Type 1.x Generalized Feistel Structures

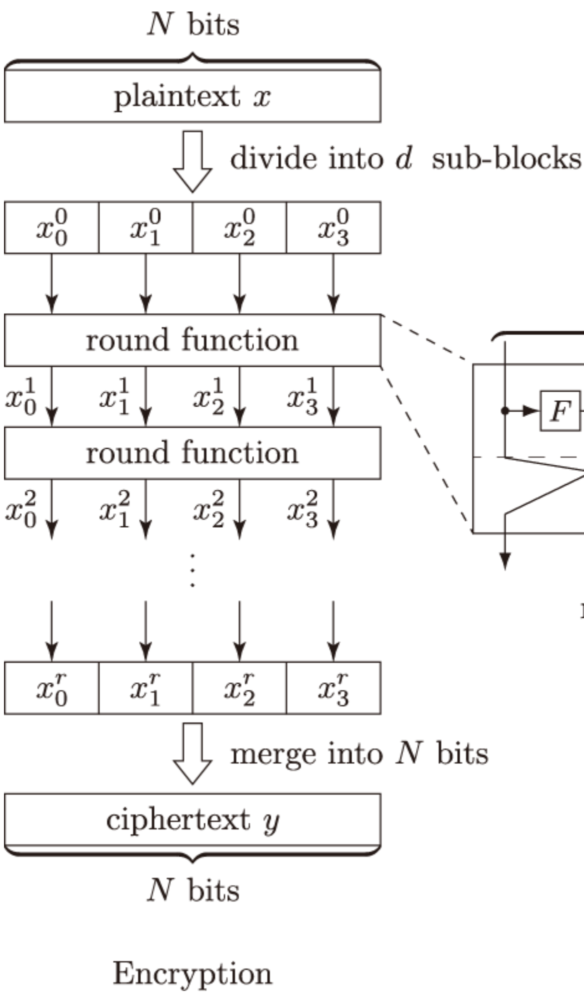
Shingo Yanagihara and Tetsu Iwata

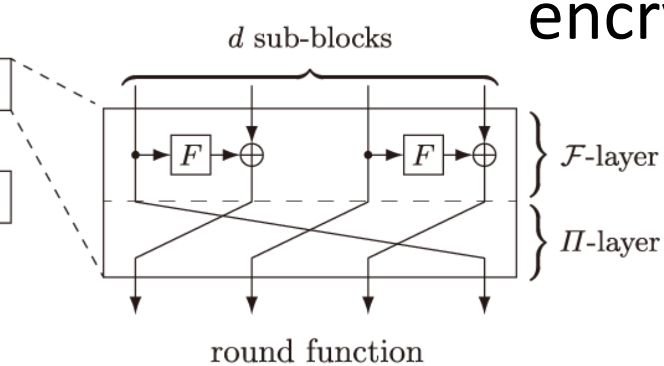
Nagoya University, Japan

WCC 2013,

April 15-19, 2013, Bergen (Norway)

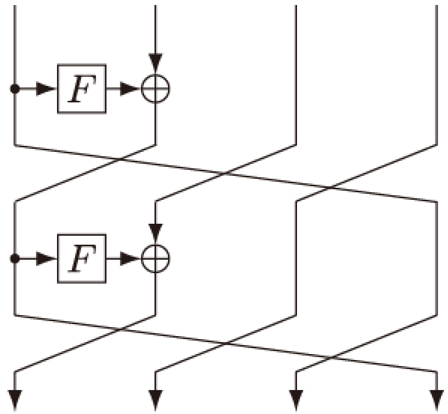
Generalized Feistel Structure (GFS)



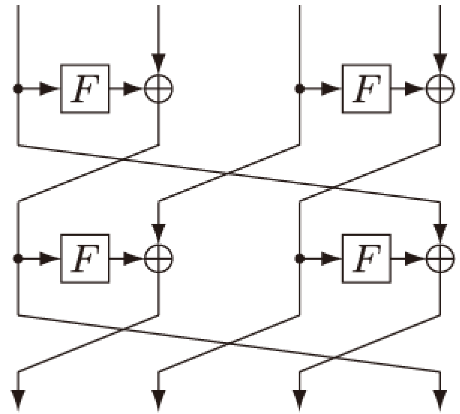


- The same computation of the nonlinear functions in encryption and decryption

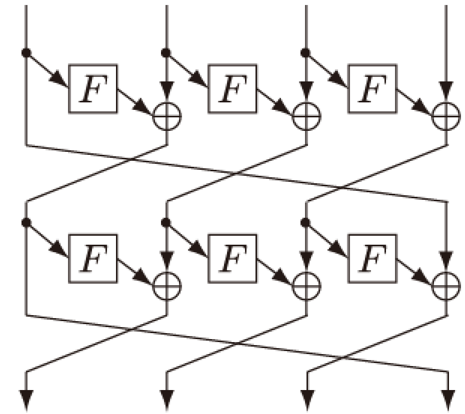
- Poor diffusion property
  - It requires many rounds to be secure.



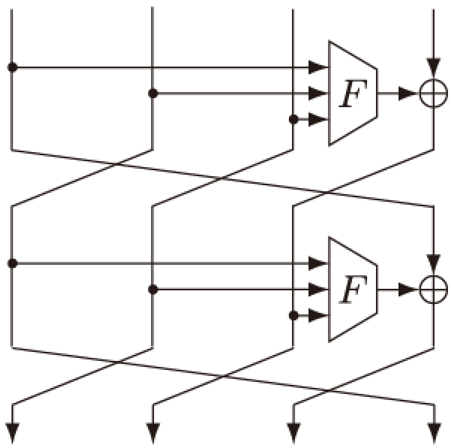
Type 1
CAST-256



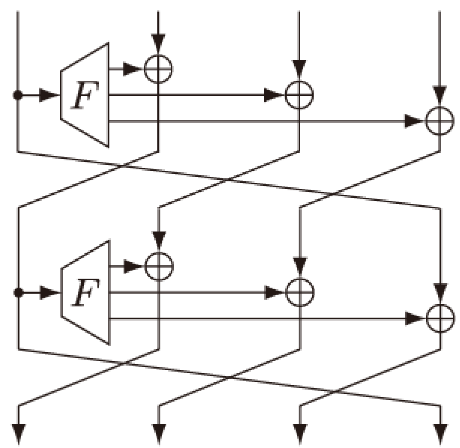
Type 2
RC6, HIGHT, CLEFIA



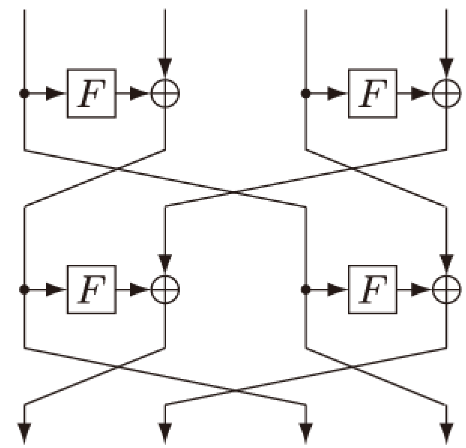
Type 3



Source-Heavy
RC2, SPEED

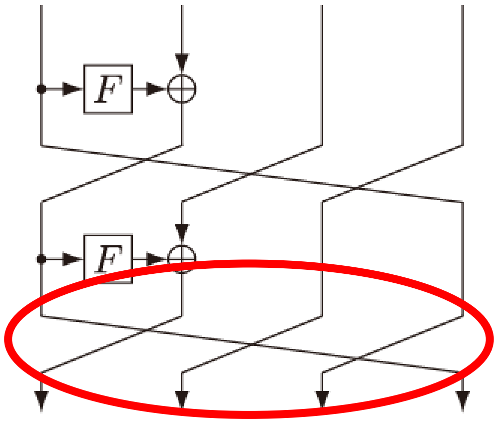


Target-Heavy
MARS

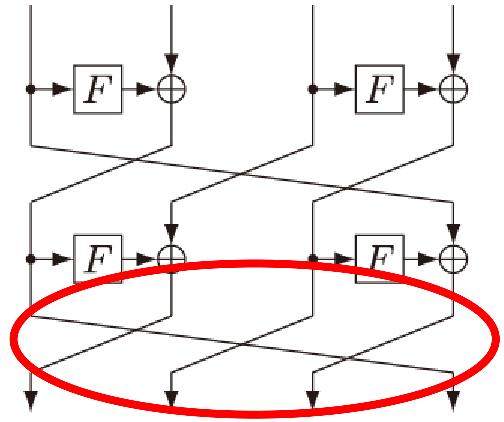


Nyberg's GFS

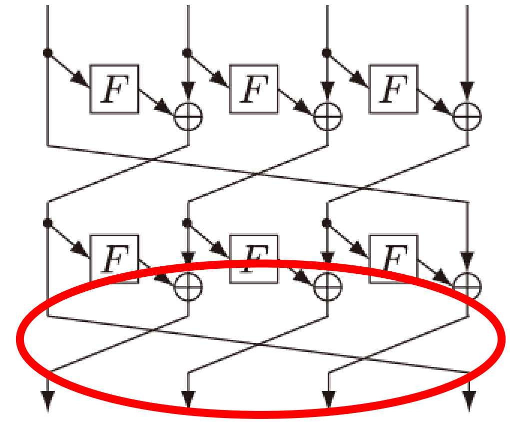
- Generally, GFS has the sub-block-wise cyclic shift (π_s).



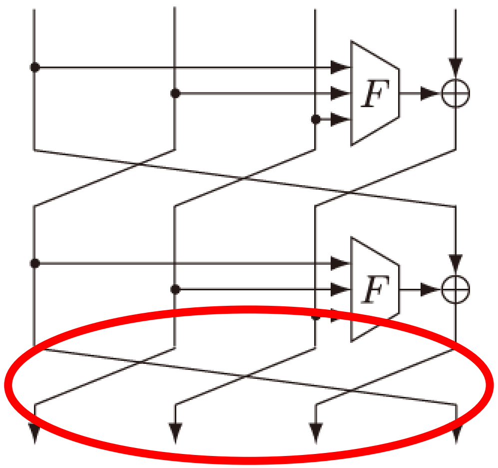
Type 1
CAST-256



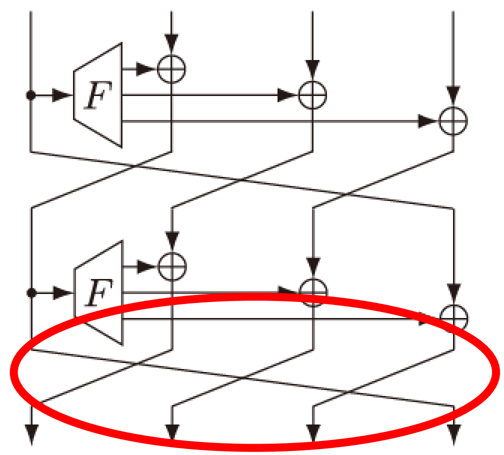
Type 2
RC6, HIGHT, CLEFIA



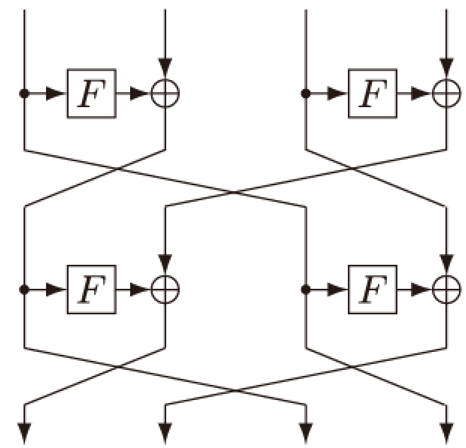
Type 3



Source-Heavy
RC2, SPEED



Target-Heavy
MARS



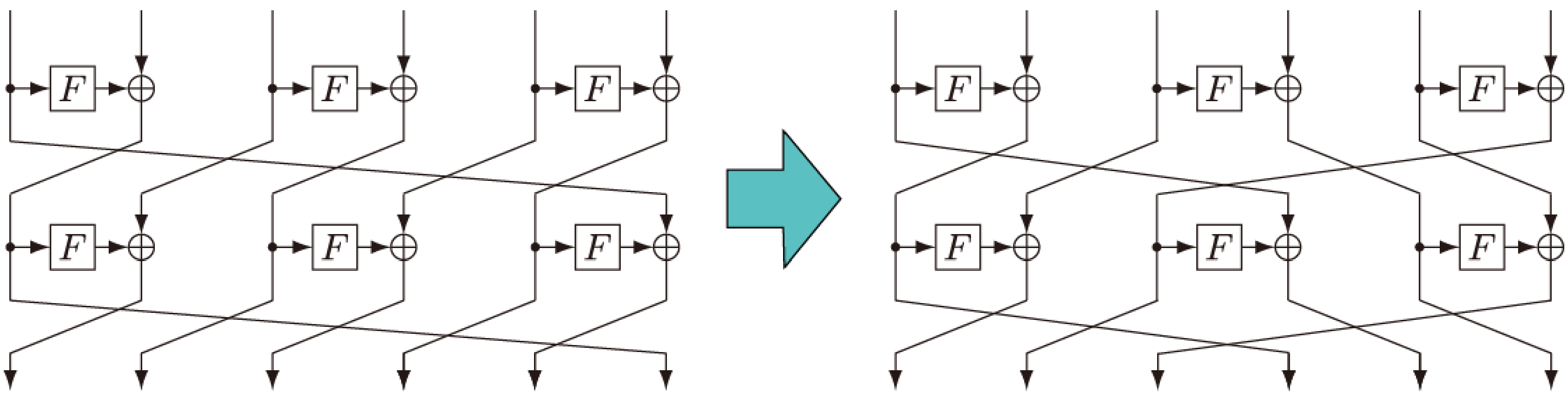
Nyberg's GFS

- Generally, GFS has the sub-block-wise cyclic shift (π_s).

