General Diffusion Analysis: How to Find Optimal Permutations for Generalized Type-II Feistel Schemes

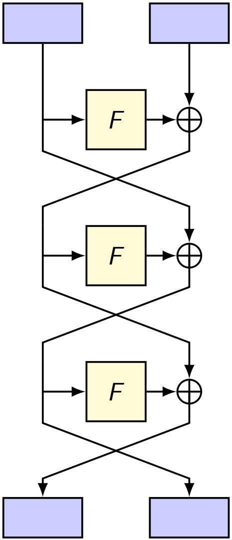
Victor Cauchois[1,2], Clément Gomez[1], Gaël Thomas[1]

[1]DGA Maitrise de l'Information, Bruz, France

[2]IRMAR, Université de Rennes 1, Rennes, France

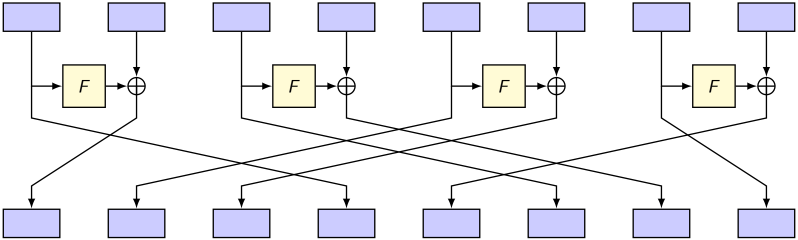
Fast Software Encryption — 2019-03-26 — Paris, France

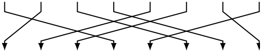
The Feistel Network



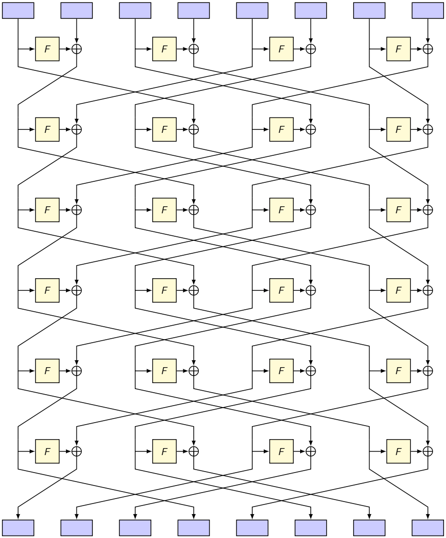
- How to construct a permutation?
- Challenging task
- Split the problem in half and iterate
- DES, Camellia, Simon, . . .

Type-II Generalized Feistel Structure (GFS)

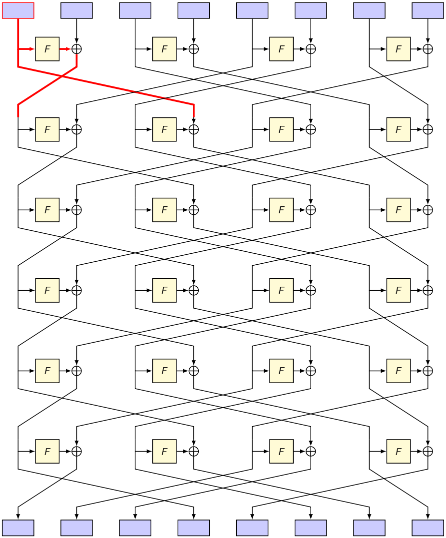


- Split into k blocks
- $k/2$ parallel mini-Feistel functions F (easier to design)
- Then a block-wise permutation $\pi \in \mathcal{S}_k$: 
- CLEFIA ($k = 4$), Simpara ($k = 4, 6, 8$), TWINE ($k = 16$)
- Problem: Diffusion needs more rounds

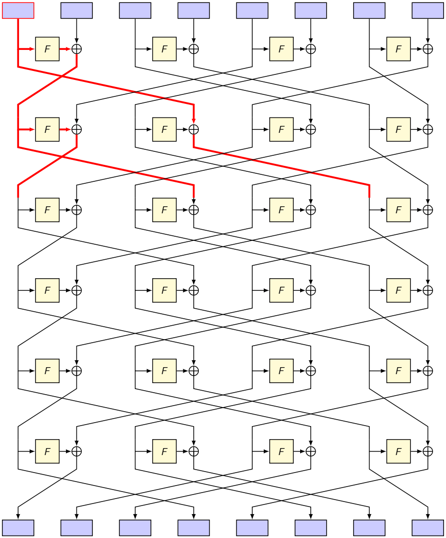
Maximum Diffusion Round (DR)



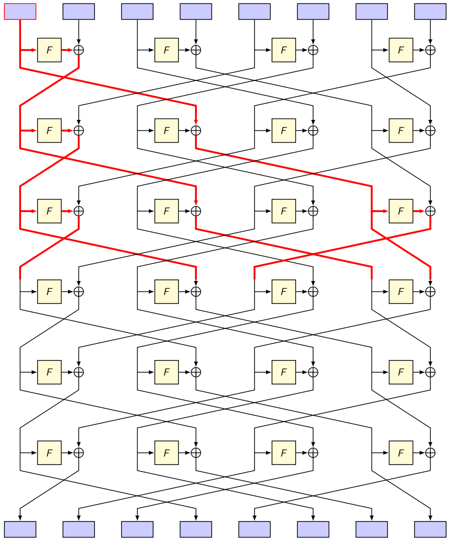
Maximum Diffusion Round (DR)



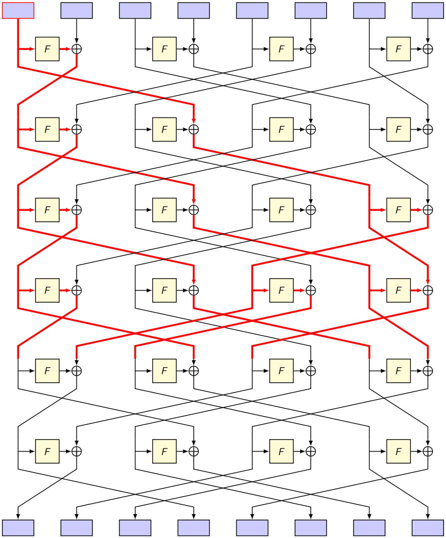
Maximum Diffusion Round (DR)



