Improving the Generalized Feistel

Tomoyasu Suzaki and Kazuhiko Minematsu
NEC Corporation

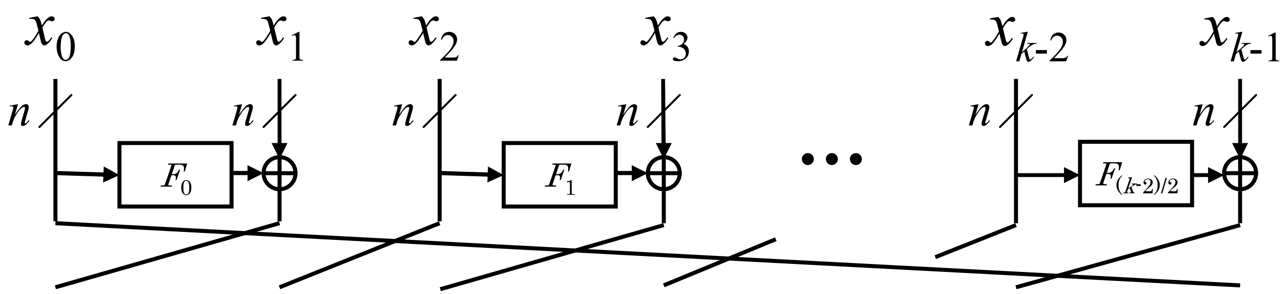
FSE 2010 Feb. 7-10, Seoul Korea

Generalized Feistel Structure (GFS)

- One of the basic structure of block cipher.
- Proposed by Zheng et al. in 1989 (CRYPTO ‘89)*.
- GFS is a generalized form of the classical Feistel structure.
  - Classical Feistel structure
    divide a message into two sub blocks.
  - GFS
    divide a message into k sub blocks ($k > 2$).

* Zheng et al. refers as a Feistel-Type Transformation (FTT).

Type-II GFS



Single round GFS :

$(x_0, x_1, ..., x_{k\text{-}2}, x_{k\text{-}1}) \rightarrow (F_0(x_0) \oplus x_1, x_2, F_1(x_2) \oplus x_3, x_4, ..., F_{(k\text{-}2)/2}(x_{k\text{-}2}) \oplus x_{k\text{-}1}, x_0)$

where $F : \{0,1\}^n \rightarrow \{0,1\}^n$

Employed by many ciphers, such as CLEFIA (k=4), HIGHT (k= 8).

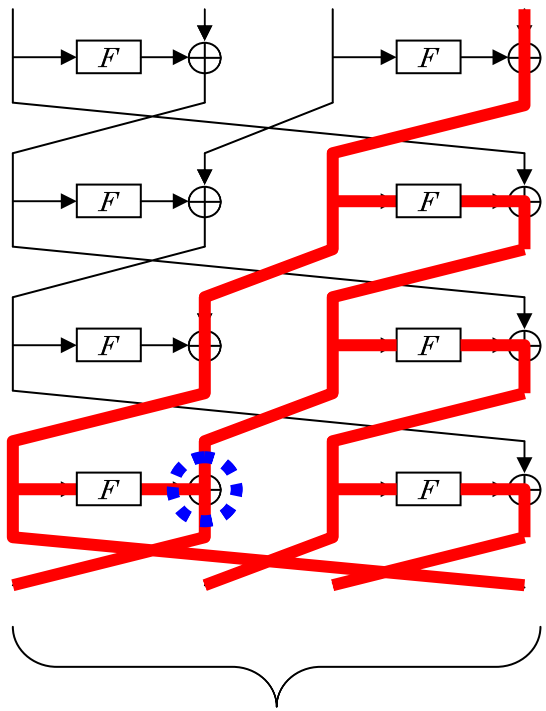
Advantage/Disadvantage of GFS

- Advantage
  For a fixed message length, input/output length of round function gets shorter as the partition number k grows.
  $\rightarrow$ suitable for small-scale implementations.

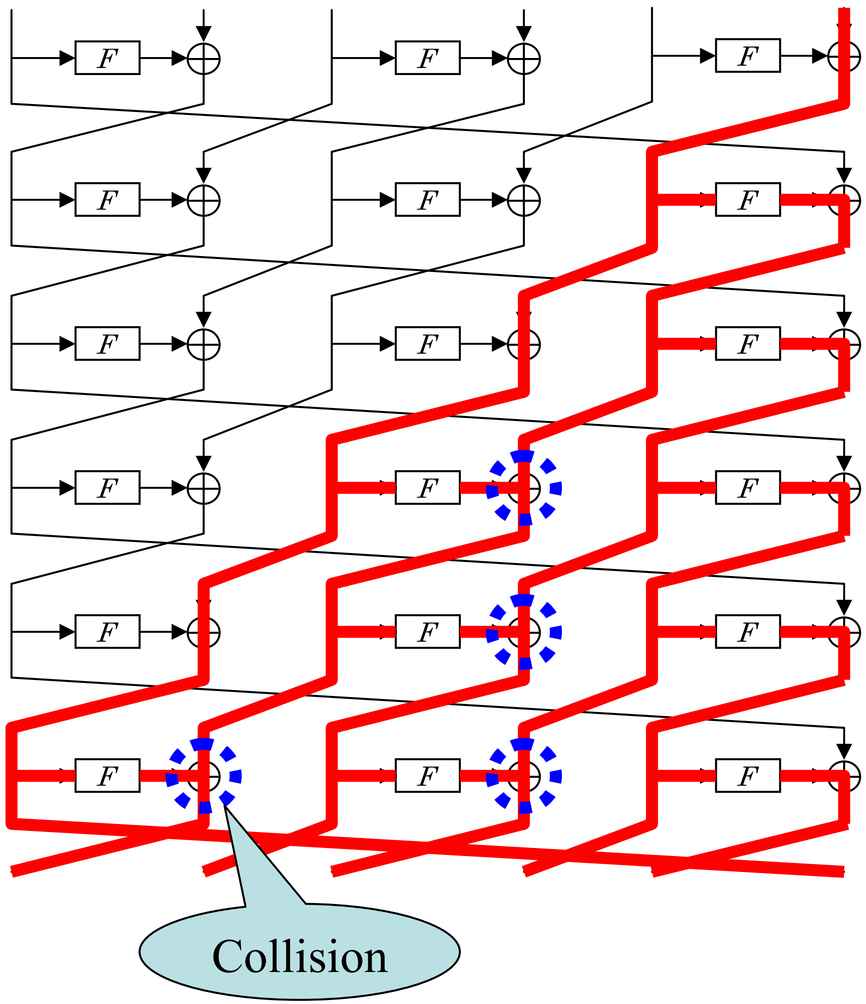
- Disadvantage
  As k grows, the diffusion property gets worse.