Previous work
[FSE 2010, Suzaki, Minematsu]

- Changing the permutation of Type 2 GFS from π_s
- There are permutations such that
  - the diffusion property and
  - the security against several attacks

  are better than π_s.



The diffusion property and
the security improve.

Previous work [IEICE 2013, Yanagihara, Iwata]

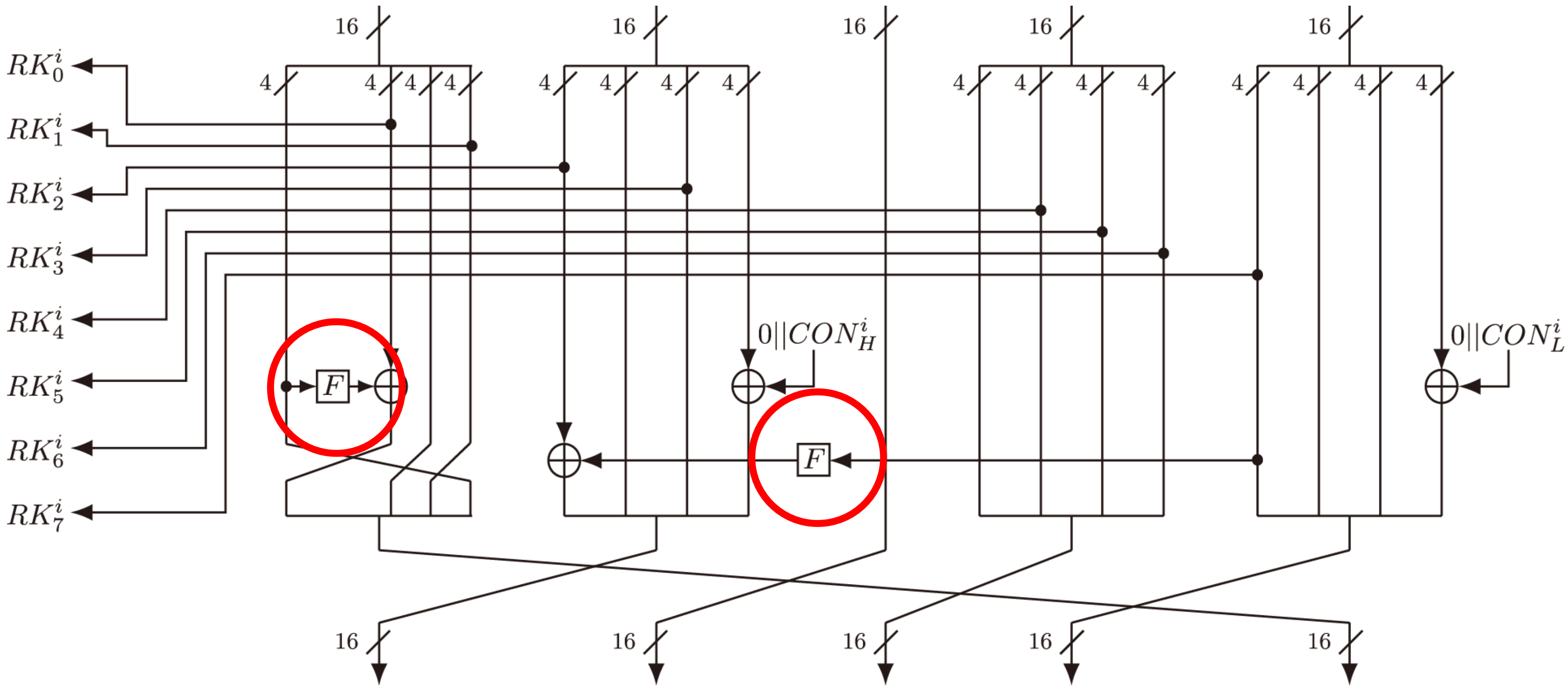
- FD (full diffusion):
  every output sub-blocks depend on all input sub-blocks
- For Type 1 GFS
  - π_s : the worst permutation in terms of the diffusion property among permutations archive FD.
  - The construction of the best permutation

Previous work [IEICE 2013, Yanagihara, Iwata]

- For Type 3 GFS,
  - The condition of a permutation which cannot archive FD with any number of rounds.
- For Source-Heavy and Target-Heavy GFSs
  - π_s : the best permutation in terms of the diffusion property.

Example of unclassified types of GFS

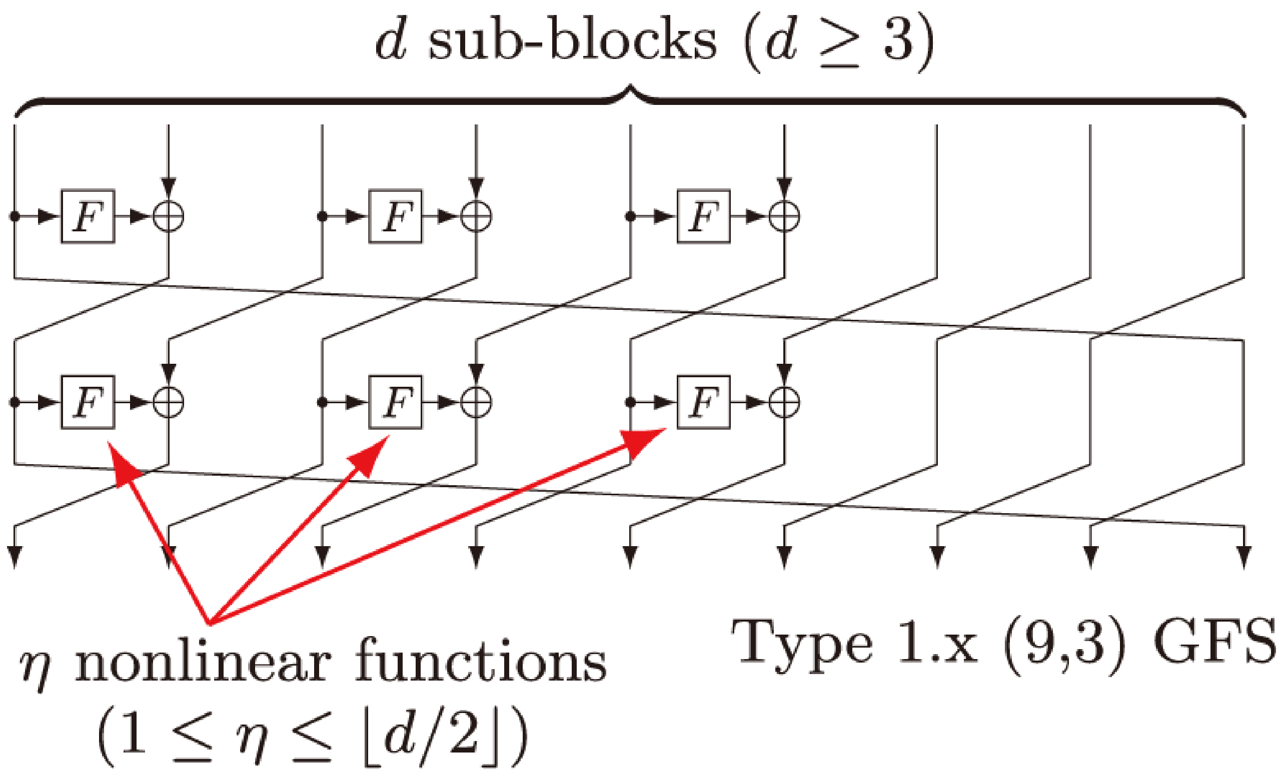
- Key schedule function of TWINE [SAC 2012]
  - Two nonlinear functions in $\mathcal{F}$ -Layer



Our work

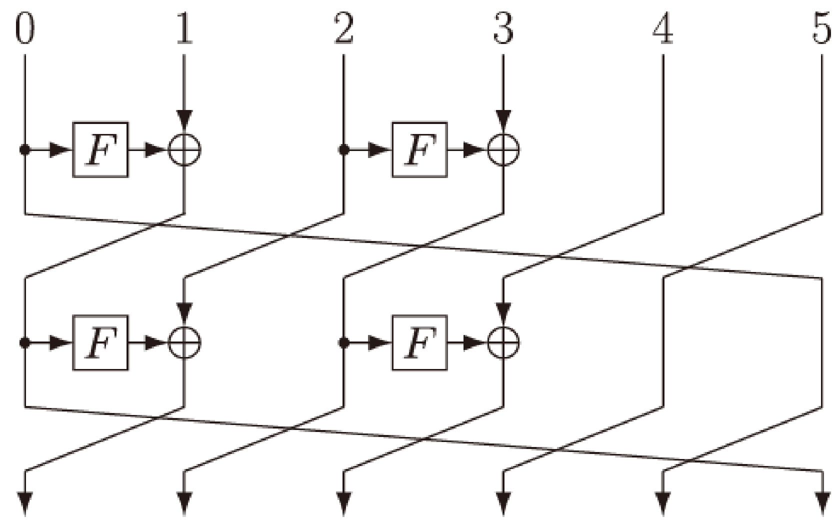
- Propose Type 1.x GFS
  - covers Type 1 and Type 2 GFSs as special cases
- Propose a construction of a permutation for Type 1.x GFS with two nonlinear functions in F-Layer
- Present analysis of Type 1.x GFS with π_s
  - compare proposed construction with π_s
- Show experimental results for Type 1.x GFS for $3 \leq d \leq 8$

Type 1.x (d, η) GFS



- Type 1.x $(d, 1)$ GFS ⇔ Type 1 GFS
- Type 1.x $(d, d/2)$ GFS (d is even) ⇔ Type 2 GFS

