n pairs are generated.
- Pick up pairs satisfying $2^{n/4}$ choices of $(0, X')$. $2^{n/4}$ pairs will be obtained.
- Iterate the above $2^{n/4}$ times by changing the value of v_0. $2^{n/2}$ pairs are expected.

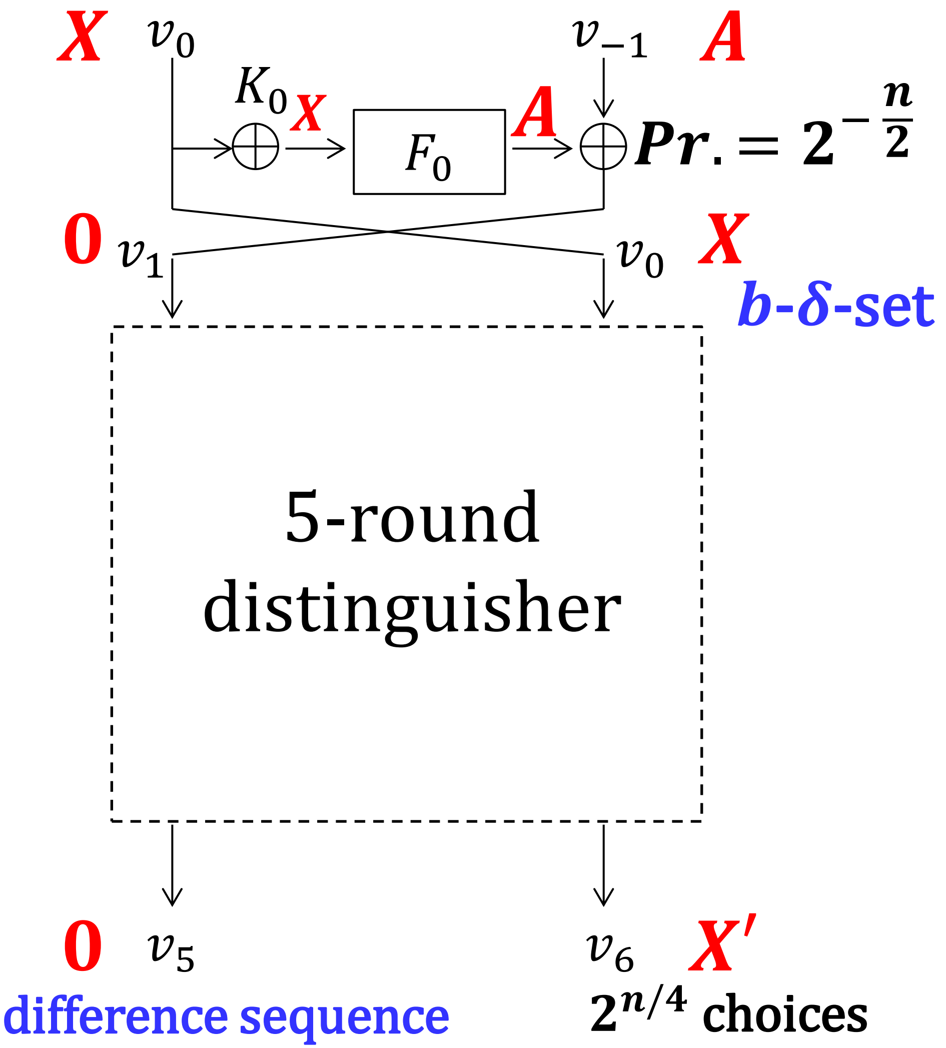
Data Complexity: $2^{3n/4}$



Copyright©2014 NTT corp. All Rights Reserved.

Online Phase (Recovery of K_0)

- For each of $2^{n/2}$ pairs, obtain 1 solution of F_0 that maps X to A. This leads to K_0.
- Make a b-δ-set at v_0, and compute the corresponding v_{-1} with the recovered K_0.
- Check the sequence of Δv_5 of the ciphertexts, and check the match with pre-computed T_δ.



Copyright©2014 NTT corp. All Rights Reserved.

Evaluation of Attacks

- $2^{3n/4}$ difference sequences are stored in T_δ offline.
- $2^{n/2}$ difference sequences are computed online.
- In total, $2^{5n/4}$ matching candidates. Each match succeeds with $\Pr. = 2^b \cdot 2^{-n/2}$.
- With $b = 2$, the right key is obtained.

- Offline: (Data, Time, Mem.) = $(0, 2^{3n/4}, 2^{3n/4})$
- Online: (Data, Time, Mem.) = $(2^{3n/4}, 2^{3n/4}, 2^{3n/2})$

Copyright©2014 NTT corp. All Rights Reserved.

