Equivalence of Generalised Feistel Networks

Patrick Derbez [1], **Marie Euler** [1,2]

[1]Univ Rennes, Inria, CNRS, IRISA
[2]DGA

March 29, 2024

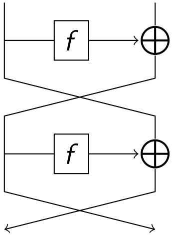
Table of Contents

The original Feistel Network

- Invented by Horst Feistel [Smi71; Fei73]
- Data Encryption Standard (DES) in 1977

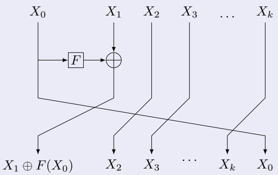
Properties

- The state is divided in two branches
- Decryption is similar to encryption
- Transform a "pseudorandom" function in a "pseudorandom" permutation [LR88]

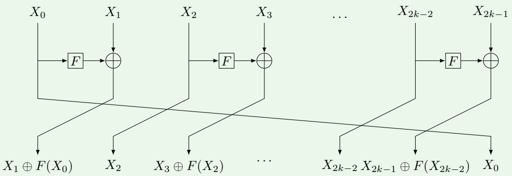


Generalisations of Feistel Networks [ZMI89]

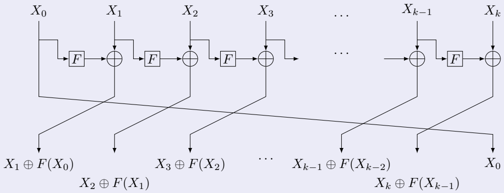
Type I



Type II



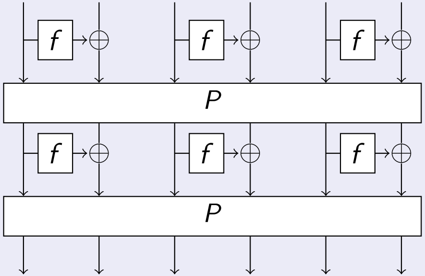
Type III



Generalisations of Feistel Networks

[Nyb96] Replace the cyclic shift by another well-chosen permutation.

A generic shuffle [SM10]

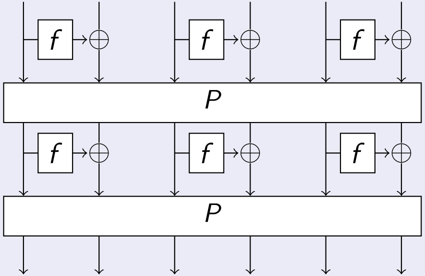


r rounds: $(PF)^r$

Generalisations of Feistel Networks

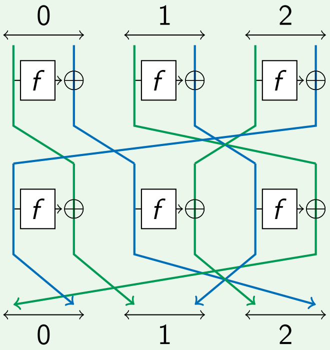
[Nyb96] Replace the cyclic shift by another well-chosen permutation.

A generic shuffle [SM10]



r rounds: $(PF)^r$

Even-odd GFNs



Can be described by two smaller permutations $L = [0, 2, 1]$, $R = [1, 2, 0]$

Properties of the linear layer (Independant of the Feistel function)

Diffusion round

- $DR(P)$ is the minimum number of rounds r such that all the output branches depend on all the input branches (and conversely).
- Helps to quantify the resistance to integral cryptanalysis, impossible differential attacks and meet-in-the-middle attacks.
- Easy to compute.
- Equal to the number of branches for the cyclic shift.