Notation

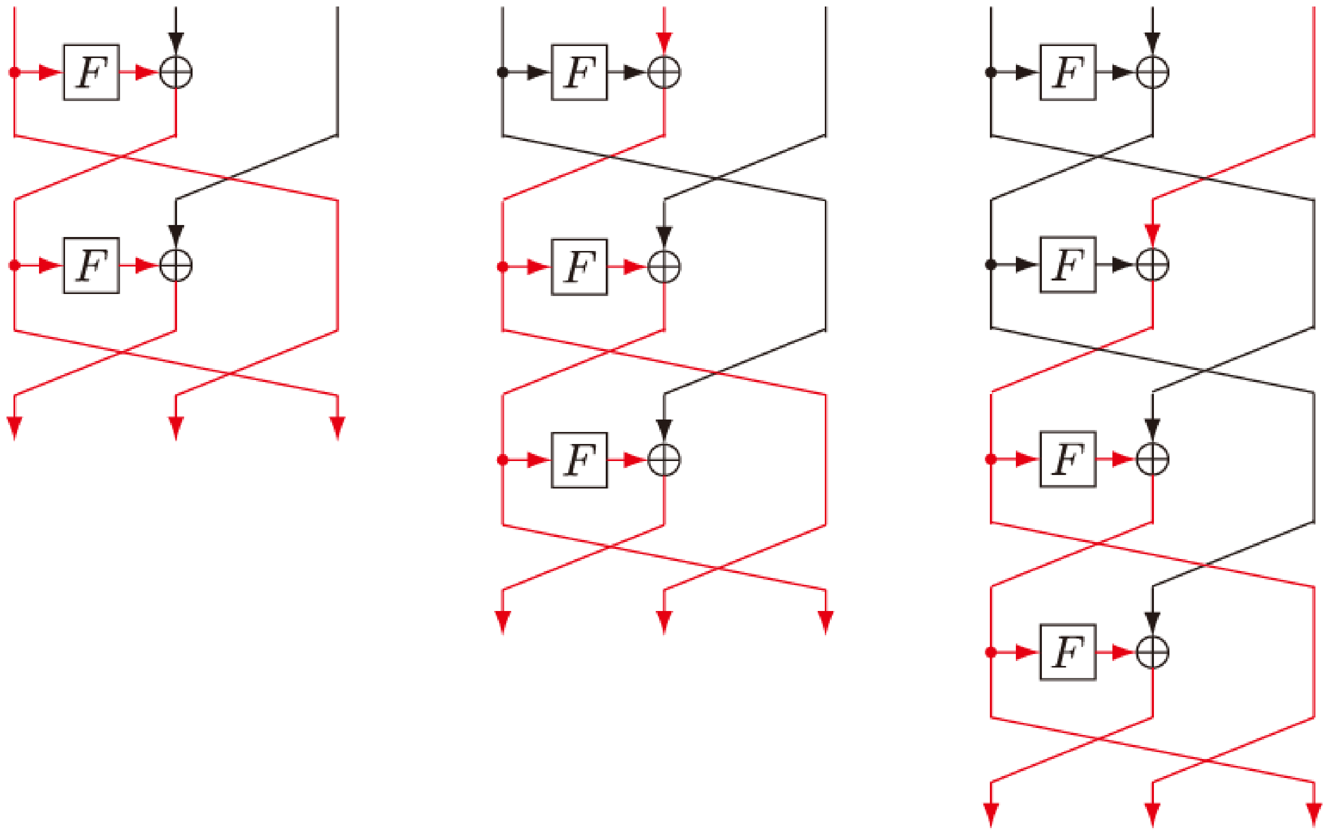


$\pi = (5, 0, 1, 2, 3, 4)\ (= \pi_s)$

- $\pi_s = (d-1, 0, 1, \ldots, d-2)$ (← left cyclic shift)
- $\pi(i)$: the sub-block after applying π to the i-th sub-block.
- r_{ij} : the smallest number r such that $\pi^r(i) = j$.

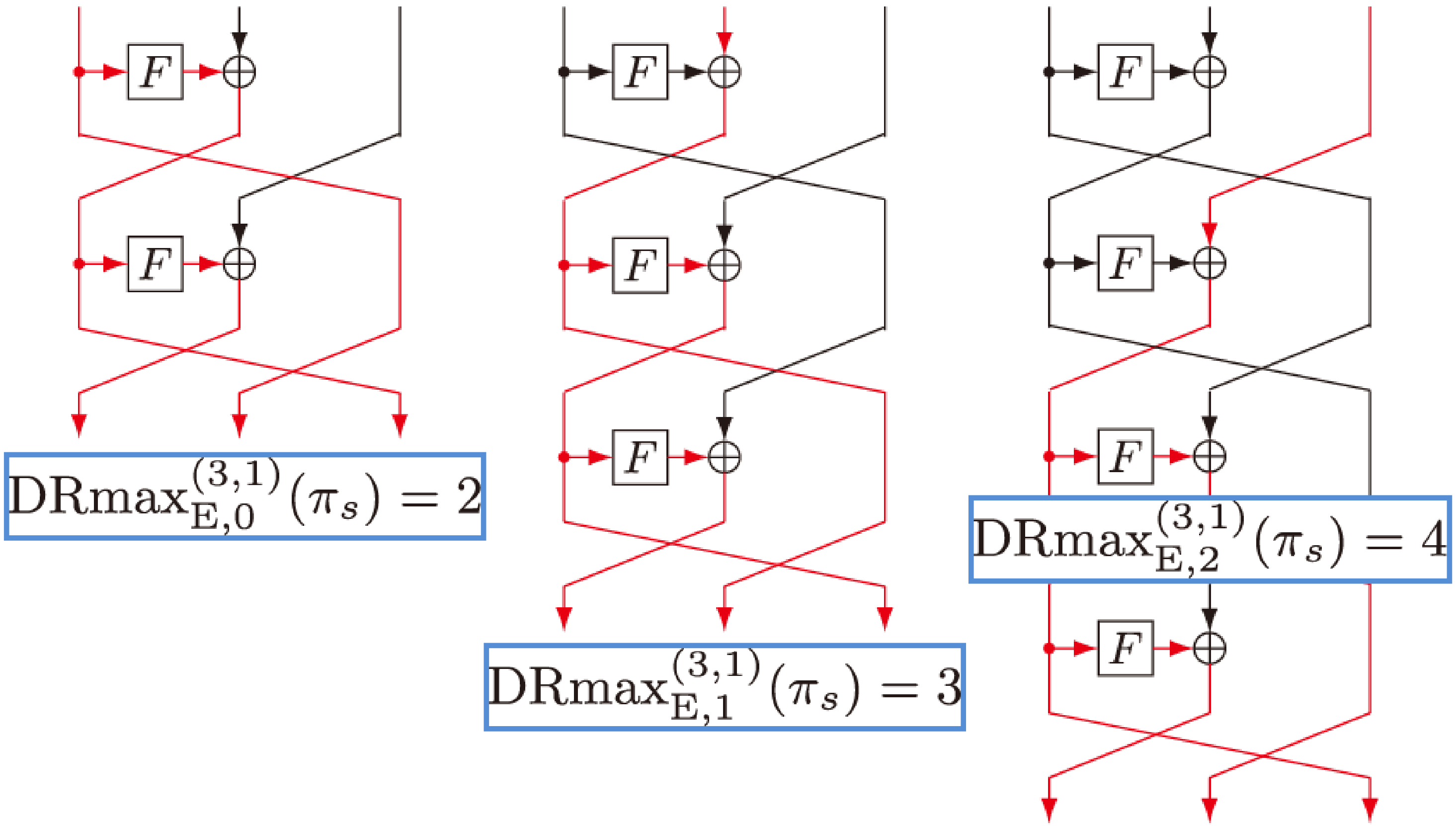
DRmax [Suzaki, Minematsu, FSE 2010]

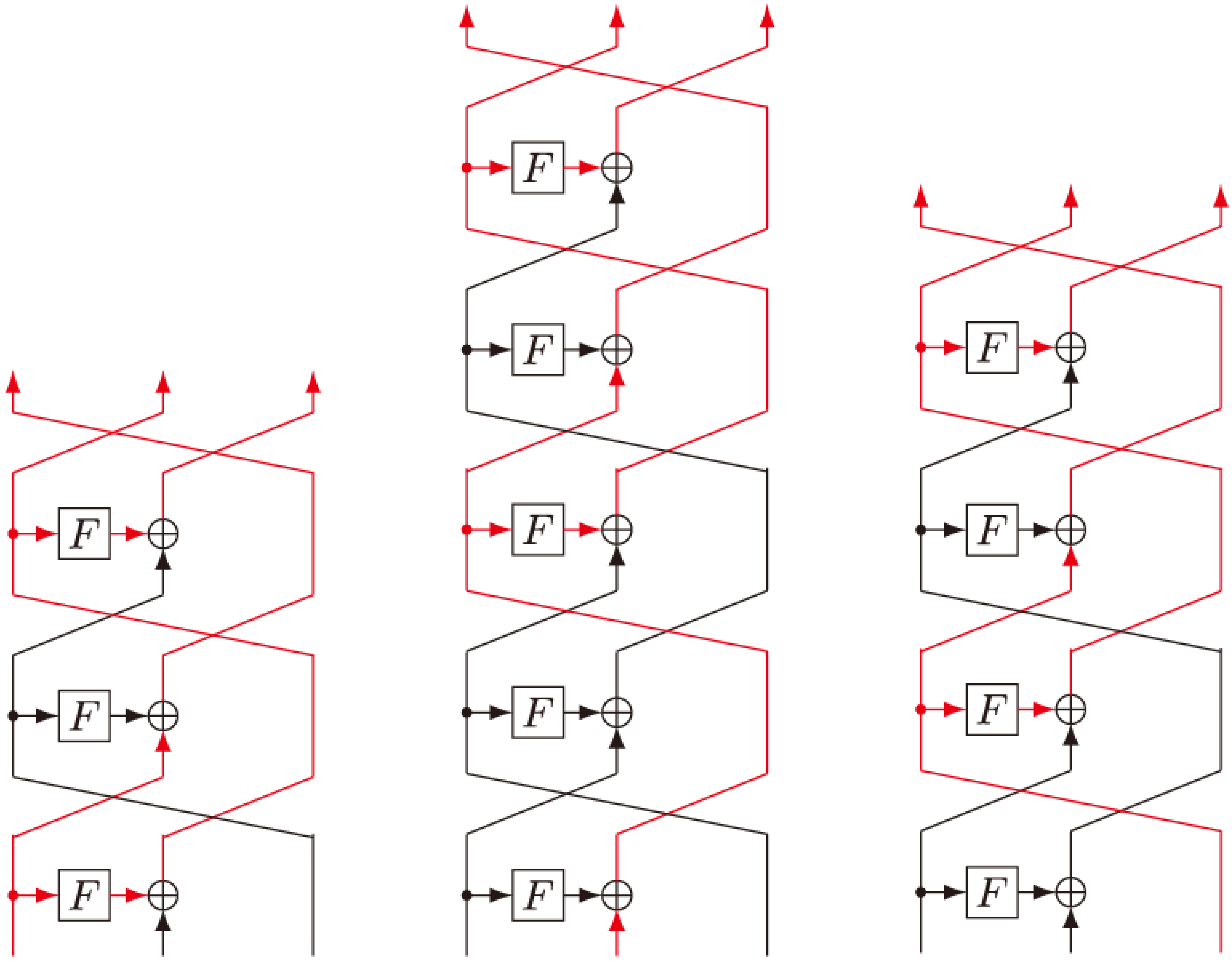
- $\mathrm{DRmax}^{(d,\eta)}(\pi)$: The smallest round such that every output sub-blocks depend on all input sub-blocks.