(We will explain this in the next slides)

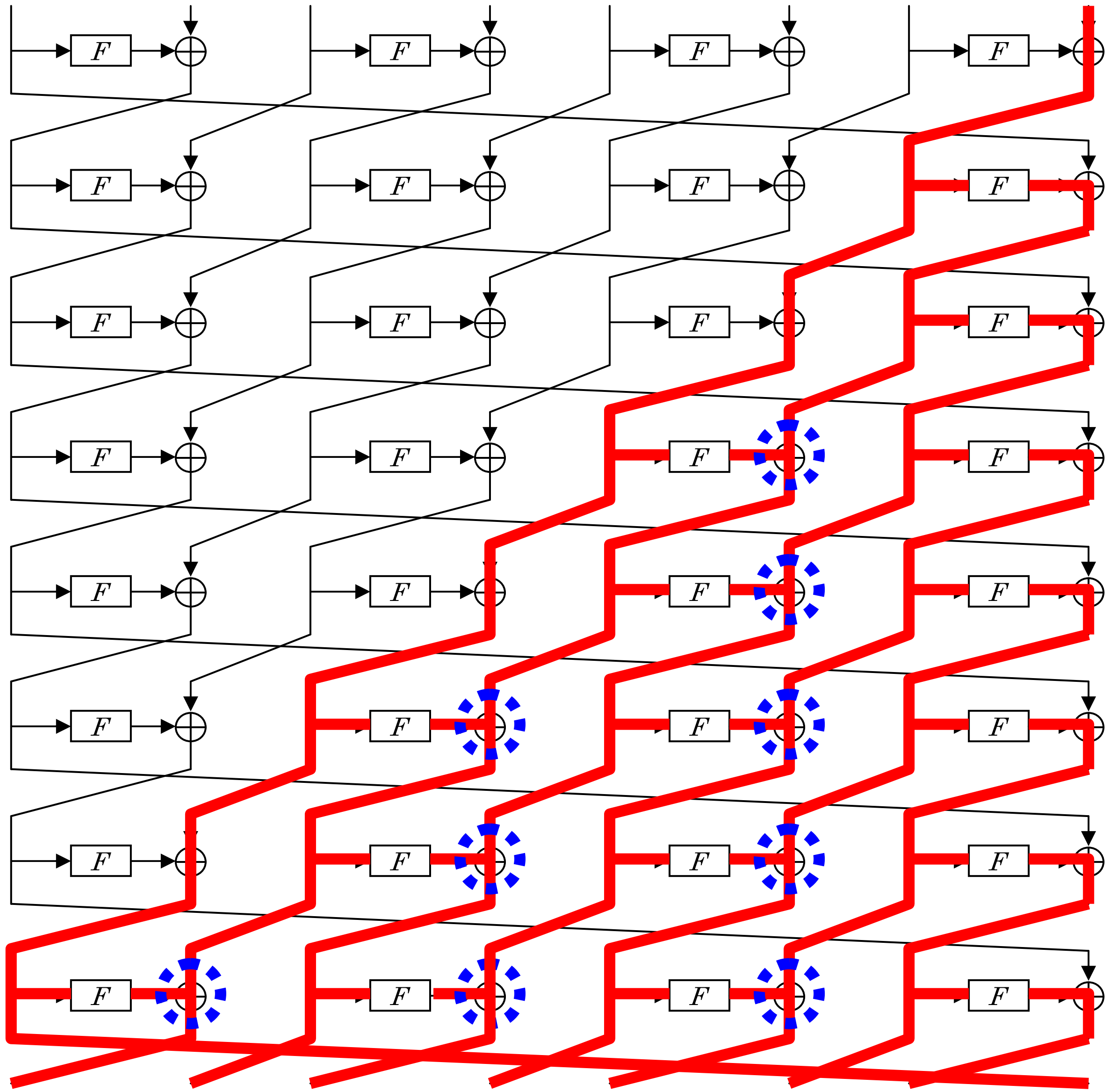
Diffusion path of Type-II GFS (k=4,6)



Full diffusion



Diffusion path of Type-II GFS (k=8)



Collision of data paths for *k* partition Type-II GFS

Partition number *k*	Number of collision	Proportion(%)
2	0	0
4	1	12.5
6	4	22.2
8	9	28.1
10	16	32.0
12	25	34.7
14	36	36.7
16	49	38.2