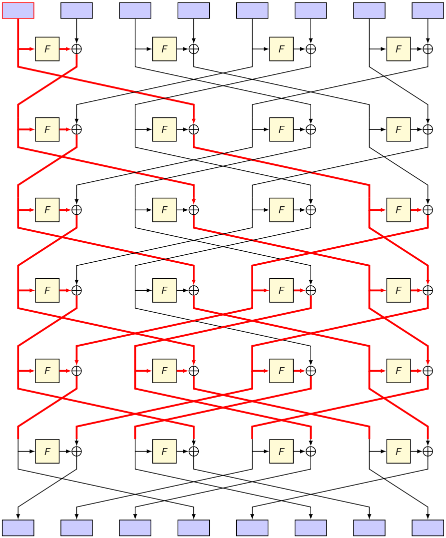
Maximum Diffusion Round (DR)



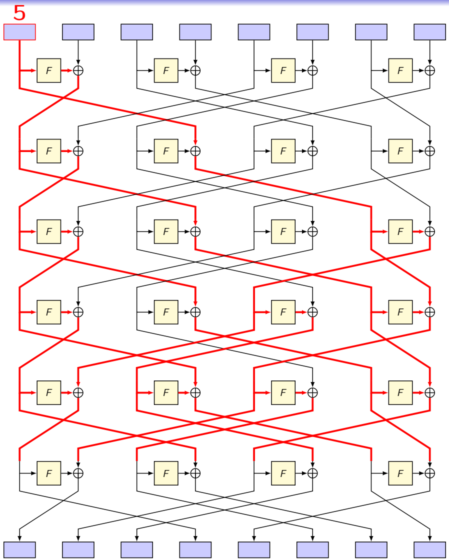
Maximum Diffusion Round (DR)



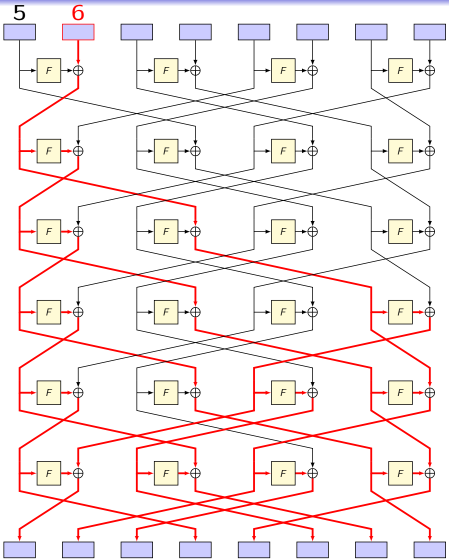
Maximum Diffusion Round (DR)



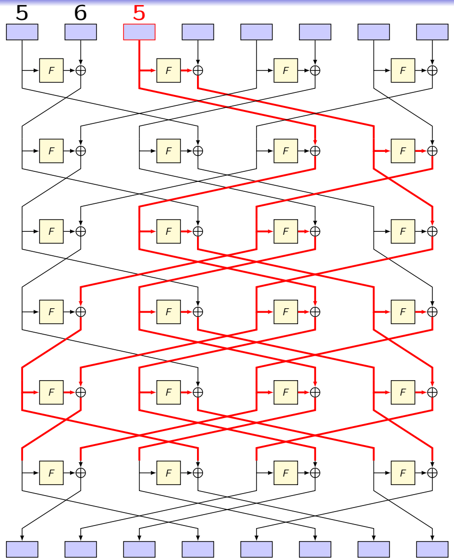
Maximum Diffusion Round (DR)



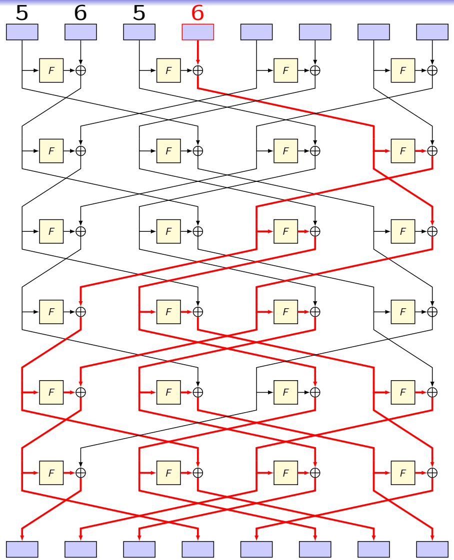
Maximum Diffusion Round (DR)



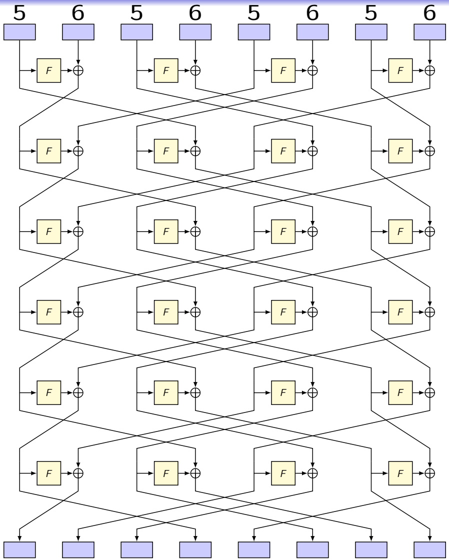
Maximum Diffusion Round (DR)



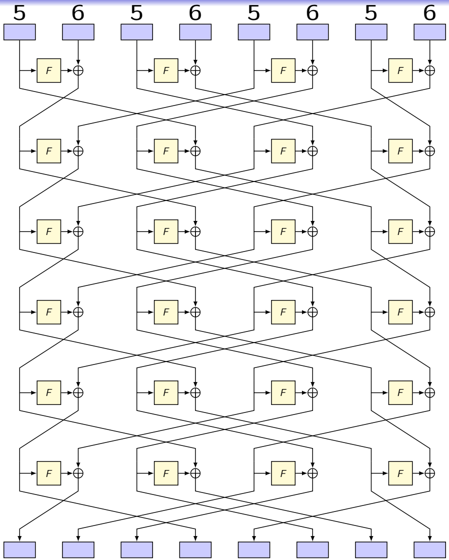
Maximum Diffusion Round (DR)



Maximum Diffusion Round (DR)

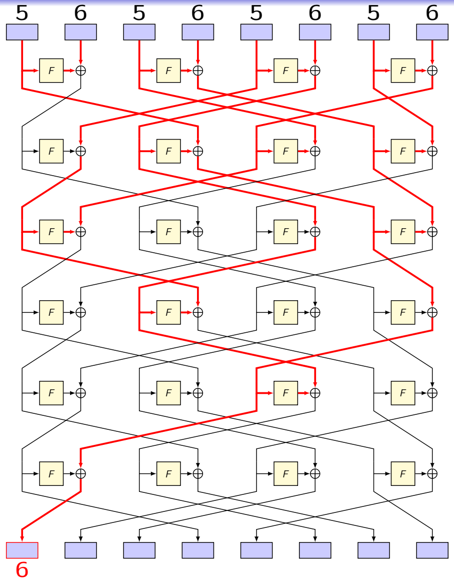


Maximum Diffusion Round (DR)



