New Algorithm for Exhausting Optimal Permutations for Generalized Feistel Networks

Stéphanie Delaune Patrick Derbez **Arthur Gontier** Charles Prud'homme

14 mars 2023

Context : Feistel schemes

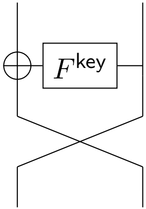
Symmetric Block cipher :

$$(X_0, X_1) \rightarrow (X_1, X_0 \oplus F(X_1))$$

1977 - DES Data Encryption Standard

1989 - Type 2 Generalized Feistel Networks

1996 - GFN with a permutation π



In the following F will be considered as an arbitrary SBox

Feistel schemes

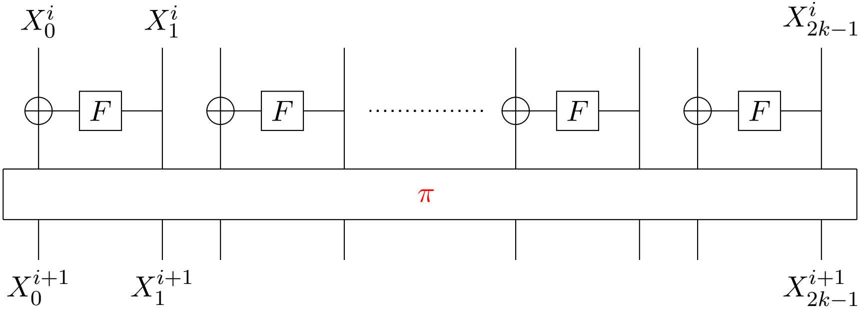


Figure – Round function $\mathcal{R}_i$ of a GFN with k Feistel pairs

$$(X_0^i, X_1^i, \ldots, X_{2k-1}^i) \rightarrow \pi(X_0^i \oplus F_0^i(X_1^i), X_1^i, \ldots, X_{2k-2}^i \oplus F_{k-1}^i(X_{2k-1}^i), X_{2k-1}^i)$$

Diffusion round

Definition (Diffusion round)

$DR(\pi)$ is the minimum number of rounds R such that all X_i^0 fully diffuses after R rounds.

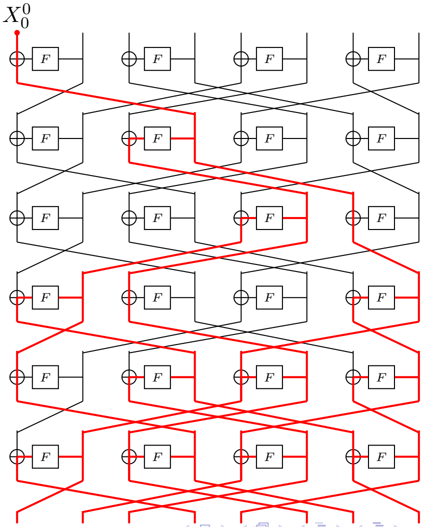
Find the "best" permutation :

2010 - Diffusion round studies

$\hookrightarrow$ impossible differential attacks

2019 - Focus on even-odd permutations

NEW- General Graph algorithm



Even-odd permutation

Definition (even-odd permutation)

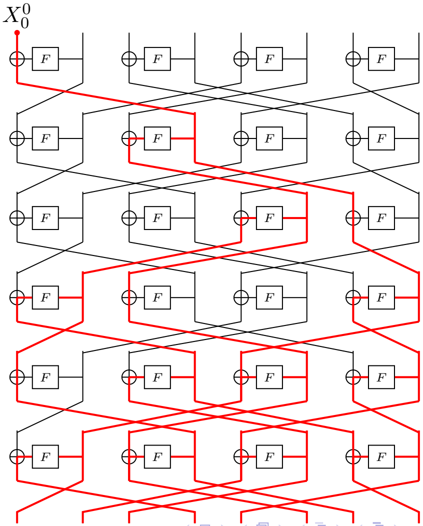
A permutation π where the even blocks go to odd ones and odd blocks to even ones

Example : $\pi = (3, 0, 5, 6, 1, 2, 7, 4)$

Properties :

Can double each 2 round

$\hookrightarrow$ Lower bound : Fibonacci suite



Problem :

Enumerate all the permutations with the optimal diffusion round.