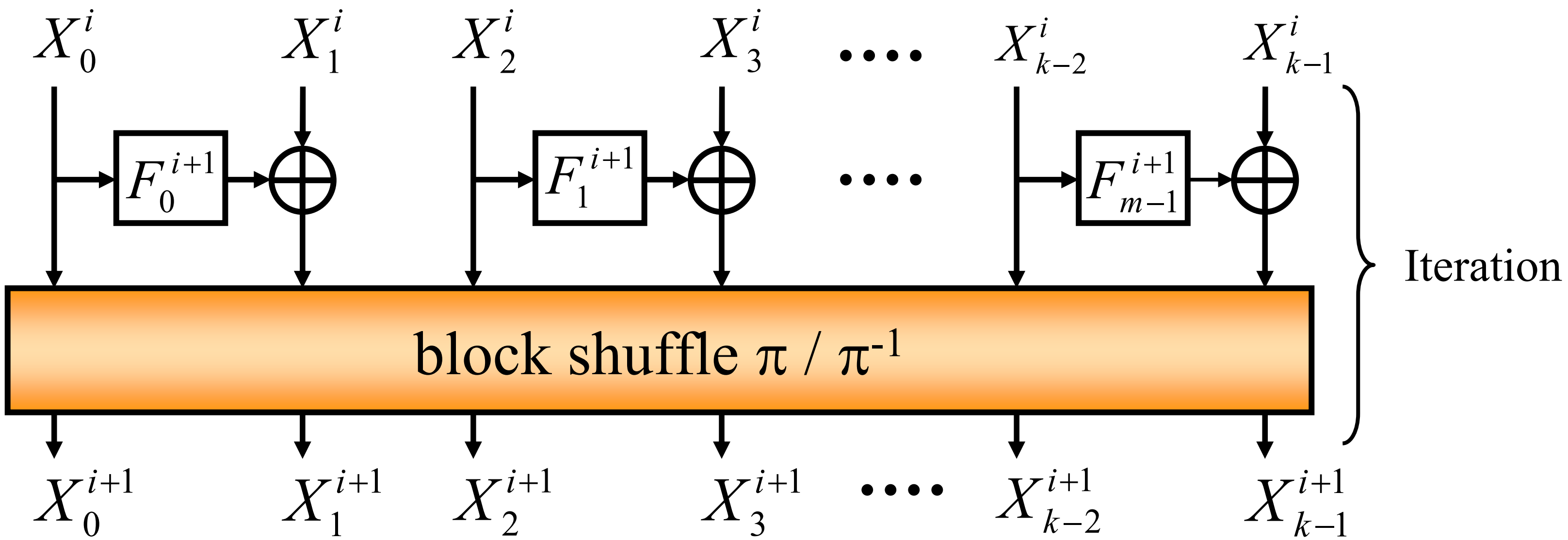
$$\text{Proportion} = \frac{\text{Number of Collisions}}{\text{Number of XORs for full diffusion}} \times 100$$

Improvement possible ?

Contribution

- Propose “generalized” GFS (GGFS)
  - GGFS allowing arbitrary network (but identical for each round)
  - Propose criteria for the diffusion property
  - Confirm the relationship between our criteria and several known security measures
    - Pseudorandomness
    - impossible differential characteristics
    - saturation characteristics
- Build GGFSs with “good” diffusion
  - Exhaustive search
  - Graph-based

Generalized GFS



$y = \pi(x) \leftrightarrow x = \pi^{-1}(y)$

Our goal is to find “good” block shuffle !

Criteria for the diffusion property

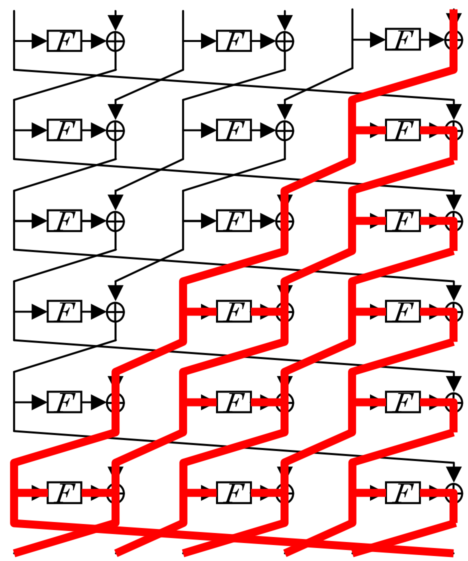
$DR_i(\pi)$: Minimum rounds which *i*-th input block reaches all output blocks.
Using $DR_i(\pi)$ we define the following criteria.

$$\mathrm{DRmax}(\pi) \overset{\mathrm{def}}{=} \max_{0 \le i \le k-1} \mathrm{DR}_i(\pi).$$

$$\mathrm{DRmax}^{\pm}(\pi) \overset{\mathrm{def}}{=} \max\{\mathrm{DRmax}(\pi), \mathrm{DRmax}(\pi^{-1})\}.$$

$$\mathrm{DRmax}_k^{*} \overset{\mathrm{def}}{=} \min_{\pi \in \Pi_k}\{\mathrm{DRmax}^{\pm}(\pi)\}.$$