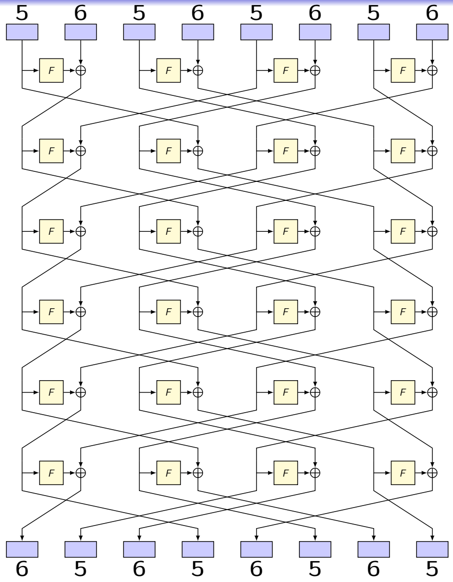
- Simple criterion
- Depends only on the permutation π
- Link with impossible differential and saturation attacks
- Encryption

Maximum Diffusion Round (DR)



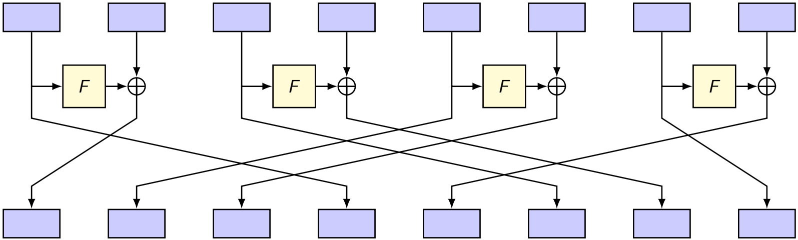
- Simple criterion
- Depends only on the permutation π
- Link with impossible differential and saturation attacks
- Encryption
  AND
  Decryption

Maximum Diffusion Round (DR)



- Simple criterion
- Depends only on the permutation π
- Link with impossible differential and saturation attacks
- Encryption
  AND
  Decryption
- here $DR(\pi) = 6$

Previous Works



- Suzaki and Minematsu, FSE 2010
- Focus on even-odd GFS ($\mathcal{S}_k^{eo}$)
- Exhaustive search for $k \leq 16$ blocks
- Power of two case : generic construction in $DR(\pi) = 2\log_2 k$

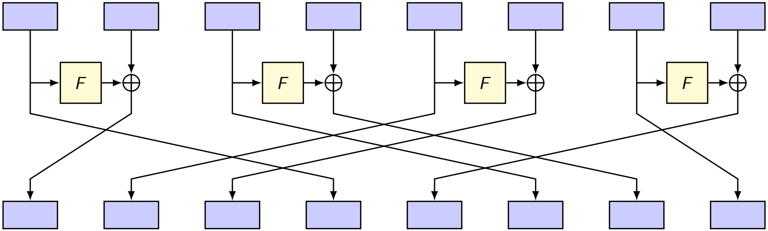
k	DR(rot)	min $DR(\pi)$
4	4	4
6	6	5
8	8	6
10	10	7
12	12	8
14	14	8
16	16	8

Our Contributions

- Constructive upper-bound on the number of even-odd GFS up to equivalence
- Exhaustive search for $k \leq 24$
- New criterion to reduce search space: Collision-free depth
- Power of two case: new permutations based on graph coloring
- Case of non even-odd permutations

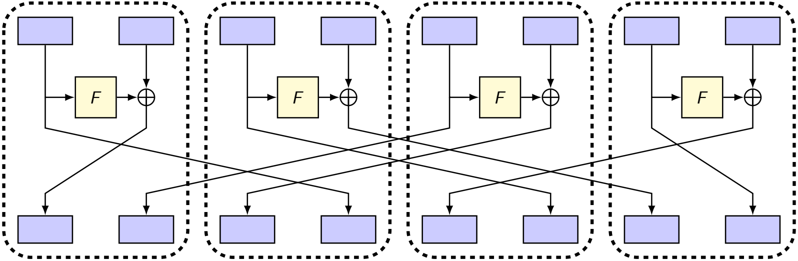
k	[SM10]	this paper
4	4	4
6	5	5
8	6	6
10	7	7
12	8	8
14	8	8
16	8	8
18		8
20		9
22		8
24		9
26		9
32	10	10
64	12	11
128	14	13

Equivalence of GFS



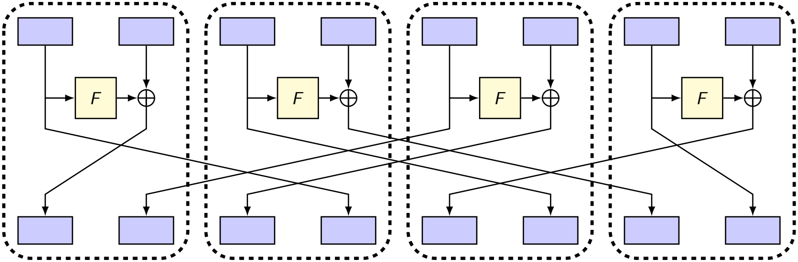
- Equivalence up to block reindexing

Equivalence of GFS



- Equivalence up to block reindexing
- Permutations of pairs: swap blocks in a pair-wise manner

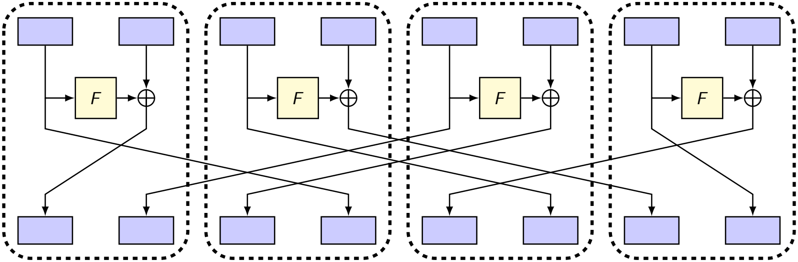
Equivalence of GFS



- Equivalence up to block reindexing
- Permutations of pairs: swap blocks in a pair-wise manner

$$\mathcal{S}_k^p := \{\varphi \in \mathcal{S}_k | \forall i \leq \frac{k}{2} - 1,\ \varphi(2i) \text{ is even and } \varphi(2i+1) = \varphi(2i) + 1\}$$