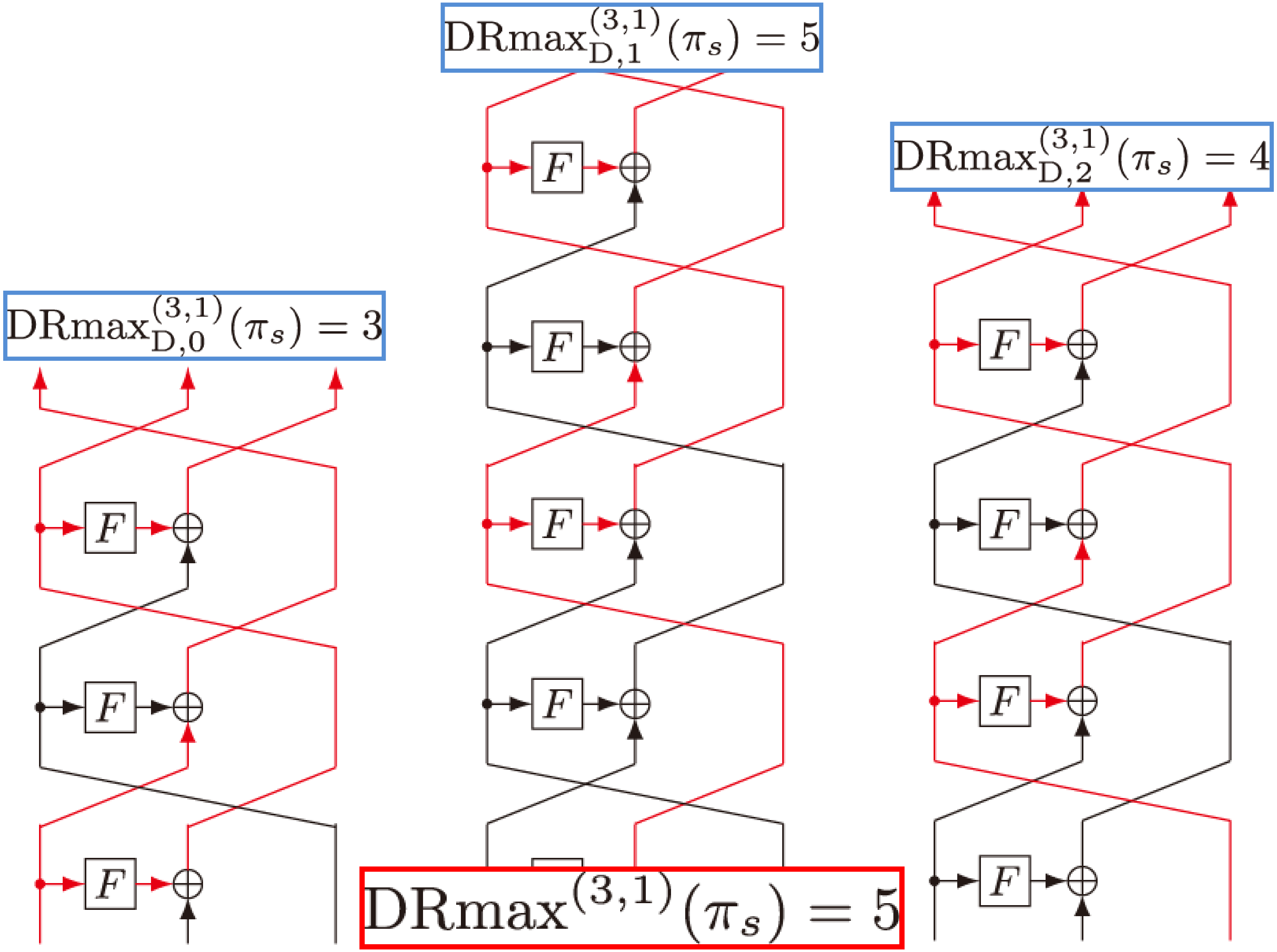


DRmax
[Suzaki, Minematsu, FSE 2010]

- $\mathrm{DRmax}^{(d,\eta)}(\pi)$: The smallest round such that every output sub-blocks depend on all input sub-blocks.




F
F
F
F
F
F
F
F
F
F
F
F



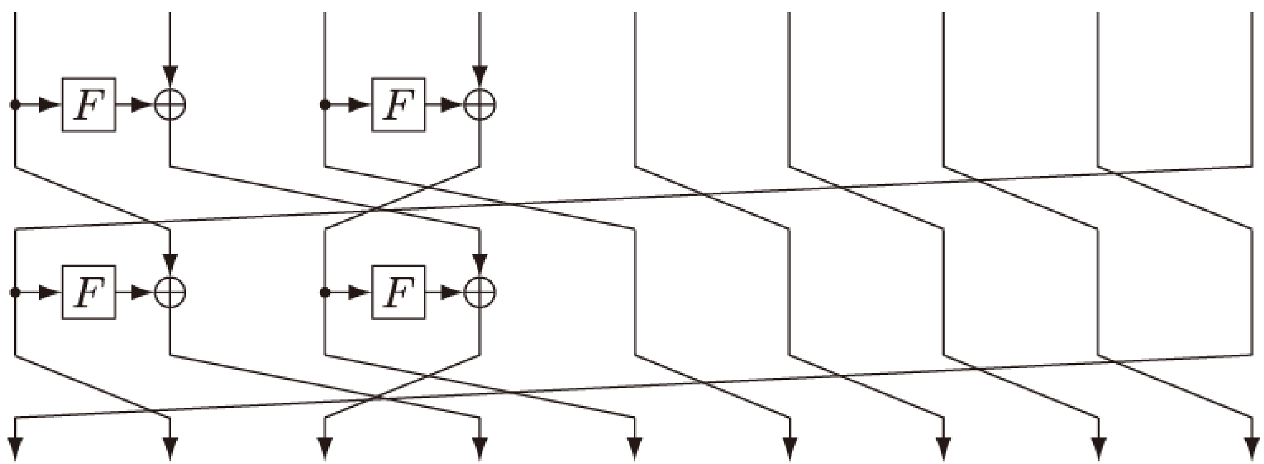
$\mathrm{DRmax}_{\mathrm{D},1}^{(3,1)}(\pi_s) = 5$
$\mathrm{DRmax}_{\mathrm{D},2}^{(3,1)}(\pi_s) = 4$
$\mathrm{DRmax}_{\mathrm{D},0}^{(3,1)}(\pi_s) = 3$
F
$\mathrm{DRmax}^{(3,1)}(\pi_s) = 5$

Proposed construction for $\eta = 2$

Let $d \geq 5$ and a be an integer

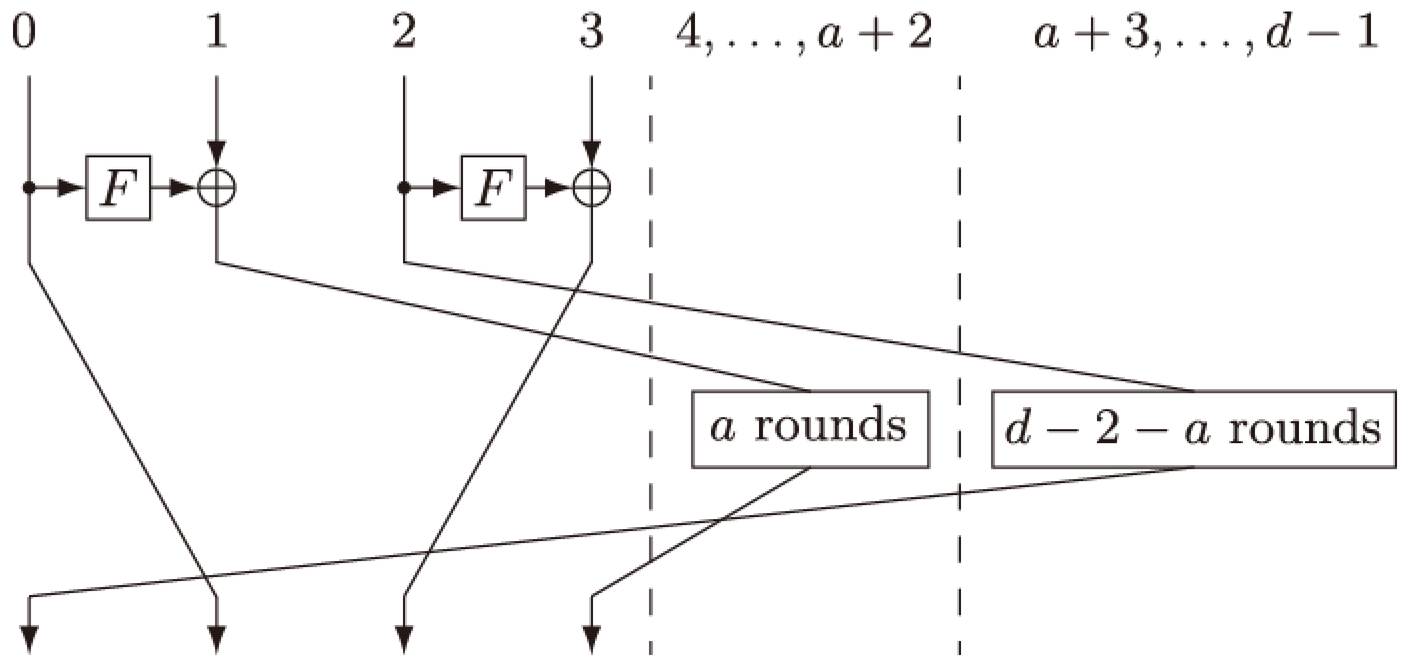
such that $1 \leq a \leq d-3$

$$\pi_p = \begin{cases} (1,3,4,2,5,6,\ldots,d-1,0) & \text{if } a=1 \\ (1,4,0,2,5,6,\ldots,d-1,3) & \text{if } a=d-3 \\ (1,4,a+3,2,5,6,\ldots,a+2,3,a+4,a+5,\ldots,d-1,0) & \text{otherwise} \end{cases}$$



Type 1.x (9,2) GFS with π_p when $a = 1$

Properties of the proposed construction π_p



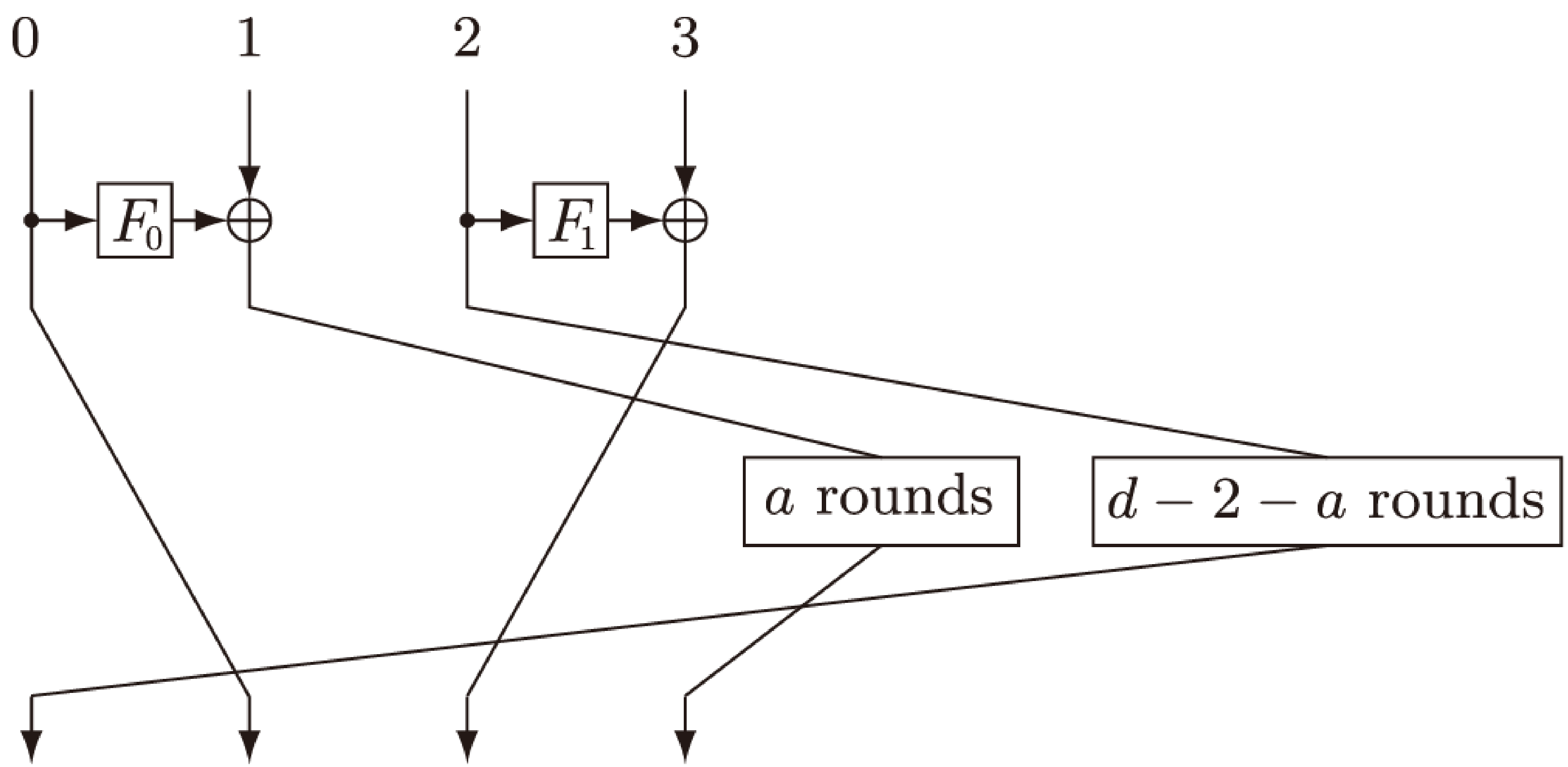
$$r_{01} = r_{32} = 1, r_{13} = a, r_{20} = d - 2 - a$$