Optimum π is one that achieves $\mathrm{DRmax}_k{}^*$



DR_6(cyclic shift) = 6

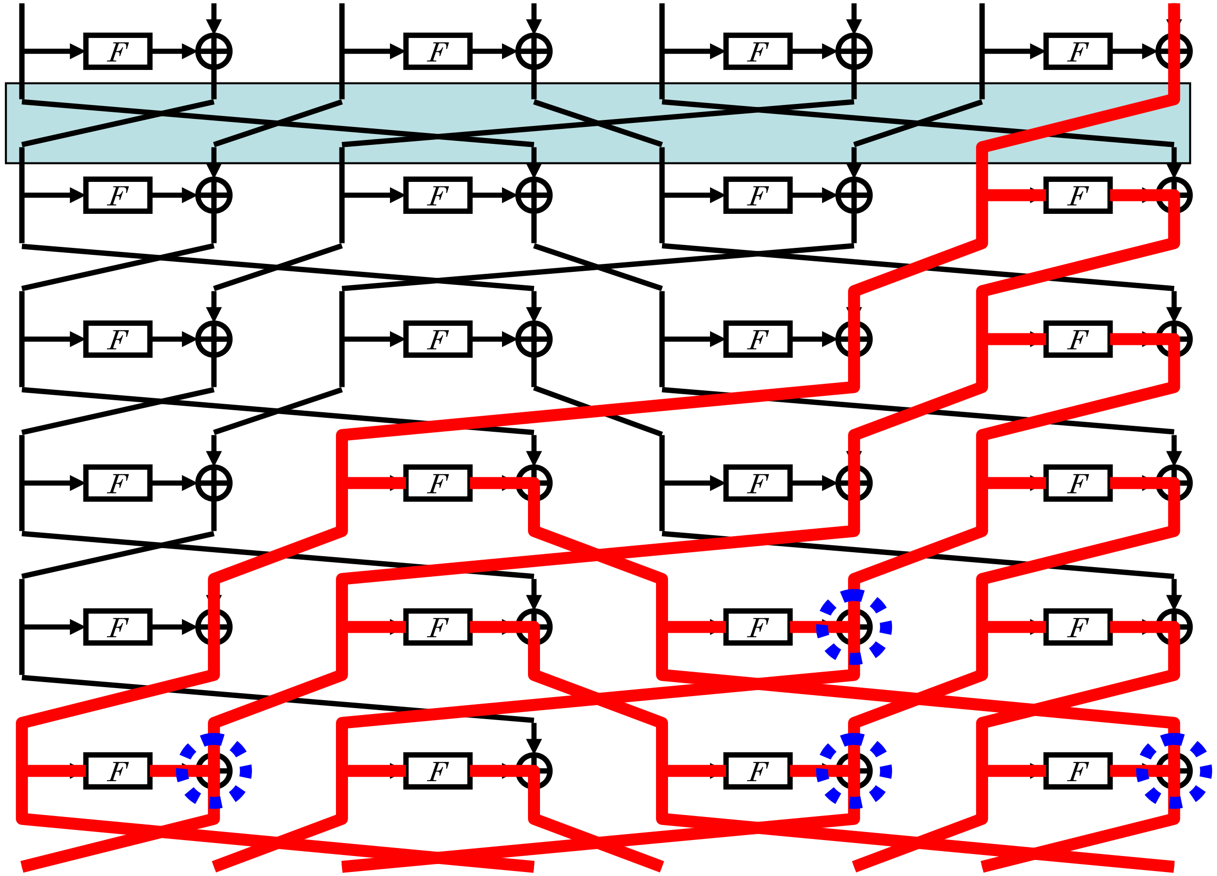
DRmax for practical *k*

We evaluated DRmax of all block shuffles for *k* up to 16.

Partition number *k*	Type-II / Nyberg [1]	$DRmax^*_k$
4	4	4
6	6	5
8	8	6
10	10	7
12	12	8
14	14	8
16	16	8

[1] Nyberg's Generalized Feistel Network

Optimum block shuffle for k=8



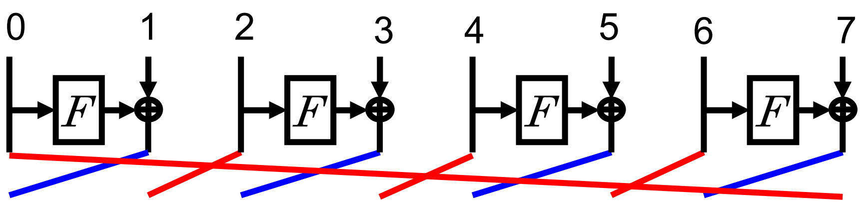
Any even (odd) input block is connected to an odd (even) output block.
We define such shuffle "even-odd shuffle".
Optimum shuffles we found are all even-odd shuffle.

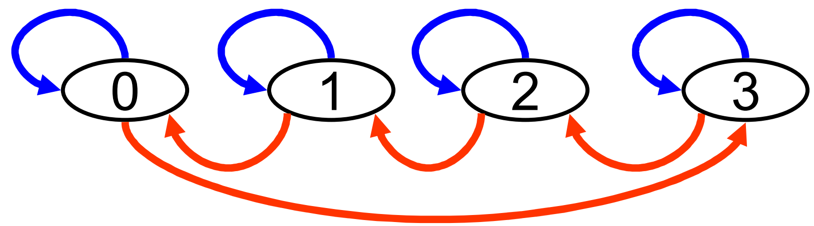
Graphical interpretation

- As *k* grows, the cost of exhaustive search is expensive, therefore we have to take a different approach.
- From the previous search result, we focus on even-odd shuffles.
- We represent an even-odd shuffle as a graph and translate DRmax evaluation into a graph theoretic problem.