Equivalence of GFS



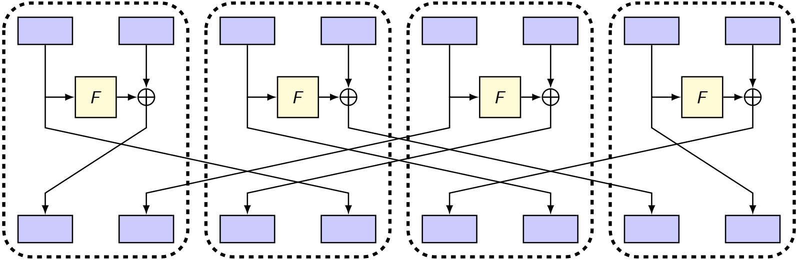
- Equivalence up to block reindexing
- Permutations of pairs: swap blocks in a pair-wise manner

$$\mathcal{S}_k^p := \{\varphi \in \mathcal{S}_k | \forall i \leq \frac{k}{2} - 1,\ \varphi(2i) \text{ is even and } \varphi(2i+1) = \varphi(2i)+1\}$$

- "Pair-equivalence": $\mathcal{S}_k^p$ acts on $\mathcal{S}_k$ by conjugation

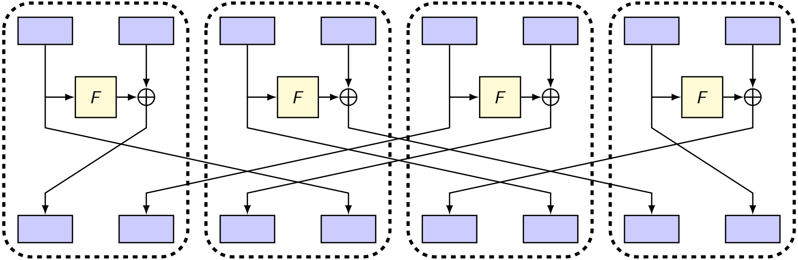
$$\pi_1 \equiv \pi_2 \text{ iff } \exists \varphi \in \mathcal{S}_k^p \text{ s.t. } \pi_1 = \varphi \circ \pi_2 \circ \varphi^{-1}$$

Number of Even-odd GFS up to Pair-equivalence



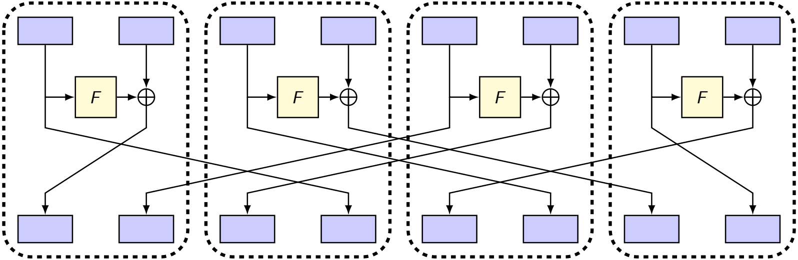
Bijection: $\begin{cases} \mathcal{S}_{k/2} \times \mathcal{S}_{k/2} \rightarrow \mathcal{S}_k^{eo} \text{ (even-odd GFS)} \end{cases}$

Number of Even-odd GFS up to Pair-equivalence



Bijection: $\begin{cases} \mathcal{S}_{k/2} \times \mathcal{S}_{k/2} & \rightarrow & \mathcal{S}_k^{eo} \text{ (even-odd GFS)} \\ (\pi_1, \pi_2) & \mapsto & \pi \text{ s.t.} \left| \begin{array}{l} \pi(2i) = 2\pi_1(i) + 1 \\ \pi(2i+1) = 2\pi_2(i) \end{array} \right. \end{cases}$

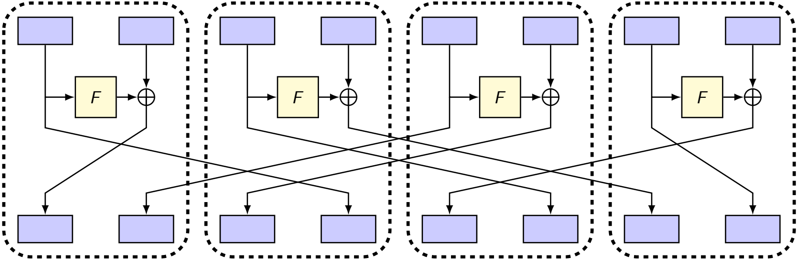
Number of Even-odd GFS up to Pair-equivalence



Bijection: $\begin{cases} \mathcal{S}_{k/2} \times \mathcal{S}_{k/2} & \rightarrow & \mathcal{S}_k^{eo} \text{ (even-odd GFS)} \\ (\pi_1, \pi_2) & \mapsto & \pi \text{ s.t. } \left| \begin{array}{l} \pi(2i) = 2\pi_1(i) + 1 \\ \pi(2i+1) = 2\pi_2(i) \end{array} \right. \end{cases}$

$$(k/2)! \leq \text{ number of classes } \leq \qquad (k/2)!^2$$

Number of Even-odd GFS up to Pair-equivalence

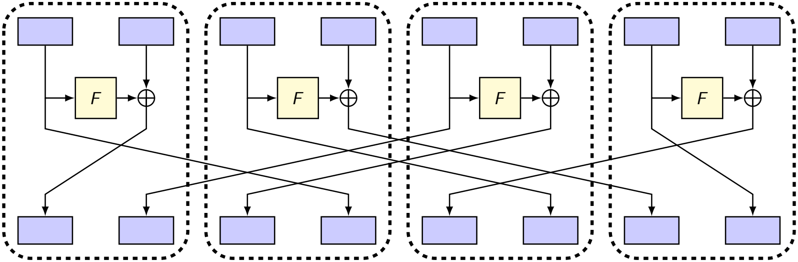


Bijection: $\begin{cases} \mathcal{S}_{k/2} \times \mathcal{S}_{k/2} & \to & \mathcal{S}_k^{eo} \text{ (even-odd GFS)} \\ (\pi_1, \pi_2) & \mapsto & \pi \text{ s.t. } \left| \begin{array}{l} \pi(2i) = 2\pi_1(i) + 1 \\ \pi(2i+1) = 2\pi_2(i) \end{array} \right. \end{cases}$