Properties of the linear layer (Independant of the Feistel function)

Diffusion round

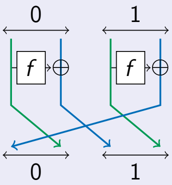
- $DR(P)$ is the minimum number of rounds r such that all the output branches depend on all the input branches (and conversely).
- Helps to quantify the resistance to integral cryptanalysis, impossible differential attacks and meet-in-the-middle attacks.
- Easy to compute.
- Equal to the number of branches for the cyclic shift.

Number of active S-boxes / Non-linear functions

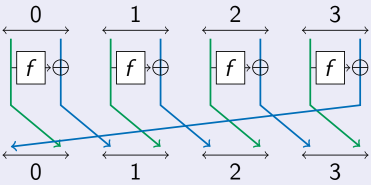
- $AS(P, r)$ is the minimum number of active S-boxes in a differential/linear trails on r rounds.
- Helps to quantify the resistance to differential and linear attacks
- Computed via MILP. Much harder !

Blockciphers based on type-II GFNs

CLEFIA [Shi+07] $DR = 4$

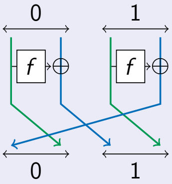


HIGHT [Hon+06] $DR = 8$

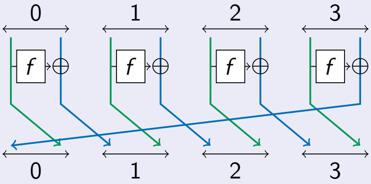


Blockciphers based on type-II GFNs

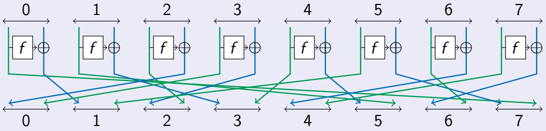
CLEFIA [Shi+07] $DR = 4$



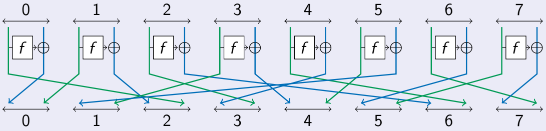
HIGHT [Hon+06] $DR = 8$



LBlock [WZ11] $DR = 8$

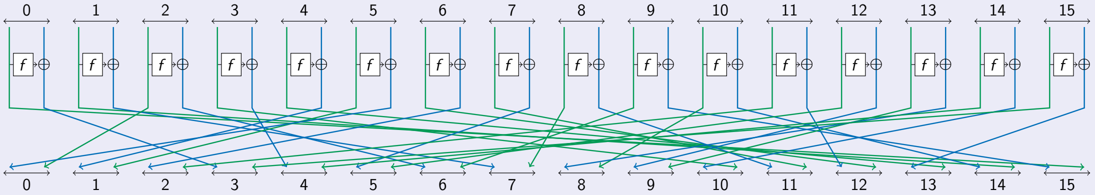


TWINE [Suz+12] $DR = 8$



Blockciphers based on type-II GFNs

WARP [Ban+20] $DR = 10$



How to find a good permutation of $2k$ branches?

Generic case: $(2k)!$ possibilities $\qquad 32! \simeq 2^{118}$

Even-odd case: $(k!)^2$ possibilities $\qquad (16!)^2 \simeq 2^{88}$

How to deal with the huge size of the search space?

- [SM10] Enumerate all the permutations — Up to 16 branches
- [CGT19] Use equivalence classes — Up to 20/24 branches
- [Der+19] Tree pruning (even-odd case) — Up to 36 branches
- [Del+22] Tree pruning (generic case) — Up to 32 branches

How to find a good permutation of $2k$ branches?

Generic case: $(2k)!$ possibilities $32! \simeq 2^{118}$

Even-odd case: $(k!)^2$ possibilities $(16!)^2 \simeq 2^{88}$

How to deal with the huge size of the search space?