Example : The diffusion round of the cycle shift for 32 blocks is 32 rounds (optimal DR is 9)

Even-odd complexity :

Enumerate 2 sides : $(k!)^2$

Enumerate partitions : $k!\mathcal{N}_k$

General case complexity :

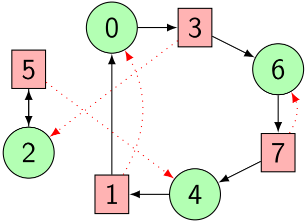
Enumerate permutations : $(2k)!$

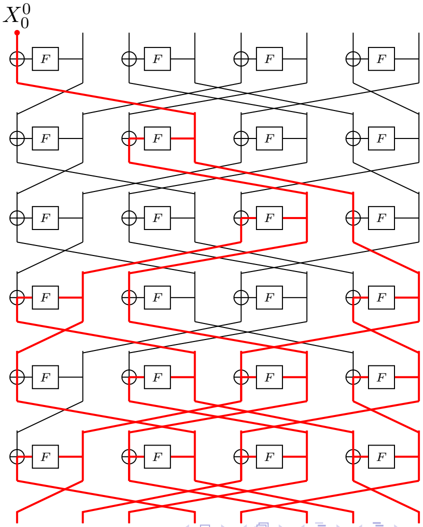
NEW : $\tilde{k}!\sum_{i=0}^{k}\mathcal{N}_i \times \mathcal{N}_{k-i}$

New approach

Previous methods : Build the diffusion trees of each block in the cipher

NEW : Build a graph with paths $\pi = (3, 0, 5, 6, 1, 2, 7, 4)$:





Proof by enumeration : The even-odd permutations are optimal up to $2k = 32$ blocks

20 blocks :

"$2^{46.4}$ DR tests"

$\rightarrow$ 8 sec

32 blocks :

$\rightarrow$ 8 hours

$2k$	Fibonacci bound	even-odd DR	even-odd Ref	non-even-odd DR	non-even-odd Ref
6	5	5	Suzaki10	6	Suzaki10
8	6	6		6	
10	6	7		7	
12	7	8		8	
14	7	8		8	
16	7	8		8	
18	8	8	Cauchois19	9	Cauchois19
20	8	9		9	
22	8	8		9	NEW
24	8	9		≥ 9	
26	8	9	Derbez19	≥ 9	
28	9	9		≥ 9	
30	9	9		≥ 9	
32	9	9		≥ 9	

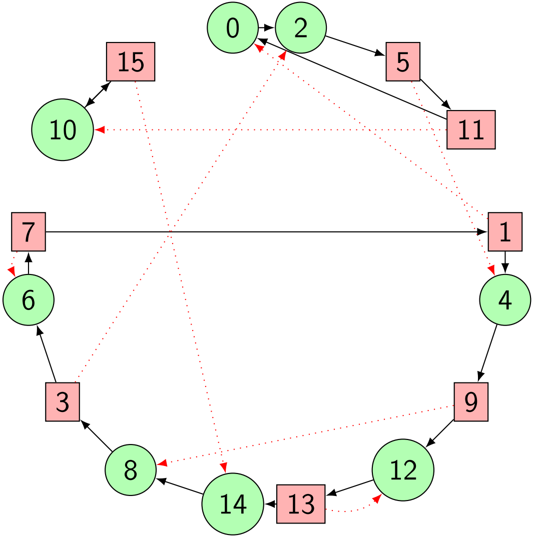
Summary

1. Graph representation of GFN
2. Path building Algorithm
   - Example
   - Symmetries and Skeletons
3. Results
   - Non-even-odd
   - Even-odd
4. Conclusion

Section Summary

1. Graph representation of GFN
2. Path building Algorithm
   - Example
   - Symmetries and Skeletons
3. Results
   - Non-even-odd
   - Even-odd
4. Conclusion

Graph representation of a Feistel permutation



Legend :