DRmax of the proposed construction

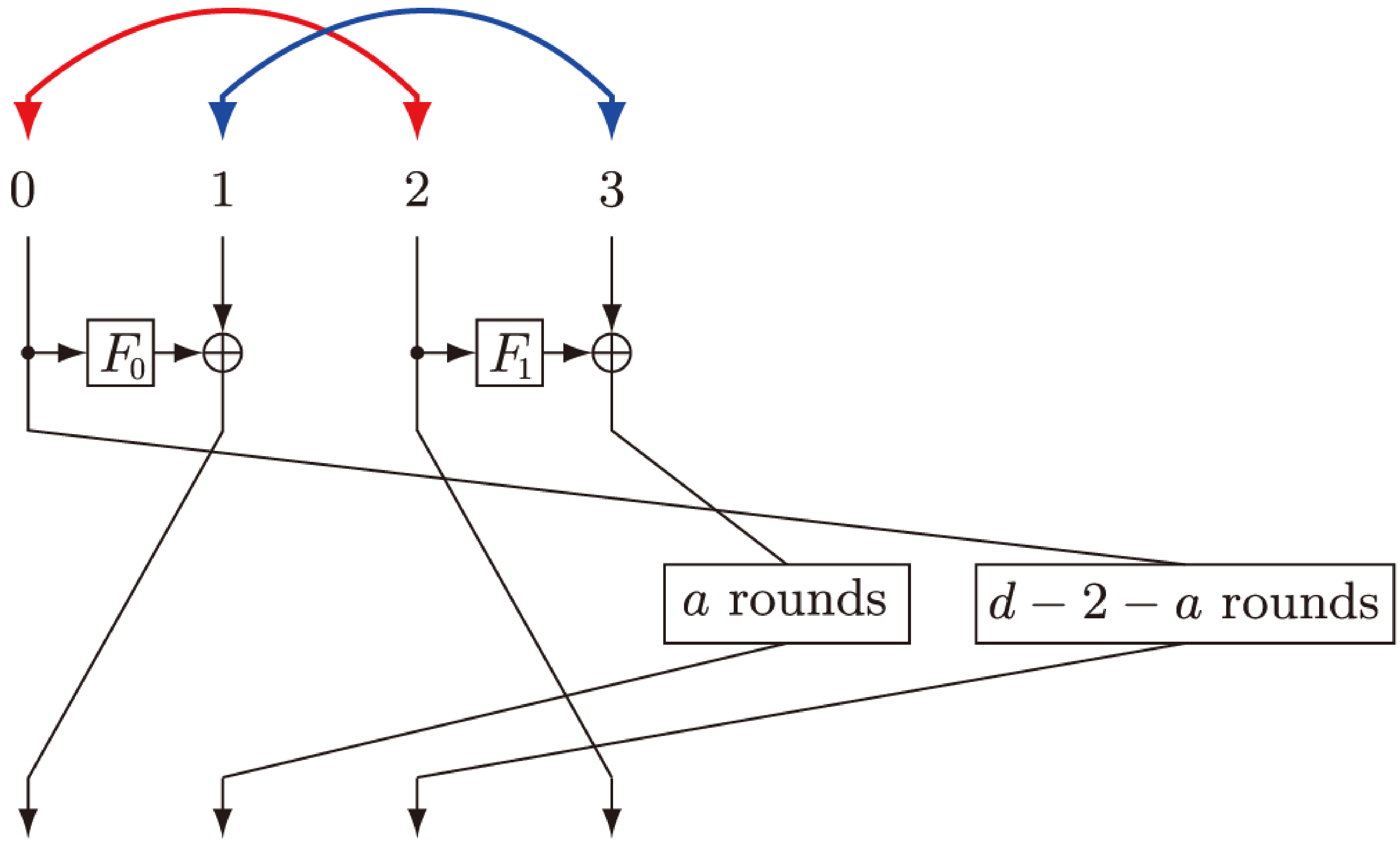
Lemma *Let* $d \geq 5$. *Then we have* $\mathrm{DRmax}^{(d,2)}(\pi_p) = 2d - 4$.

- Brief overview of the proof:
  Using the property,
  - The largest DRmax for encryption is
    $\mathrm{DRmax}^{(d,2)}_{\mathrm{E},\pi_p(2)}(\pi_p) = 2(r_{13} + r_{20}) = 2d - 4$
  - The largest DRmax for decryption is $2d - 4$, because the structures of encryption and decryption are equivalent.