Idea Only enumerate a single π_1 for each conjugacy class in $\mathcal{S}_{k/2}$ w.r.t regular conjugation

$$(k/2)! \leq \text{ number of classes } \leq (k/2)!^2$$

Number of Even-odd GFS up to Pair-equivalence

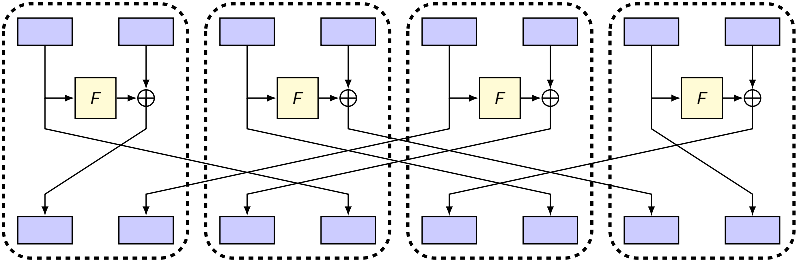


Bijection: $\begin{cases} \mathcal{S}_{k/2} \times \mathcal{S}_{k/2} & \rightarrow & \mathcal{S}_k^{eo} \text{ (even-odd GFS)} \\ (\pi_1, \pi_2) & \mapsto & \pi \text{ s.t.} \left| \begin{array}{l} \pi(2i) = 2\pi_1(i) + 1 \\ \pi(2i+1) = 2\pi_2(i) \end{array} \right. \end{cases}$

Idea Only enumerate a single π_1 for each conjugacy class in $\mathcal{S}_{k/2}$ w.r.t regular conjugation

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

Number of Even-odd GFS up to Pair-equivalence



$$\text{Bijection:} \begin{cases} \mathcal{S}_{k/2} \times \mathcal{S}_{k/2} & \rightarrow \quad \mathcal{S}_k^{eo} \text{ (even-odd GFS)} \\ (\pi_1, \pi_2) & \mapsto \quad \pi \text{ s.t.} \left| \begin{array}{l} \pi(2i) = 2\pi_1(i) + 1 \\ \pi(2i+1) = 2\pi_2(i) \end{array} \right. \end{cases}$$

Idea Only enumerate a single π_1 for each conjugacy class in $\mathcal{S}_{k/2}$ w.r.t regular conjugation

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

- Number of conjugacy class in $\mathcal{S}_{k/2}$: $N_{k/2} = \mathcal{O}(e^{\pi\sqrt{k/3}})$

Exhaustive search of Optimal Even-odd GFS

k		min $DR(\pi)$	Number of classes
6		5	1
8		6	2
10		7	3
12		8	32
14		8	23
16		8	13
18		8	2
20		9	2133
22		8	4
24		9	56

Exhaustive search of Optimal Even-odd GFS

k		$\min DR(\pi)$	Number of classes
6		5	1
8		6	2
10		7	3
12		8	32
14		8	23
16		8	13
18		8	2
20		9	2133
22		8	4
24		9	56

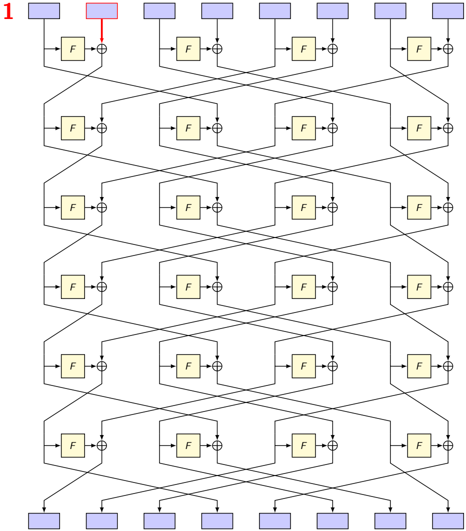
- What happens with $k = 18$, 20 and 22?

Exhaustive search of Optimal Even-odd GFS

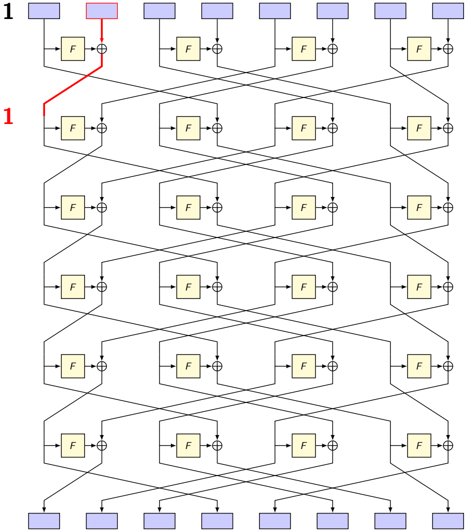
k	lower bound	min $DR(\pi)$	Number of classes
6	5	5	1
8	6	6	2
10	6	7	3
12	7	8	32
14	7	8	23
16	7	8	13
18	8	8	2
20	8	9	2133
22	8	8	4
24	8	9	56

- What happens with $k = 18$, 20 and 22? $\longrightarrow$ lower bound

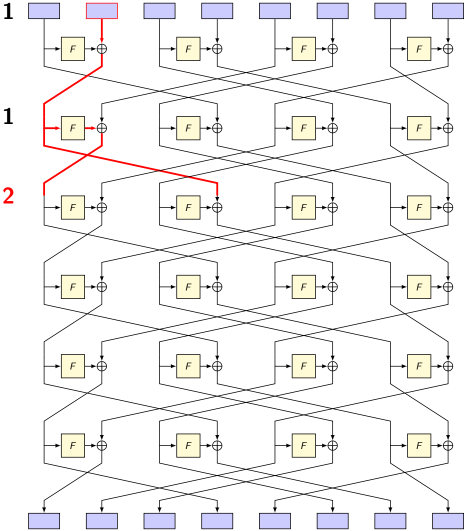
Lower Bound on the Diffusion Round of Type-II GFS



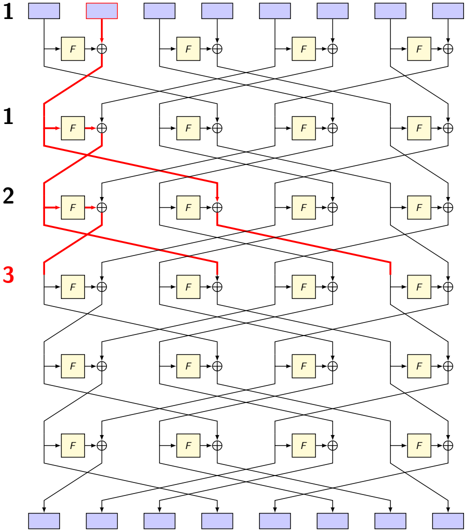
Lower Bound on the Diffusion Round of Type-II GFS