- odd blocks
- even blocks
- permutation
- S-Boxes

New Properties

Corollary ($DR(\pi) = R$)

$\forall\ u, v \in V$, *there exists a path of length* R *from* u *to* v*.*

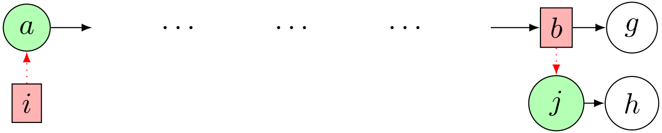
New Properties

Corollary ($DR(\pi) = R$)

$\forall\ u, v \in V$, *there exists a path of length* R *from* u *to* v.

Proposition ($DR(\pi) = R$)

$\forall a \in$ , $\forall b \in$  , *there exists a path of length* $R - 1$ *from* a *to* b.



Even-odd properties

We extend the even-odd property for $R - 1$ rounds in Derbez19.

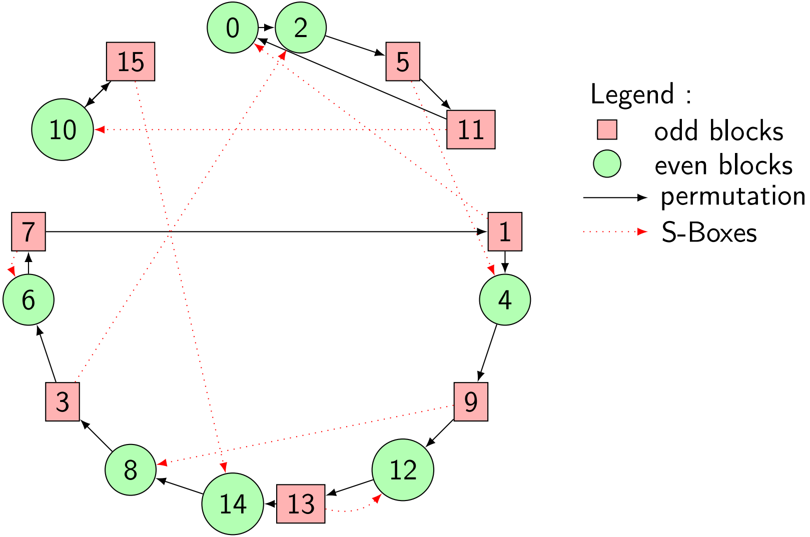
Proposition ($DR(\pi) = R$ and π is even-odd)

$\forall c \in$ □ , $\forall d \in$ ○ , *there exists a path of length* $R - 3$ *from* c *to* d.

Section Summary

1. Graph representation of GFN
2. Path building Algorithm
   - Example
   - Symmetries and Skeletons
3. Results
   - Non-even-odd
   - Even-odd
4. Conclusion

GOAL : build this permutation graph by adding paths

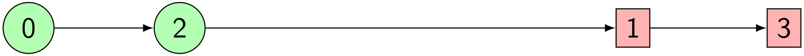


Example : $(DR = 5)$

Paths of length 4 :

0 to 3 ?

Example : $(DR = 5)$



Paths of length 4 :

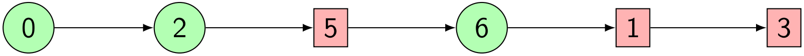
0 to 3 Fail

Example : $(DR = 5)$

Paths of length 4 :

0 to 3 ?

Example : $(DR = 5)$



Paths of length 4 :

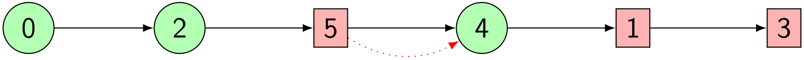
0 to 3 Fail

Example : $(DR = 5)$

Paths of length 4 :

0 to 3 Ok

Example : $(DR = 5)$

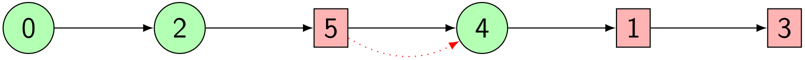


Paths of length 4 :