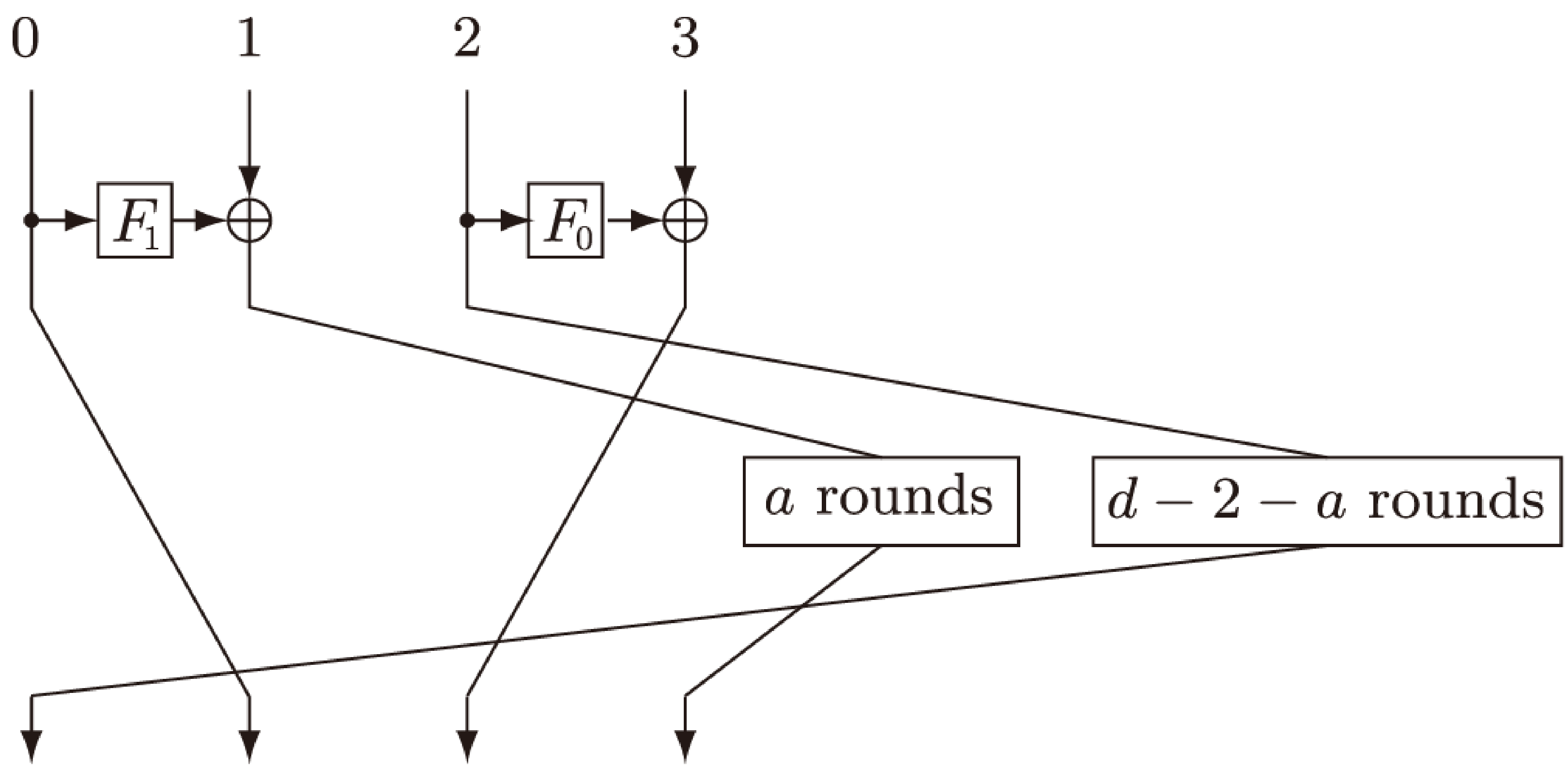
Equivalence of the structure



Equivalence of the structure

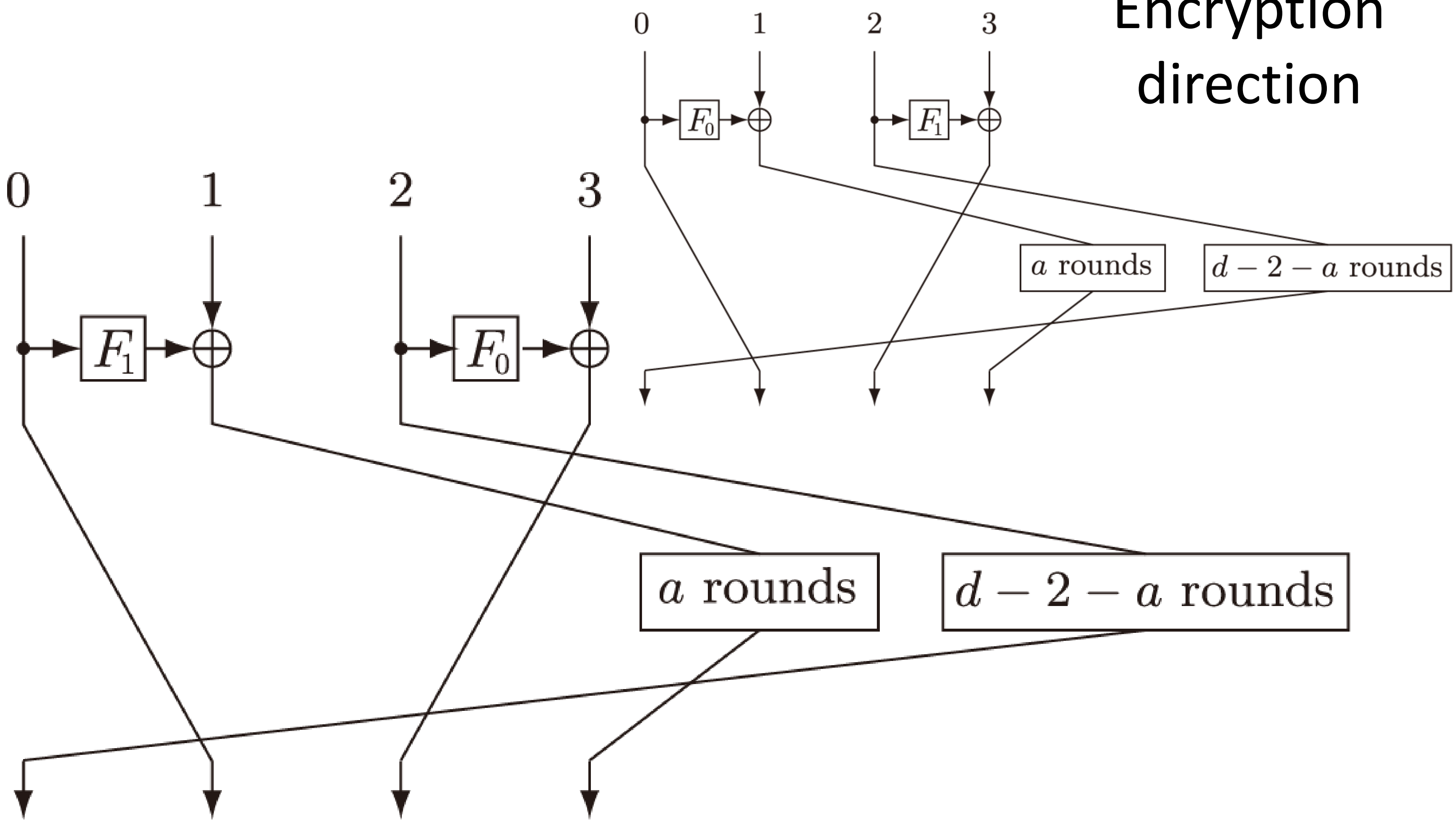


Equivalence of the structure



Equivalence of the structure

Encryption direction



DRmax with π_s

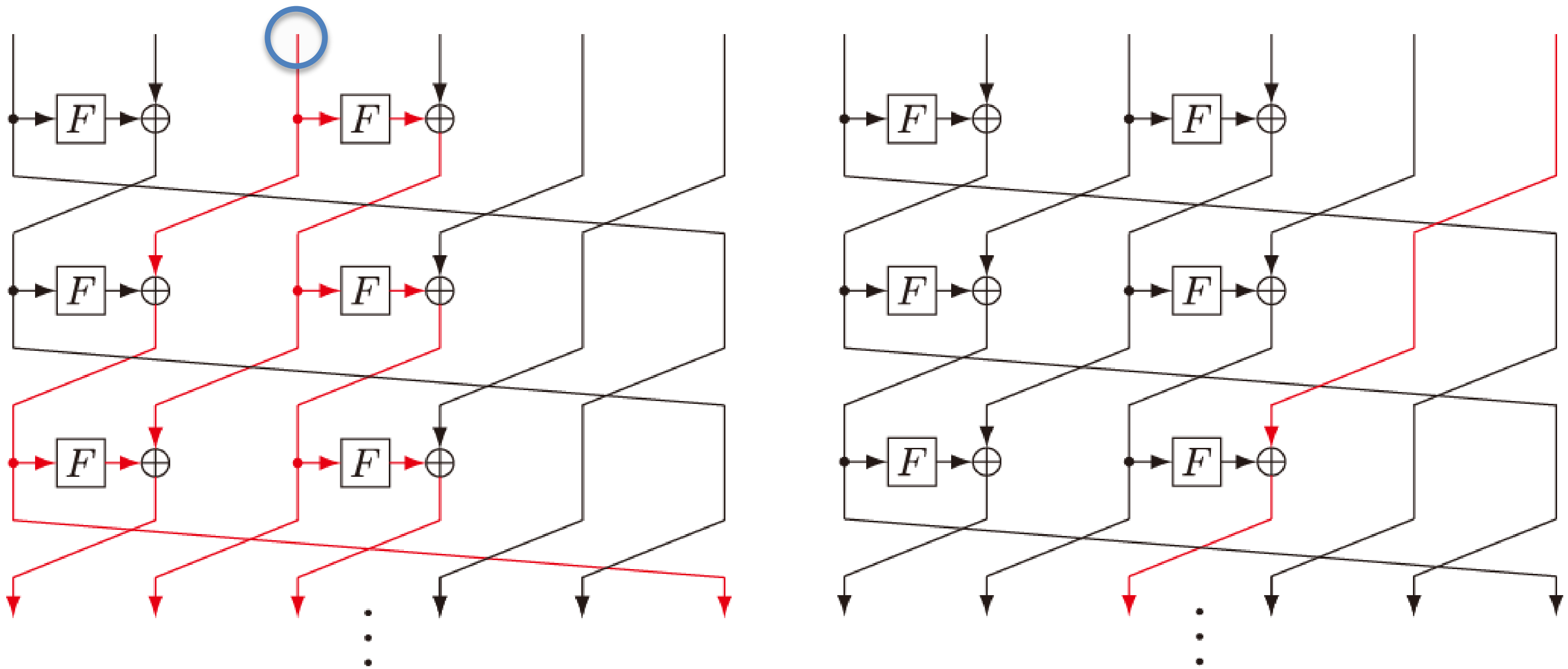
Lemma : *For any* $d \geq 3$ *and* $1 \leq \eta \leq \lfloor d/2 \rfloor$, *we have*
$\mathrm{DRmax}^{(d,\eta)}(\pi_s) = \max\{\mathrm{DRmax}^{(d,\eta)}_{\mathrm{D},2\eta-3}(\pi_s), \mathrm{DRmax}^{(d,\eta)}_{\mathrm{D},2\eta-1}(\pi_s)\}$, *where*

$$\mathrm{DRmax}^{(d,\eta)}_{\mathrm{D},2\eta-3}(\pi_s) = \begin{cases} \left(\dfrac{d-2}{\eta}\right)(d-\eta)+2 & \text{if } (d-2) \bmod \eta = 0 \\ \left\lfloor \dfrac{d-2}{\eta} \right\rfloor (d-2\eta)+2(d-\eta) & \text{otherwise} \end{cases}$$

$$\mathrm{DRmax}^{(d,\eta)}_{\mathrm{D},2\eta-1}(\pi_s) = \begin{cases} \left(\dfrac{d-1}{\eta}\right)(d-\eta)+1 & \text{if } (d-1) \bmod \eta = 0 \\ \left\lfloor \dfrac{d-1}{\eta} \right\rfloor (d-2\eta)+2(d-\eta) & \text{otherwise.} \end{cases}$$