Graphical representation

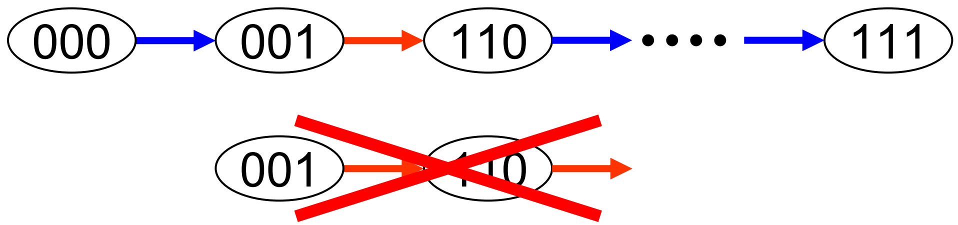
GFS with even-odd shuffle π	Corresponding graph $G[\pi]$
k sub blocks (k : even)	Edge-colored directed graph with $k/2$ nodes (degree 2)
$2i^{th}$ block $\rightarrow$ $2j+1^{th}$ block	$v_i \longrightarrow v_j$
$2i+1^{th}$ block $\rightarrow$ $2j^{th}$ block	$v_i \longrightarrow v_j$
DRmax(π)	Sufficient distance ($SD(G[\pi])$) $\rightarrow$ Next slide





Sufficient Distance (*SD*)

- appropriate path :
  First and last are blue.
  The next of red is blue.



- *L*-appropriately-reachable :
  Any two (possibly the same) nodes are connected via an appropriate path of length *L*.

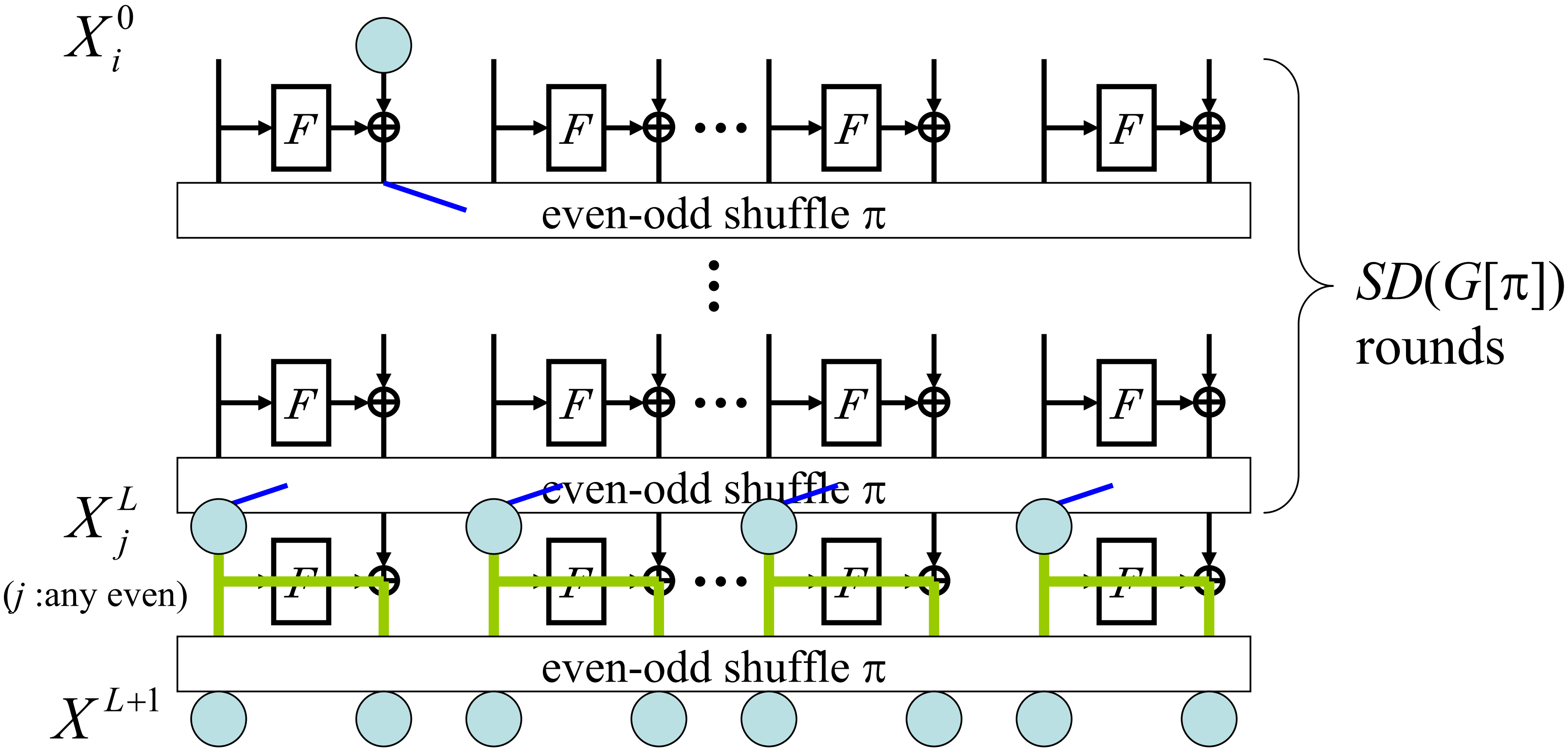
- Sufficient distance (*SD*) :
  Minimum of *L* such that the graph is *L*-appropriately-reachable.