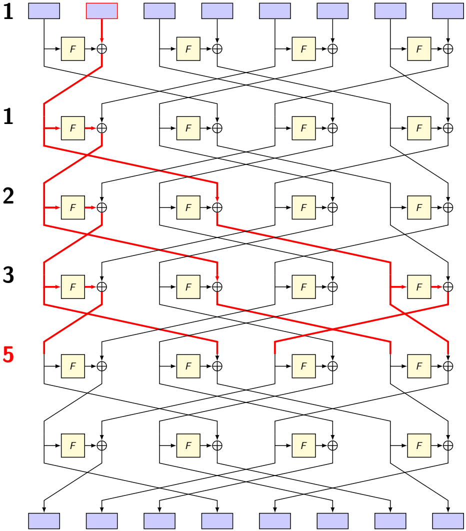
Lower Bound on the Diffusion Round of Type-II GFS



Lower Bound on the Diffusion Round of Type-II GFS

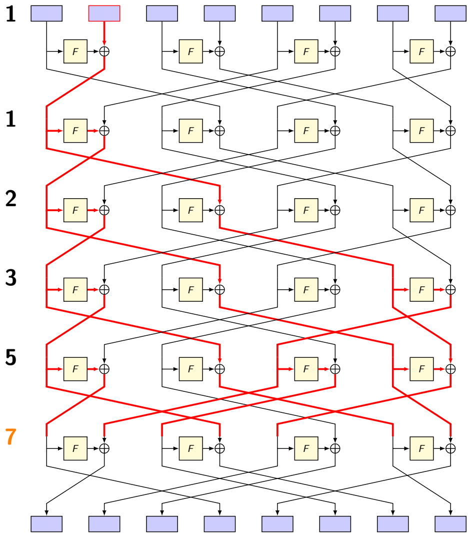


Lower Bound on the Diffusion Round of Type-II GFS



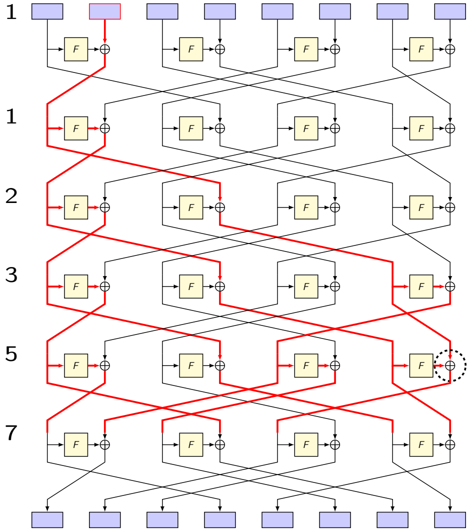
- Fibonacci Sequence

Lower Bound on the Diffusion Round of Type-II GFS



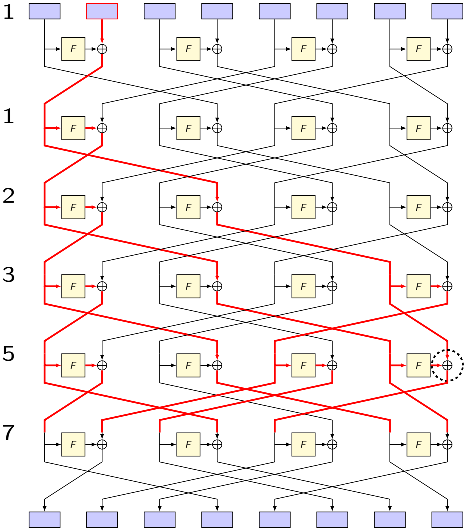
- Fibonacci Sequence

Lower Bound on the Diffusion Round of Type-II GFS



- Fibonacci Sequence
- Until Collision

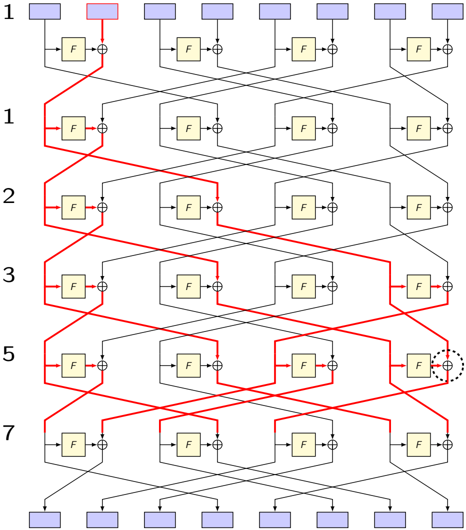
Lower Bound on the Diffusion Round of Type-II GFS



- Fibonacci Sequence
- Until Collision
- Lower Bound: no collision happens

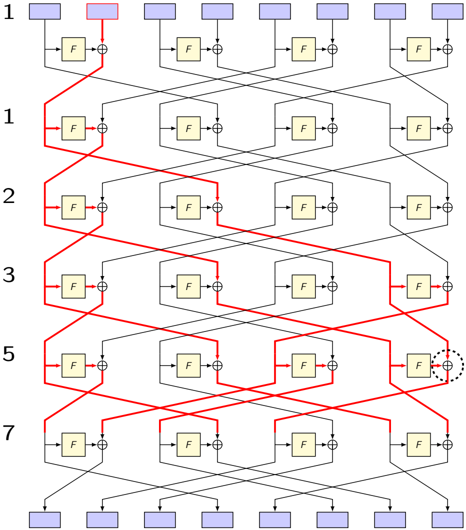
$$2 \cdot Fib(DR(\pi)) \geq k$$

New Idea for finding good GFS



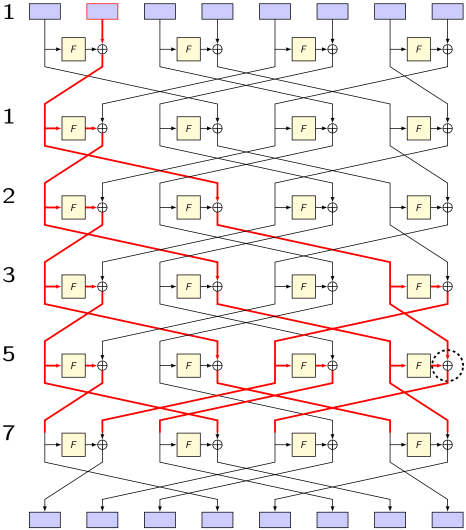
- $k > 26 \longrightarrow$ exhaustive search intractable