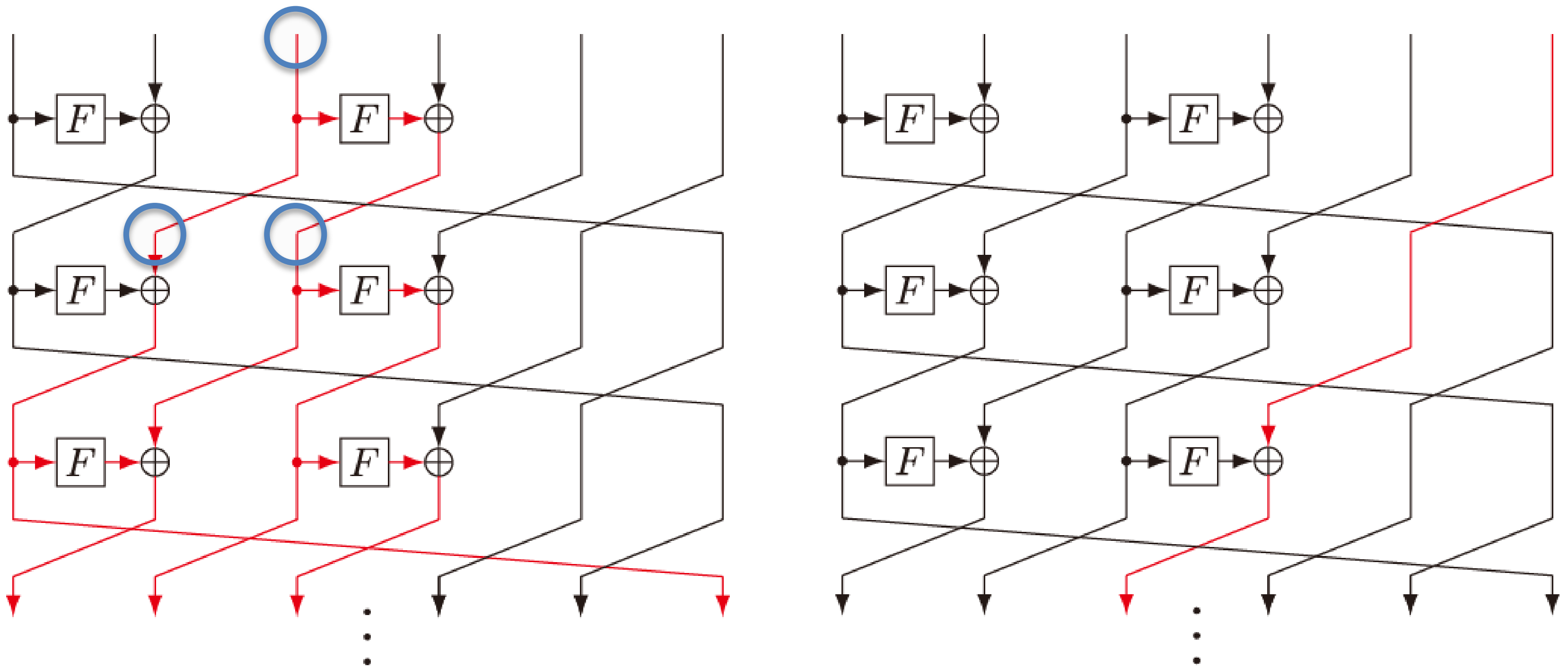
Brief overview of the proof

- For encryption



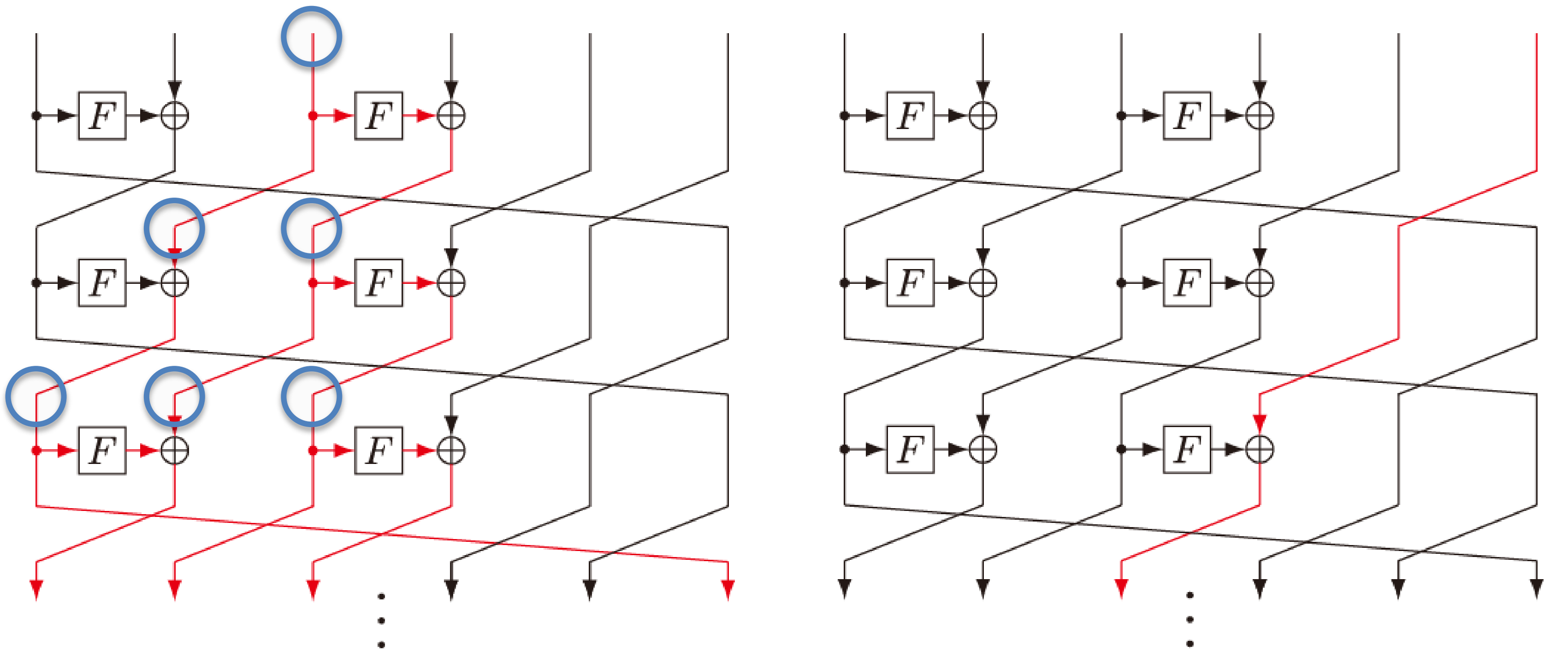
Brief overview of the proof

- For encryption



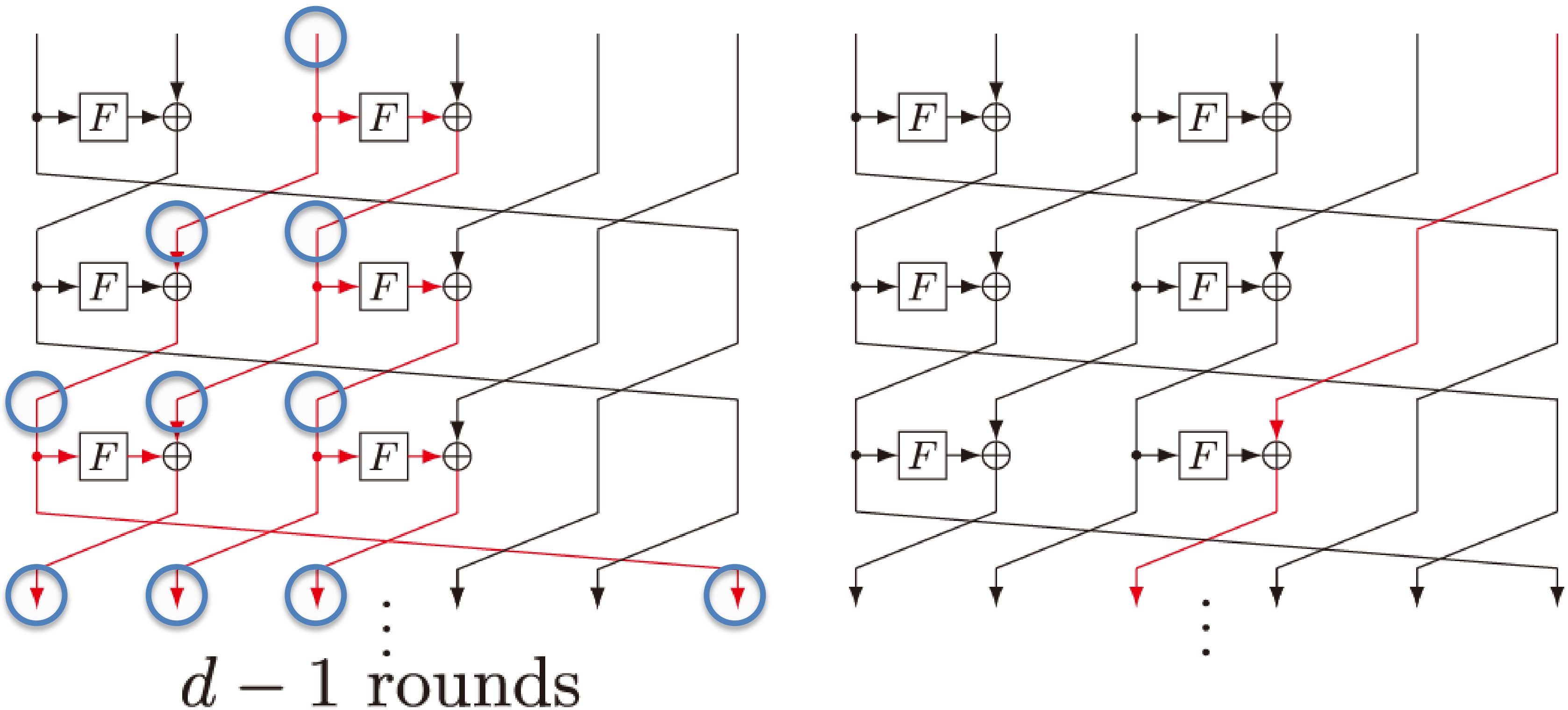
Brief overview of the proof

- For encryption



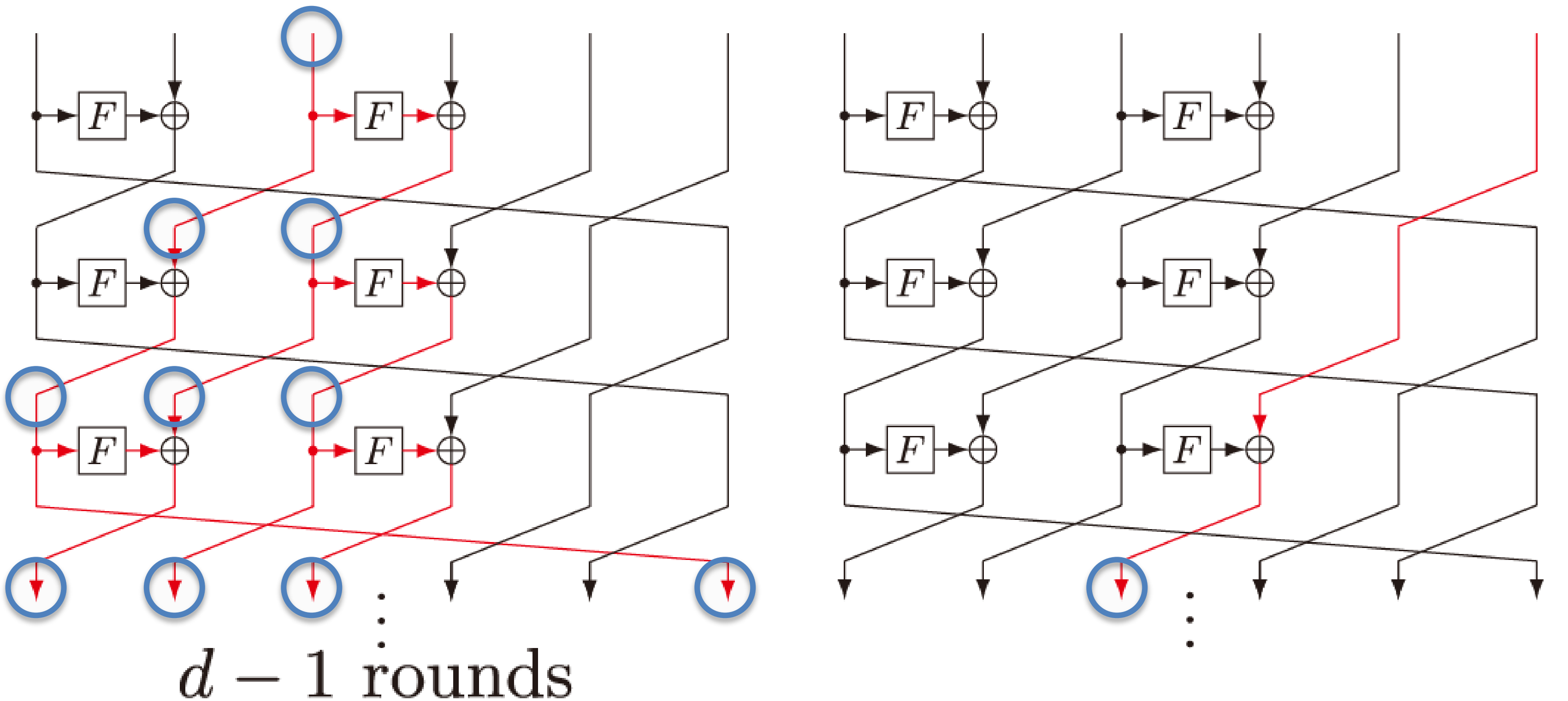
Brief overview of the proof

- For encryption



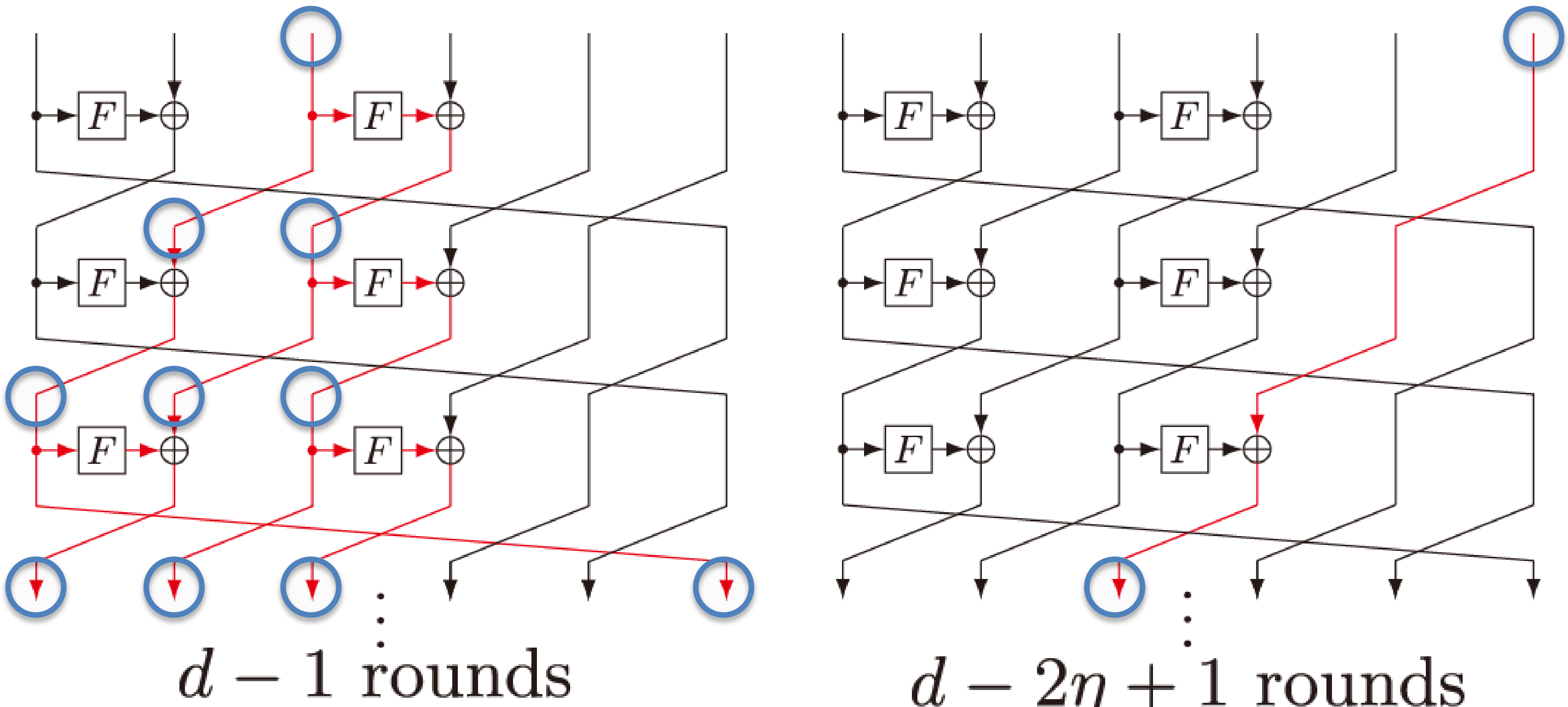
Brief overview of the proof

- For encryption



Brief overview of the proof

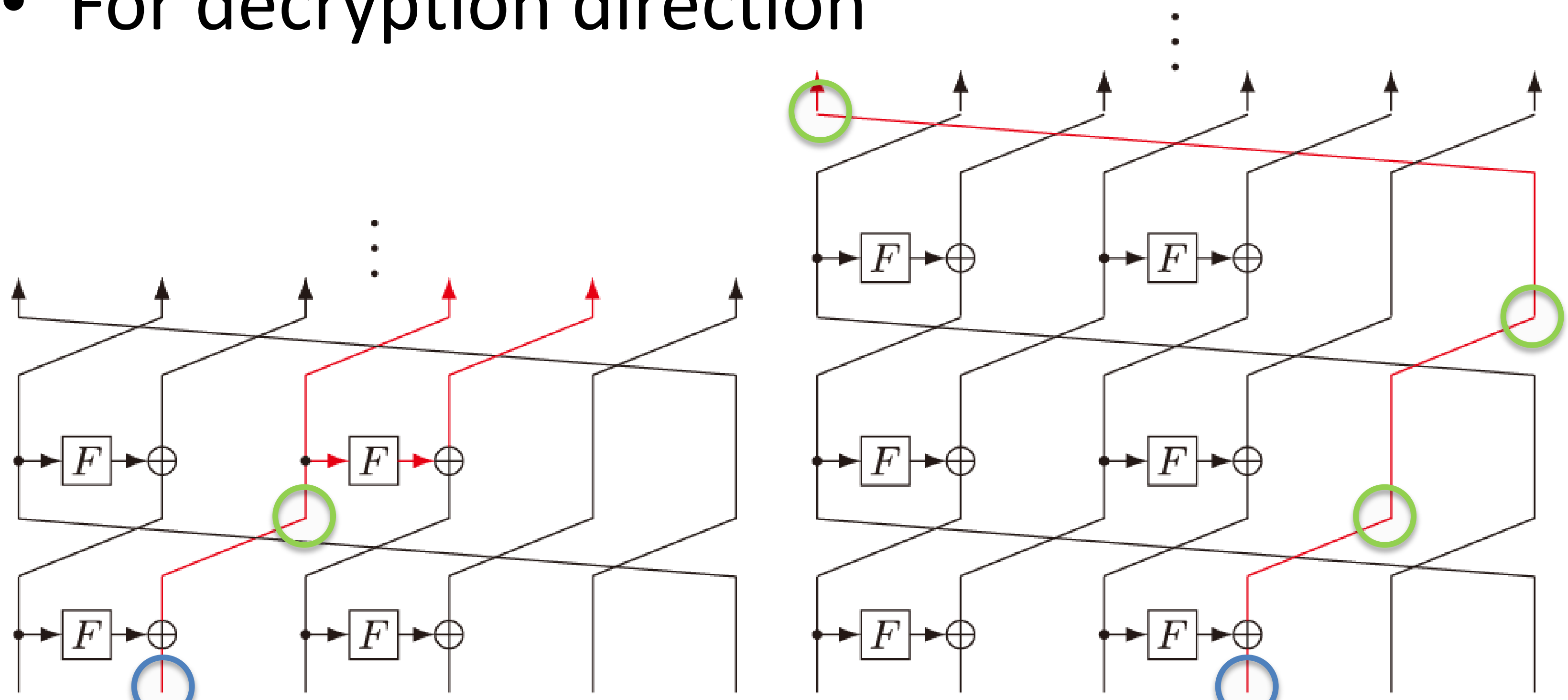
- For encryption



$$\mathrm{DRmax}_{\mathrm{E},d-1}^{(d,\eta)}(\pi_s) = 2d - 2\eta$$

Brief overview of the proof

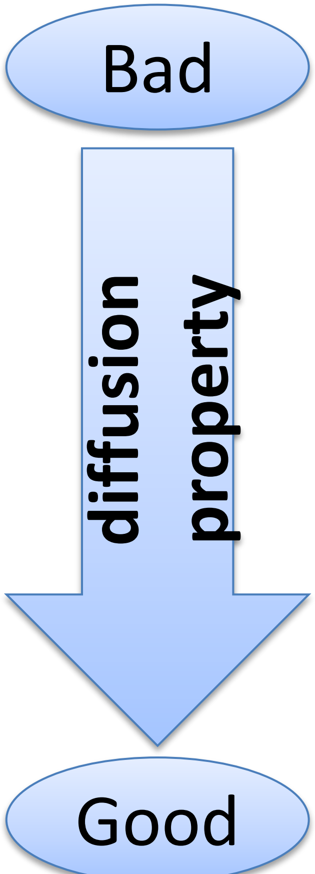
- For decryption direction

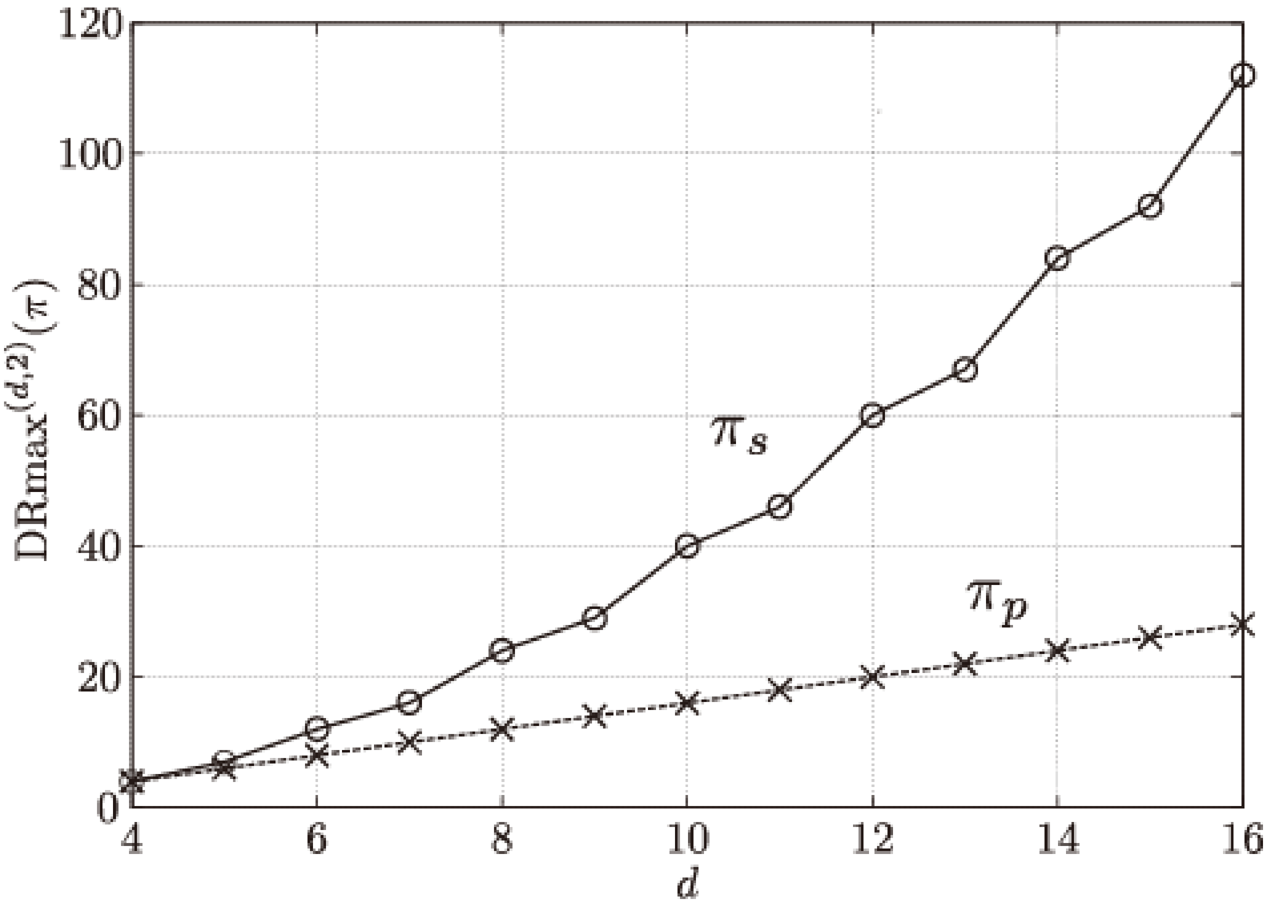


$$\mathrm{DRmax}_{\mathrm{D},2\eta-3}^{(d,\eta)}(\pi_s) \geq 2d - 2\eta \qquad \mathrm{DRmax}_{\mathrm{D},2\eta-1}^{(d,\eta)}(\pi_s) \geq 2d - 2\eta$$

$$\mathrm{DRmax}^{(d,\eta)}(\pi_s) = \max\{\mathrm{DRmax}_{\mathrm{D},2\eta-3}^{(d,\eta)}(\pi_s), \mathrm{DRmax}_{\mathrm{D},2\eta-1}^{(d,\eta)}(\pi_s)\}$$

A comparison of two lemmas





Experimental results

- Compute $\mathrm{DRmax}^{(d,\eta)}(\pi)$ for all $3 \leq d \leq 8$ and $1 \leq \eta \leq \lfloor d/2 \rfloor$.
- List π_s and all optimum permutations in terms of the diffusion property.
- Present only the lexicographically first permutations in the equivalent classes.
- Result for $\eta = 1$ is analyzed in [IEICE 2013]

Result for $\eta = 2$

d	π	DRmax
4	$(1,3,0,2)_p^1$	4
	$(3,0,1,2)_s$	4
5	$(1,3,4,2,0)_p^1$	6
	$(1,4,0,2,3)_p^2$	6
	$(3,0,4,2,1)_s$	7
6	$(1,3,4,2,5,0)_p^1$	8
	$(1,4,0,2,5,3)_p^3$	8
	$(1,4,5,2,3,0)_p^2$	8
	$(3,0,4,2,5,1)_s$	12
	$(3,4,5,0,2,1)$	8
7	$(1,3,4,2,5,6,0)_p^1$	10
	$(1,4,0,2,5,6,3)_p^4$	10
	$(1,4,5,2,3,6,0)_p^2$	10
	$(1,4,5,2,6,0,3)_p^3$	10
	$(3,0,4,2,5,6,1)_s$	16
8	$(1,3,4,2,5,6,7,0)_p^1$	12
	$(1,4,0,2,5,6,7,3)_p^5$	12
	$(1,4,5,2,3,6,7,0)_p^2$	12
	$(1,4,5,2,6,0,7,3)_p^4$	12
	$(1,4,5,2,6,7,3,0)_p^3$	12