0 to 3 Ok

0 to 1 Ok

Example : $(DR = 5)$



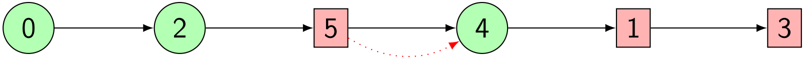
Paths of length 4 :

0 to 3 Ok

0 to 1 Ok

2 to 3 Ok

Example : $(DR = 5)$



Paths of length 4 :

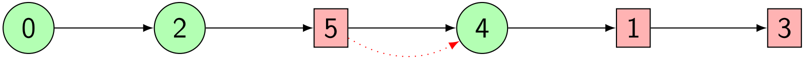
0 to 3 Ok

0 to 1 Ok

2 to 3 Ok

2 to 1 Fail

Example : $(DR = 5)$



Paths of length 4 :

0 to 3 Ok

0 to 1 Ok

2 to 3 Ok

2 to 1 Fail

No π with $DR = 5$

Makepath Algorithm

Fail early for fast enumeration

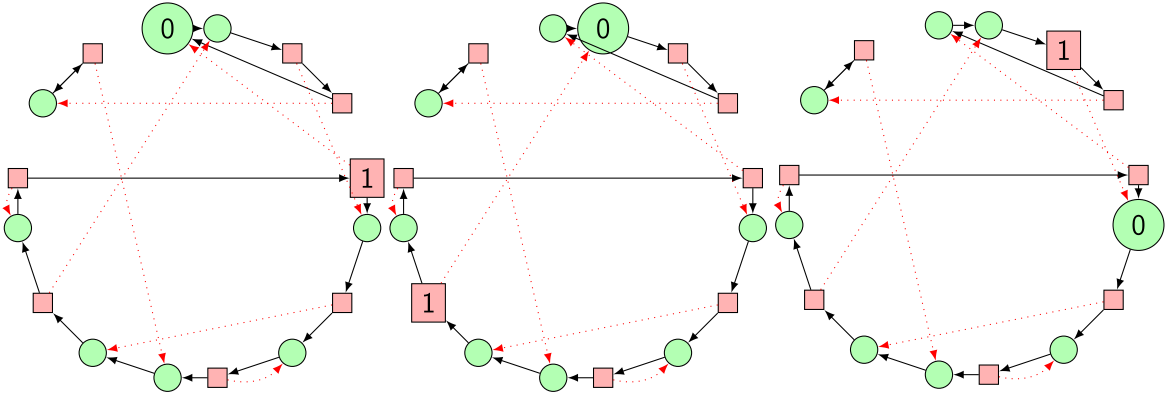
Strategy : start by the hard paths

- Dynamic : evaluate current graph
- Static : exploit the starting structure

Symmetries : prevent similar π

- Starting structure in the general case ?

Symmetries : pair renumbering



Break symmetries : even-odd : ϵ-Cycles

Definition (ϵ-cycle)

An ϵ-cycle is a path $c = (e_1, \ldots, e_{2l})$ in which the first and last nodes are equal and edges alternate between $\longrightarrow$ and $\dashrightarrow$.

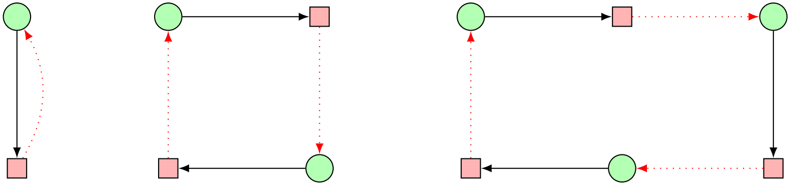


Figure – 1-ϵ-cycle, 2-ϵ-cycle, and 3-ϵ-cycle

Break symmetries : non-even-odd : ϵ-Chains

Definition (ϵ-chain)

An ϵ-chain is a path $ch = (e_1, \ldots, e_{2l+1})$ in which the two first nodes are □ and the two last nodes are ○. The edges alternate between $\longrightarrow$ and $\dashrightarrow$.