Diam(G) ≤ SD(G)
where Diam(G) is the diameter of G.
i.e., the maximum distance of any two vertices.

Relation between DRmax and *SD*

If $SD(G[\pi])=L$ for even-odd shuffle π,

$\mathrm{DRmax}(\pi) \leq SD(\mathrm{G}[\pi])+1$.



de Bruijn Graph

To build a graph having small *SD* $\rightarrow$ de Bruijn graph

- Property of de Bruijn graph :
  - order 2^s
  - two-regular
  - directed
  - minimum diameter (s)

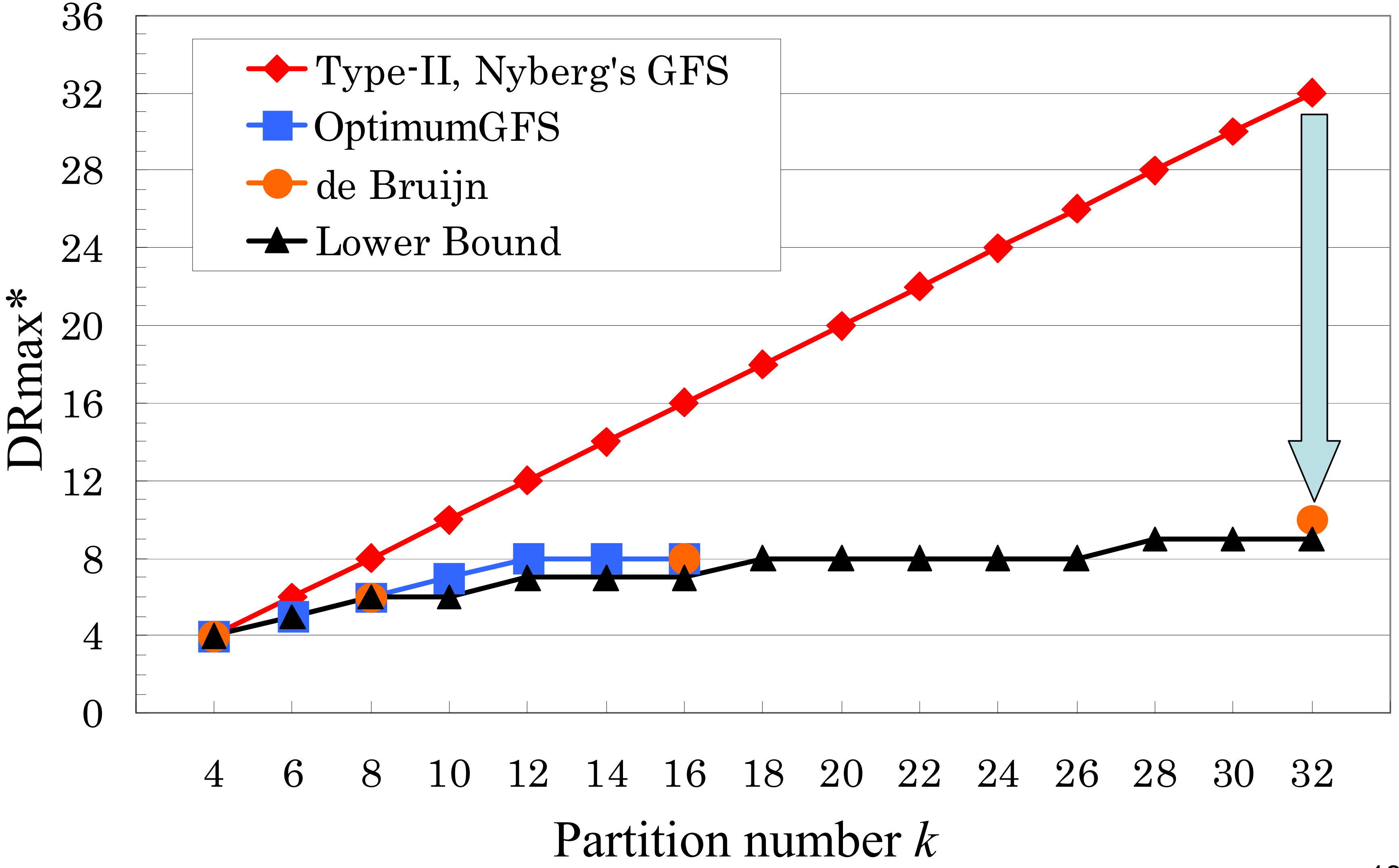
} Good candidate for a graph with small *SD* !

How to color the edges ?

We found a coloring of de Bruijn which achieves *SD* at most 2s+1.

(see the paper for details)

Our result


36
32
28
24
20
16
12
8
4
0
DRmax*
Type-II, Nyberg's GFS
OptimumGFS
de Bruijn
Lower Bound
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
Partition number k

Security evaluation

- Pseudorandomness
- Cryptanalysis
  - Impossible Differential Attack
  - Saturation Attack

Previous study of Pseudorandomness

- Luby and Rackoff proved pseudorandomness of Feistel structure.
  3 rounds Feistel is pseudorandom permutation (prp).
  4 rounds Feistel is strong prp (sprp).

- Mitsuda and Iwata proved pseudorandomness of Type-II GFS [MI08].
  k+1 rounds Type-II is prp.
  2k rounds Type-II is sprp.