More Discussion on Feistel-2

- Once K_0 is recovered, recovering all the other subkeys is quite easy.
- Generalization in terms of $|K|$

$\|K\|$	#rounds for dist.	#rounds for key recov.
n	5	1
$s(n/2)$	$s+3$	$s-1$

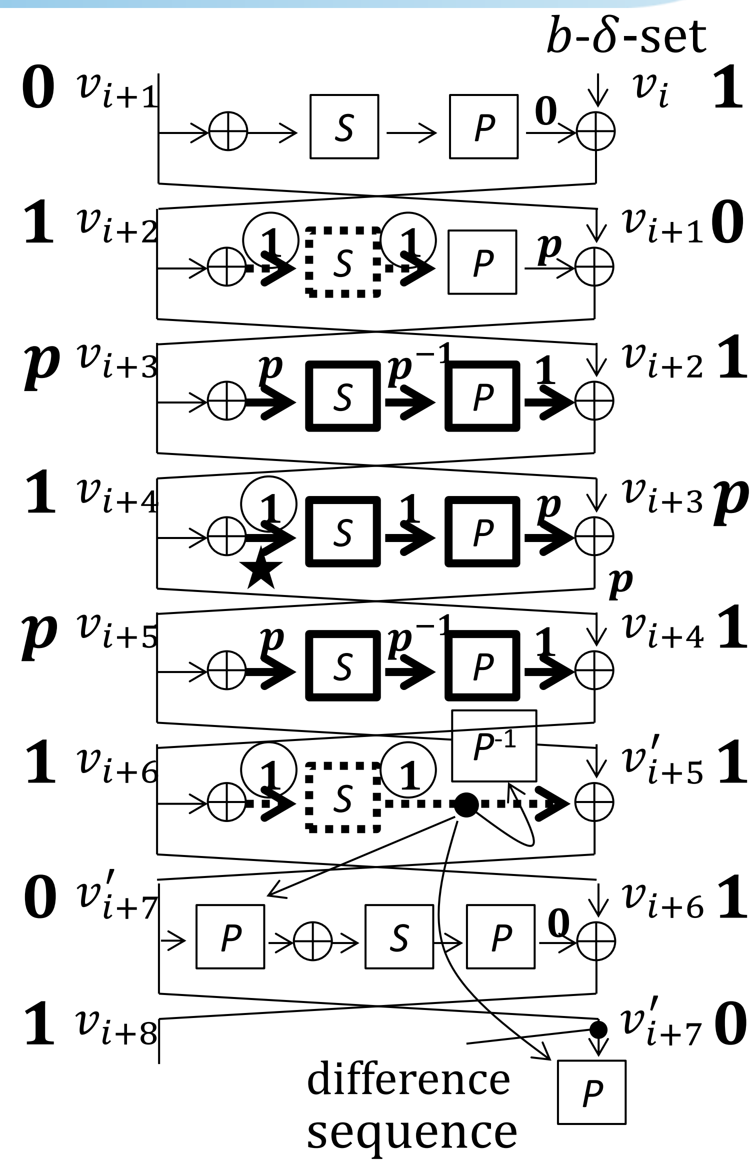
- Optimization with time-memory tradeoff

  Similarly to the prev work on AES, trunc diff chara is relaxed. Data decreases, but Time, Mem increase.

Copyright©2014 NTT corp. All Rights Reserved.

Summary of MitM Attacks on Feistel-3

- Sophisticated trunc. diff. chara with rebound attack.
- If P is identical in particular 2 rounds, the attack can be improved by applying equivalent transformation.
- Attack complexity depends on the ratio of the block size n and the S-box size c.



Copyright©2014 NTT corp. All Rights Reserved.

Concluding Remarks

We improved generic attacks on Feistel with the MitM attack.

	F-function	#rounds for $\lvert K \rvert =$ n	$3n/2$	$2n$	Method	Ref.
Feistel-2	any	5	6	7	imp. diff.	[Knu02]
	any	5	7	9	MitM(ASR)	[IS13]
	bij., ident.	6	–	–	Integ.-like	[Tod13]
	any	**6**	**8**	**10**	**MitM**	**Ours**
Feistel-3	any	7	9	11	MitM(ASR)	[IS13]
	any	**9**	**11**	**13**	**MitM**	**Ours**
	identical	**10**	**12**	**14**	**MitM**	**Ours**

Future work: application to concrete designs
application to other variants of Feistel

Copyright©2014 NTT corp. All Rights Reserved.

Thank you for your attention !!

Copyright©2014 NTT corp. All Rights Reserved.