New Idea for finding good GFS



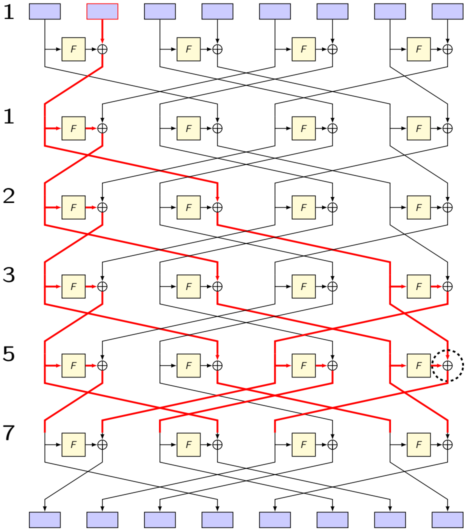
- $k > 26 \longrightarrow$ exhaustive search intractable
- Restrict search space to cases where collisions happen late

New Idea for finding good GFS



- $k > 26 \longrightarrow$ exhaustive search intractable
- Restrict search space to cases where collisions happen late
- New criterion: $CD(\pi)$ Collision-free depth

New Idea for finding good GFS



- $k > 26 \longrightarrow$ exhaustive search intractable
- Restrict search space to cases where collisions happen late
- New criterion: $CD(\pi)$ Collision-free depth
- here $CD(\pi) = 3$

Collision-free Depths of Optimal Even-odd Permutations

k	16		18	20				22	24		
min $DR(\pi)$	8		8	9				8	8		
bound on CD	4		5	5				5	5		
$CD(\pi)$	3	4	3	2	3	4	5	5	3	4	5
$\sharp$ classes	9	4	2	165	1624	340	4	4	19	32	5

- Tradeoff between search space size and number of results

Interresting Case: $k = 26$

- Exhaustive search too expensive

Interresting Case: $k = 26$

- Exhaustive search too expensive
- $2 \cdot Fib(8) = 26$: tight spot for the Fibonacci bound

Interresting Case: $k = 26$

- Exhaustive search too expensive
- $2 \cdot Fib(8) = 26$: tight spot for the Fibonacci bound
- $DR(\pi) = 8 \Rightarrow CD(\pi) = 7$

Interresting Case: $k = 26$

- Exhaustive search too expensive
- $2 \cdot Fib(8) = 26$: tight spot for the Fibonacci bound
- $DR(\pi) = 8 \Rightarrow CD(\pi) = 7$
- Exhaustive search for $CD(\pi) \geq 4$: best $DR(\pi) = 10$

Interresting Case: $k = 26$

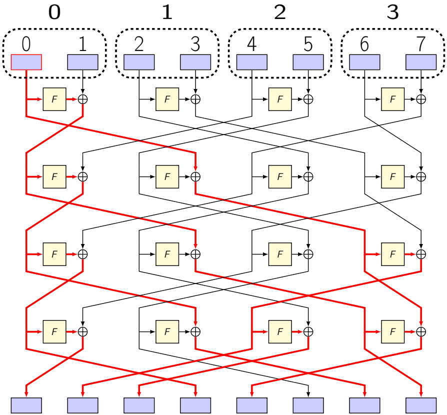
- Exhaustive search too expensive
- $2 \cdot Fib(8) = 26$: tight spot for the Fibonacci bound
- $DR(\pi) = 8 \Rightarrow CD(\pi) = 7$
- Exhaustive search for $CD(\pi) \geq 4$: best $DR(\pi) = 10$
- Random Search for $CD(\pi) = 3$: found $DR(\pi) = 9$

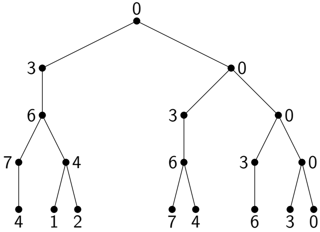
Interresting Case: $k = 26$

- Exhaustive search too expensive
- $2 \cdot Fib(8) = 26$: tight spot for the Fibonacci bound
- $DR(\pi) = 8 \Rightarrow CD(\pi) = 7$
- Exhaustive search for $CD(\pi) \geq 4$: best $DR(\pi) = 10$
- Random Search for $CD(\pi) = 3$: found $DR(\pi) = 9$

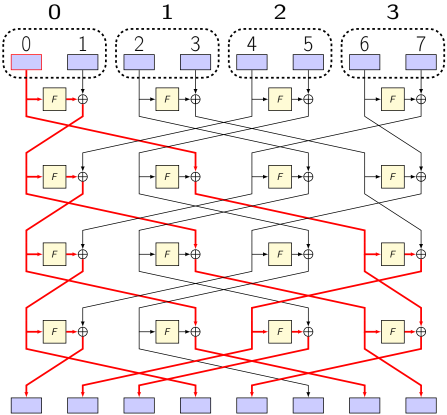
$\Rightarrow$ This MUST be optimal

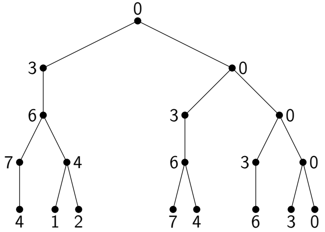
Tree and Block-Tree Representation

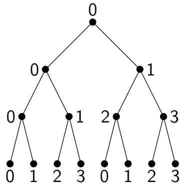




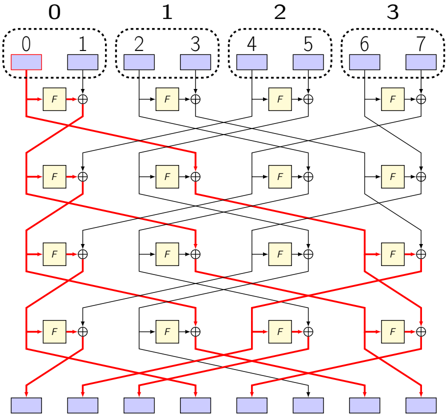
Tree and Block-Tree Representation

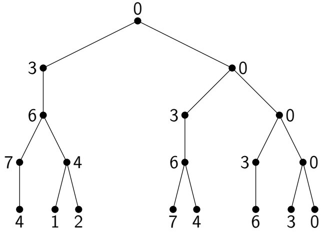


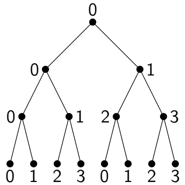




Tree and Block-Tree Representation

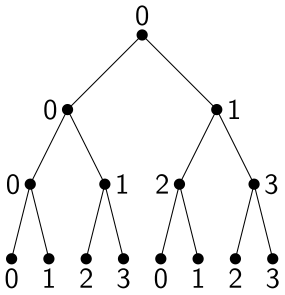






- Grouping blocks by pair is used in [SM10]

Pros and Cons of Block-Tree Representation



Pros:

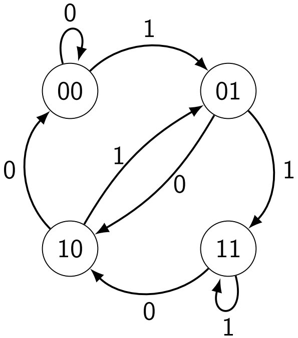
- Balanced Binary Tree
- Fewer nodes
- Simpler structure

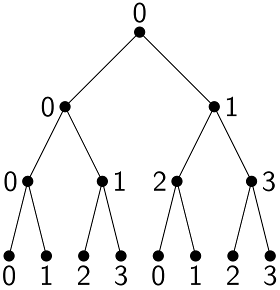
Cons:

- Does not uniquely represent a permutation π
- Where do even and odd nodes go within a block?