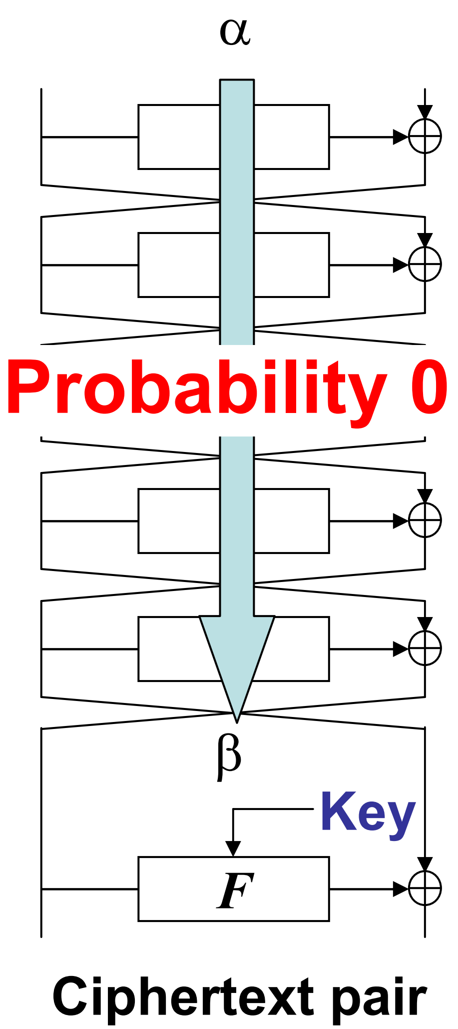
We proved pseudorandomness of GFS with even-odd shuffle using *SD*.

Pseudorandomness of GFS

	prp		sprp	
	Round	Advantage	Round	Advantage
Type-II GFS [MI08]	$k+1$	$\frac{k^2}{2^n}q^2$	$2k$	$\frac{k^2}{2^n}q^2$
GGFS with even-odd	$L+2$ $SD(G[\pi])\leq L$	$\frac{kL}{2^{n+1}}q^2$	$2L+2$ *	$\frac{kL}{2^n}q^2$
de Bruijn based GFS	$2\log k+1$	$\frac{2k\log k}{2^n}q^2$	$4\log k$	$\frac{4k\log k}{2^n}q^2$

* $\max\{ SD(G[\pi]), SD(G[\pi^{-1}]) \} \leq L$

Impossible differential characteristics



When the probability of α → β is zero (Impossible Differential Characteristics : IDC),
α → β is an impossible differential.

Decrypt one round using the ciphertext pair obtained from the plaintext pair for which the difference is α.

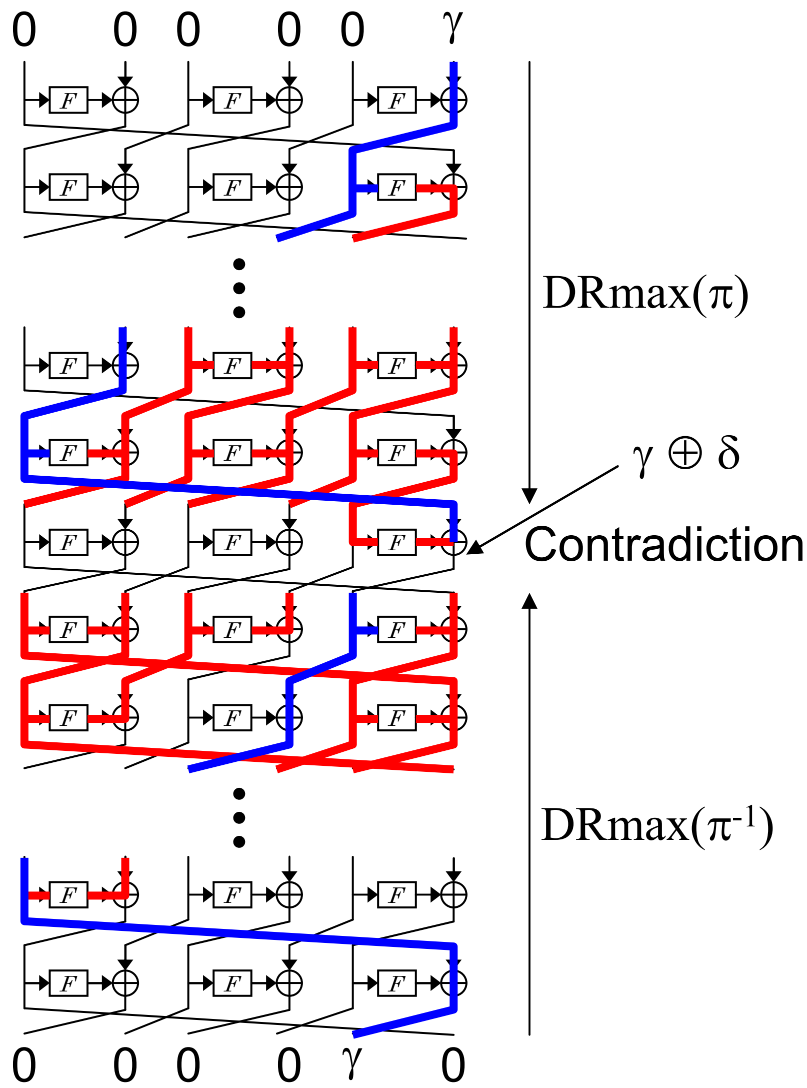
Reject the key for which the difference is β.

The last remaining key is the correct key.