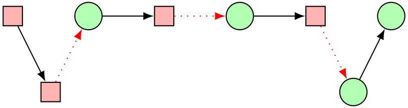


Figure – A 3-ϵ-chain.

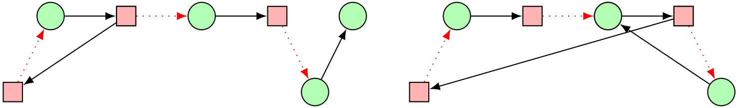
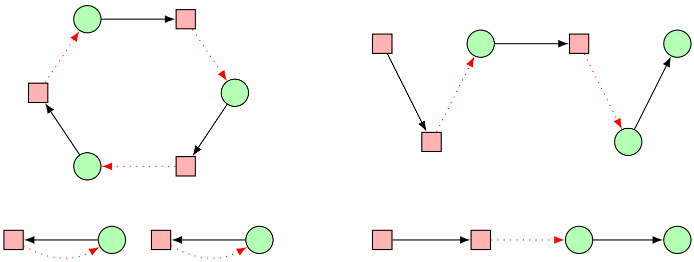


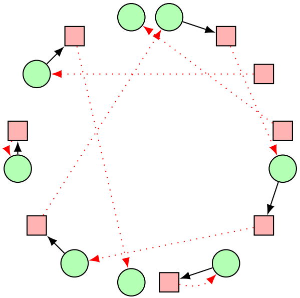
Figure – Two 3-ϵ-chains looping on themselves.

Skeletons

Definition

A <u>skeleton</u> of size k is a set of ϵ-cycles and ϵ-chains whose sum of sizes is k.

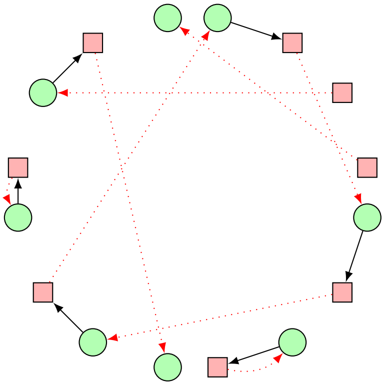




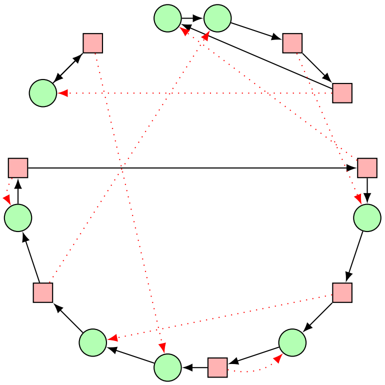
$\sum_{i=0}^{k} \mathcal{N}_i \times \mathcal{N}_{k-i}$

$\rightarrow$ Static strategy : start by small ϵ-chains then small ϵ-cycles

Skeletons



Paths Algo →



Section Summary

1. Graph representation of GFN
2. Path building Algorithm
   - Example
   - Symmetries and Skeletons
3. Results
   - Non-even-odd
   - Even-odd
4. Conclusion

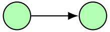
Proof by enumeration :
The even-odd permutations are optimal up to $2k = 32$

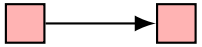
A bound for non-even-odd π ?

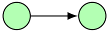
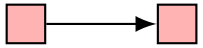
$2k$	Fibonacci bound	even-odd		non-even-odd	
		DR	Ref	DR	Ref
6	5	5	Suzaki10	6	Suzaki10
8	6	6		6	
10	6	7		7	
12	7	8		8	
14	7	8		8	
16	7	8		8	
18	8	8	Cauchois19	9	Cauchois19
20	8	9		9	
22	8	8		9	NEW
24	8	9		≥ 9	
26	8	9	Derbez19	≥ 9	
28	9	9		≥ 9	
30	9	9		≥ 9	
32	9	9		≥ 9	

Non-even-odd bound ?