$\longrightarrow$ Need to specify it as an edge-colouring

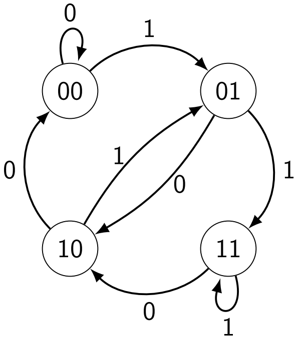
Candidates yielding good GFS?

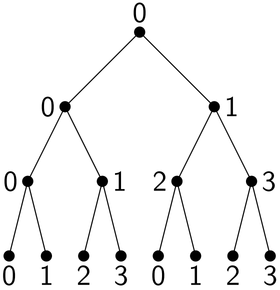




- De Bruijn graph used by [SM10]

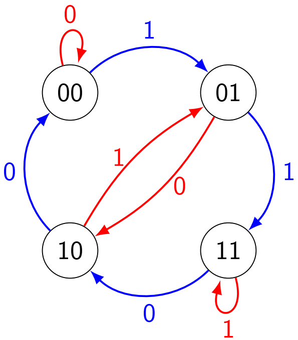
Candidates yielding good GFS?

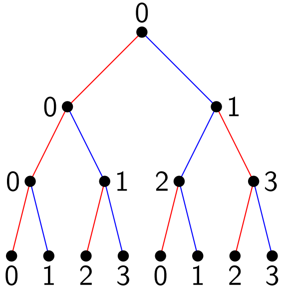




- De Bruijn graph used by [SM10]
- Fill with the least possible value

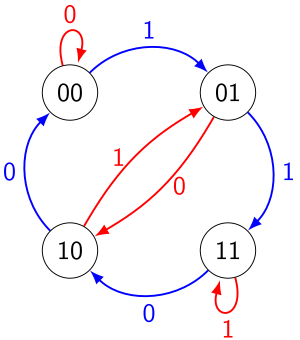
Candidates yielding good GFS?

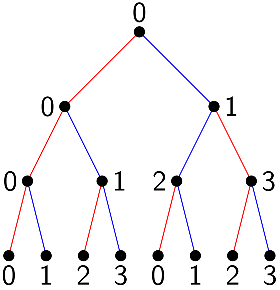




- De Bruijn graph used by [SM10]
- Fill with the least possible value
- Many ways to color the graph
- Exhaust in $\mathcal{O}(2^{k/4})$

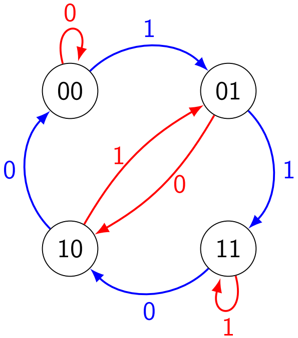
Candidates yielding good GFS?

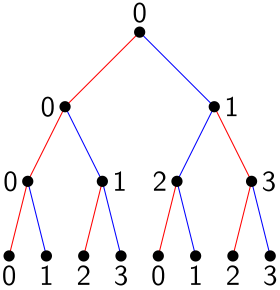




- De Bruijn graph used by [SM10]
- Fill with the least possible value
- Many ways to color the graph
- Exhaust in $\mathcal{O}(2^{k/4})$
- Some may yield better $DR(\pi)$

Candidates yielding good GFS?





- De Bruijn graph used by [SM10]
- Fill with the least possible value
- Many ways to color the graph
- Exhaust in $\mathcal{O}(2^{k/4})$
- Some may yield better $DR(\pi)$

k	[SM10]	this paper
8	6	6
16	8	8
32	10	10
64	12	11
128	14	13

Until now...

- Constructive upper-bound on the number of even-odd GFS up to equivalence
- Exhaustive search for $k \leq 24$
- New criterion to reduce search space: Collision-free depth
- Power of two case: new permutations based on graph coloring
- Case of non even-odd permutations

k	[SM10]	this paper
4	4	4
6	5	5
8	6	6
10	7	7
12	8	8
14	8	8
16	8	8
18		8
20		9
22		8
24		9
26		9
32	10	10
64	12	11
128	14	13

Number of non even-odd Permutations Classes

- Even-odd case

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

Number of non even-odd Permutations Classes

- Even-odd case

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

- General case

$$\frac{k!}{(k/2)!} \leq \text{ number of classes } \leq N_k \cdot \frac{k!}{(k/2)!}$$

Number of non even-odd Permutations Classes

- Even-odd case

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

- General case

$$\frac{k!}{(k/2)!} \leq \text{ number of classes } \leq N_k \cdot \frac{k!}{(k/2)!}$$

- N_k: Conjugacy class representatives

Number of non even-odd Permutations Classes

- Even-odd case

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

- General case

$$\frac{k!}{(k/2)!} \leq \text{ number of classes } \leq N_k \cdot \frac{k!}{(k/2)!}$$

- N_k: Conjugacy class representatives
- $\frac{k!}{(k/2)!}$: Right-coset representatives of $\mathcal{S}_k \mod \mathcal{S}_k^p$

Number of non even-odd Permutations Classes

- Even-odd case

$$(k/2)! \leq \text{ number of classes } \leq N_{k/2} \cdot (k/2)!$$

- General case

$$\frac{k!}{(k/2)!} \leq \text{ number of classes } \leq N_k \cdot \frac{k!}{(k/2)!}$$

- N_k: Conjugacy class representatives
- $\frac{k!}{(k/2)!}$: Right-coset representatives of $\mathcal{S}_k \mod \mathcal{S}_k^p$
- Exhaustive search $k \leq 20$: no result better than even-odds

Conclusion

- Study of type-II Generalized Feistel Structures
- Permutations up to pair-equivalence
- Constructive upper-bound
- Exhaustive search up to $k \leq 24$ (even-odd) or $k \leq 20$ (general)
- Permutations with no collision in the early rounds
- Improved Results for $k = 64$ and 128

Thank you for your attention.

Do you have any questions?