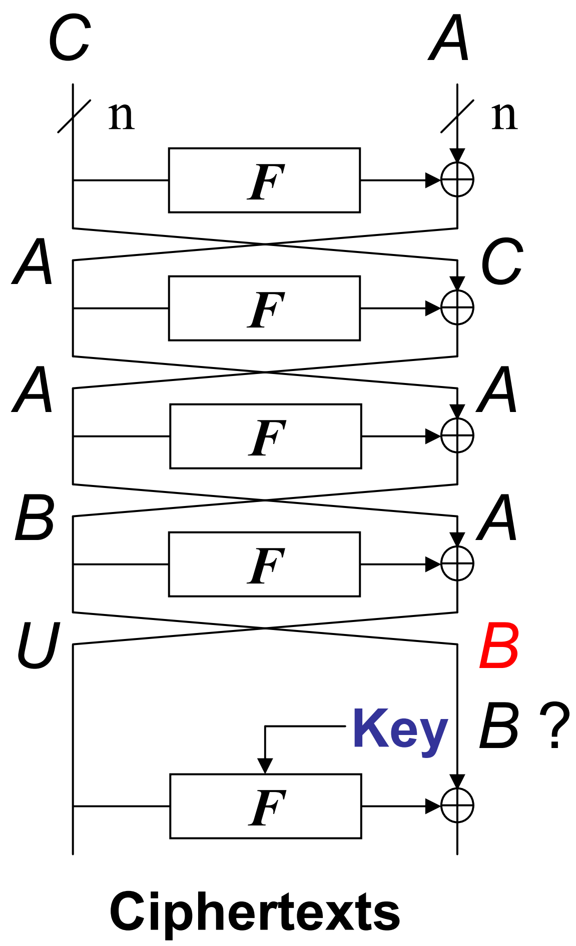
Evaluation of IDC

Kim et al. showed the number of rounds for IDC of Type-II GFS is $2k+1$.

From the characteristic of *U*-method (proposed by Kim et al.) and the definition of DRmax, the number of rounds for IDC of GFS becomes at most 2DRmax+1.



Saturation characteristics



A: *ALL* *B*: *Balance*
C: *Constant* *U*: *Unknown*

Decrypt one round using the 2^n ciphertexts obtained from the 2^n all plaintexts.

Reject the key for which the sum is not balance.

The last remaining key is the correct key.

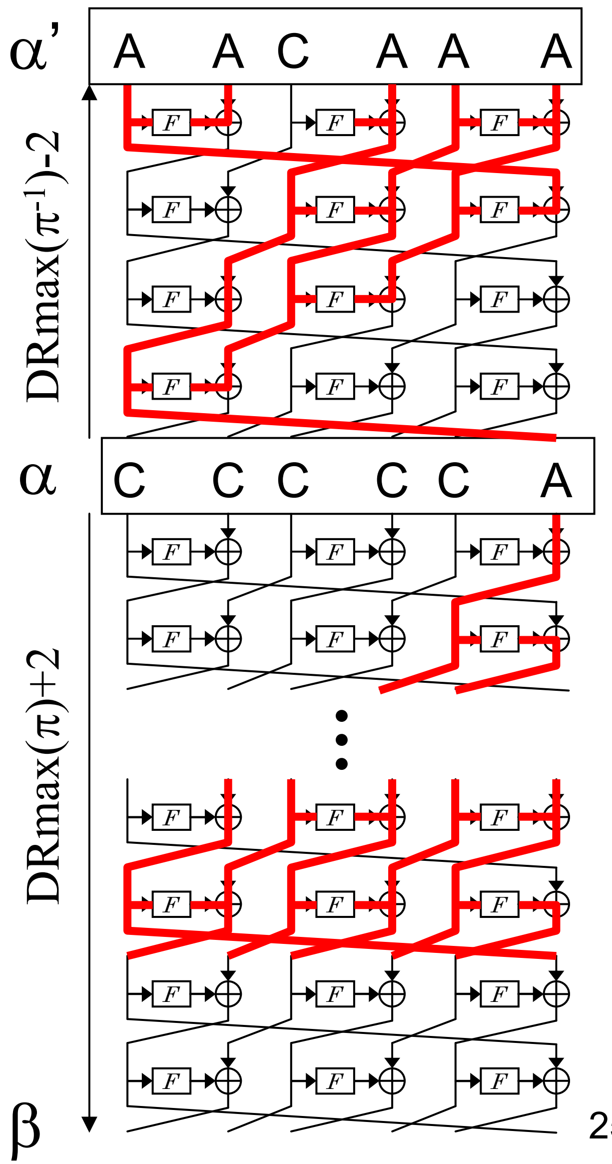
Evaluation of saturation characteristics (SC)

Search of saturation characteristics :

1. $\alpha \rightarrow \beta$
   After DRmax(π)+3 rounds, the balance state does not remain.
   $\rightarrow$ at most DRmax(π)+2 rounds.

2. Expansion from α to α'
   At least one *Constant* must be contained.
   $\rightarrow$ st most DRmax(π)-2 rounds.

$\alpha' \rightarrow \beta$ is at most 2DRmax rounds.



Numerical comparison

(round)	$k = 8$		$k = 16$	
	Type-II	optimum	Type-II	optimum
DRmax	8	6	16	8
prp	9	7	17	9
sprp	16	12	32	16
IDC	17	13	33	17
SC	16	12	32	16

Conclusion

- Propose “Generalized” GFS that allow arbitrary network
- Propose criteria (Sufficient Distance) for the diffusion property
- de Bruijn graph based GFS has GOOD diffusion property
- A diffusive improvement showed leading to the improvement of security.

Thank you for your attention !