	$(3,0,4,2,5,6,7,1)_s$	24

- Subscript
  - s: it is equivalent to π_s .
  - p: it is equivalent to π_p .
- Superscript
  - the integer a for π_p.
- For $d \geq 5$, there are better permutations than π_s .

Result for $\eta = 3$

d	π	DRmax
6	$(1,2,5,0,3,4)$	5 [FSE 2010]
	$(3,0,5,2,1,4)_s$	6
7	$(1,2,4,0,5,6,3)$	7
	$(1,2,6,0,5,3,4)$	7
	$(2,0,5,6,3,4,1)$	7
	$(3,0,1,5,6,4,2)$	7
	$(3,0,5,2,6,4,1)_s$	9
8	$(1,2,4,0,5,6,7,3)$	9
	$(1,2,6,0,5,3,7,4)$	9
	$(1,2,6,0,5,7,4,3)$	9
	$(1,2,6,7,3,4,5,0)$	9
	$(1,3,5,4,6,7,0,2)$	9
	$(1,3,6,4,7,2,5,0)$	9
	$(1,3,6,5,7,4,0,2)$	9
	$(1,3,6,7,2,4,0,5)$	9
	$(1,6,0,4,7,2,5,3)$	9

d	π	DRmax
8	$(1,6,0,5,7,4,3,2)$	9
	$(1,6,0,7,2,4,3,5)$	9
	$(1,6,0,7,3,2,5,4)$	9
	$(1,6,5,0,7,4,2,3)$	9
	$(2,0,5,4,6,7,3,1)$	9
	$(2,0,5,6,3,4,7,1)$	9
	$(2,0,5,6,3,7,4,1)$	9
	$(2,4,5,6,3,0,7,1)$	9
	$(3,0,1,5,6,4,7,2)$	9
	$(3,0,1,6,7,4,5,2)$	9
	$(3,0,5,2,6,4,7,1)_s$	13
	$(3,2,6,5,7,4,1,0)$	9
	$(3,4,1,5,6,0,7,2)$	9
	$(3,4,1,6,7,2,0,5)$	9
	$(3,4,5,6,7,0,2,1)$	9
	$(3,5,1,6,7,4,0,2)$	9

- Permutations in green are analyzed in [FSE 2010].

Result for $\eta = 4$

d	π	DRmax
8	$(1,2,4,0,7,6,5,3)$	6
	$(1,2,5,0,3,6,7,4)$	6 [FSE 2010]
	$(1,2,5,6,7,4,3,0)$	6 [FSE 2010]
	$(1,2,5,7,3,0,4,6)$	6
	$(1,3,5,6,7,4,0,2)$	6
	$(1,3,5,7,0,2,4,6)$	6
	$(2,4,7,5,1,0,3,6)$	6
	$(3,0,1,4,7,2,5,6)$	6 [FSE 2010]
	$(3,0,5,2,7,4,1,6)_s$	8

- Some permutations do not exist in [FSE 2010] results.
  - Because [FSE 2010] paper observed “even-odd shuffles”. (instead of all permutations)

Conclusion

- Proposed Type 1.x GFS
  - covers Type 1 and Type 2 GFSs
- Proposed a construction π_p for Type 1.x GFS
- Analysis of Type 1.x GFS with π_s
  - compared π_p to π_s in terms of the diffusion property
- Showed experimental results for Type 1.x GFS for $3 \leq d \leq 8$

Future work

- Analyze the security against various attacks
  - differential, linear, impossible differential, and saturation attacks
- Design optimum permutations for $\eta \geq 3$.