Properties :

 : Less paths

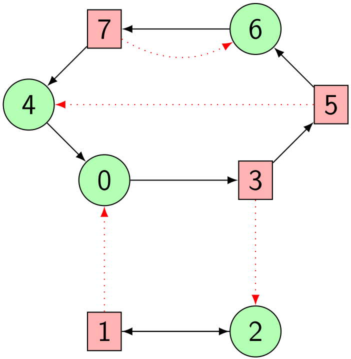
 : More paths

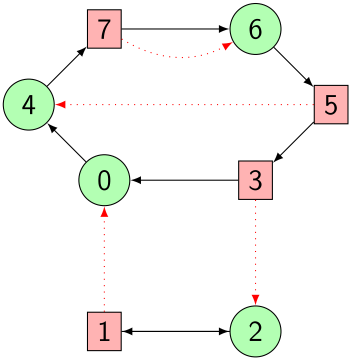
Equal number of  and 

Conjecture :

The sum of paths will not exceed the sum of Fibonacci paths in π and its inverse π^{-1}

Counterexample towards a generic proof





start node	0	2	4	6
22 paths	5	8	5	**4**

start node	0	2	4	6
21 paths	**4**	5	5	7

$$4 \times fibo(5) = 20$$

Flows against Truncated Differential analysis ?

2010 DR is good against Impossible Differential.

2019 Some π with optimal DR are not that good for Truncated Differential.

The path algorithm is generic and the criteria can be easily modified

Question : What is a good criteria ?

Test new criteria ?

Definition (X-path diffusion round)

X-$DR(\pi)$ is the smallest integer R such that : $\forall u, v \in V$, there are X paths of length R from u to v.

Test new criteria ?

Definition (X-path diffusion round)

X-$DR(\pi)$ is the smallest integer R such that : $\forall u, v \in V$, there are X paths of length R from u to v.

Definition (X-SBox diffusion round)

X-$SB(\pi)$ is the smallest integer R such that : $\forall u, v \in V$, there are X S-Boxes traversed by paths of length R from u to v.

Section Summary

1. Graph representation of GFN
2. Path building Algorithm
   - Example
   - Symmetries and Skeletons
3. Results
   - Non-even-odd
   - Even-odd
4. Conclusion

Conclusion

Contribution :

- A graph representation with friendly properties for Feistel permutations
- A generic path algorithm publicly available at : `gitlab.inria.fr/agontier/ANewAlgoForGFN`
- Proof that even-odd permutations are optimal up to $2k = 32$

Conclusion

Contribution :

- A graph representation with friendly properties for Feistel permutations
- A generic path algorithm publicly available at : `gitlab.inria.fr/agontier/ANewAlgoForGFN`
- Proof that even-odd permutations are optimal up to $2k = 32$

Future work :

- **Open question** : New criteria for more secure GFN ?

Conclusion

Contribution :

- A graph representation with friendly properties for Feistel permutations
- A generic path algorithm publicly available at : `gitlab.inria.fr/agontier/ANewAlgoForGFN`
- Proof that even-odd permutations are optimal up to $2k = 32$

Future work :

- **Open question** : New criteria for more secure GFN ?

Thank you for listening

Even-odd : New criteria ?

Definition (X-path diffusion round)

X-$DR(\pi)$ is the smallest integer R such that : $\forall u, v \in V$, there are X paths of length R from u to v.

Definition (X-SBox diffusion round)

X-$SB(\pi)$ is the smallest integer R such that : $\forall u, v \in V$, there are X S-Boxes traversed by paths of length R from u to v.

NextPath(π)

Data : π : partial permutation

foreach (a, b) **given by** Strategy() **do**

- **if** $\neg$HasPath(a, π, b, R) **then**
  - MakePath(a, π, b, R)
  - **return**

Add π to solution pool

MakePath(x, π, b, l)

Data : π : partial permutation, l : length

if $l > 0$ **then**

- **if** x is odd **then**
  - MakePath$(x - 1, \pi, b, l)$
- **if** $\pi[x]$ is fixed **then**
  - MakePath$(\pi[x], \pi, b, l - 1)$
- **else**
  - **foreach** y not used in π **do**
    - $\pi[x] \leftarrow y$
    - MakePath$(y, \pi, b, l - 1)$
  - free $\pi[x]$

else if $x = b$ **then** NextPath(π)