- [SM10] Enumerate all the permutations — Up to 16 branches
- [CGT19] Use equivalence classes — Up to 20/24 branches
- [Der+19] Tree pruning (even-odd case) — Up to 36 branches
- [Del+22] Tree pruning (generic case) — Up to 32 branches

The greedy strategy *"First focus on DR then AS"* is non-optimal for AS [Ban+20]

Table of Contents

One round equivalence [CGT19]

The Feistel step F acts similarly on all the pairs of branches
so any shuffling of pairs commutes with F.

$A \in \mathcal{S}_{2k}$ is a permutation of pairs if and only if it shuffles pairs of branches together.

One round equivalence [CGT19]

The Feistel step F acts similarly on all the pairs of branches so any shuffling of pairs commutes with F.

$A \in \mathcal{S}_{2k}$ is a permutation of pairs if and only if it shuffles pairs of branches together.

For any permutation P, for any number of rounds r,

$$\underbrace{(APA^{-1}F)^r}_{\substack{r \text{ rounds of the GFN} \\ \text{associated to } APA^{-1}}} = (APFA^{-1})^r = A \underbrace{(PF)^r}_{\substack{r \text{ rounds of the GFN} \\ \text{associated to } P}} A^{-1}$$

$\hookrightarrow$ Both GFN are identical up to a relabelling of the inputs and outputs.

One round equivalence [CGT19]

The GFNs associated with P and Q are conjugacy-based equivalent if and only if there exists a permutation of pairs A such that $Q = APA^{-1}$.

One round equivalence [CGT19]

The GFNs associated with P and Q are conjugacy-based equivalent if and only if there exists a permutation of pairs A such that $Q = APA^{-1}$.

Enumeration of even-odd GFNs

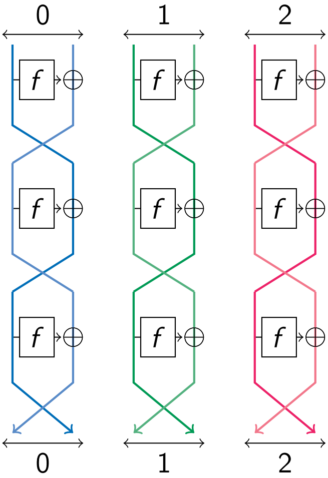
The even-odd GFN associated to (L, R) is equivalent to the even-odd GFN associated to (aLa^{-1}, aRa^{-1}) for any permutation a.

$\hookrightarrow$ There is no need to enumerate all values of (L, R): It is enough to consider one L per conjugacy class of S_k.

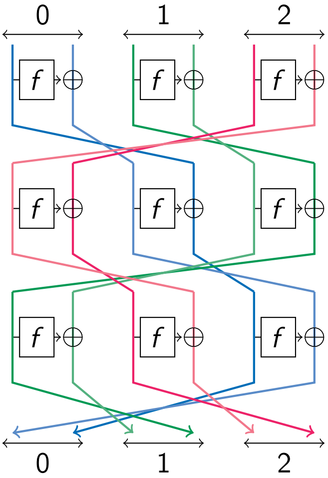
$\hookrightarrow$ The enumeration goes from $(k!)^2$ to $N_k k!$ with N_k the number of conjugacy classes in S_k.

For 32 branches: from $16!^2 \simeq 2^{88}$ to $231 \times 16! \simeq 2^{52}$.

Conjugacy is not enough



(a) $L = R = [0, 1, 2]$



(b) $L' = R' = [1, 2, 0]$

Expanded equivalence

The GFNs associated with P and Q are expanded equivalent if and only if there exists a permutation of pairs A such that for all positive integer r, $A_r := Q^r A P^{-r}$ is a permutation of pairs.

$\hookrightarrow$ It implies that for any positive integer r, $(QF)^r = A_r (PF)^r A^{-1}$: both Feistel are identical up to a relabelling of the inputs and outputs.

Exemples

- If $Q = APA^{-1}$, then for all $r \geq 0$, $A_r = A$
- If $Q = BP = PB$, then $A = \mathrm{Id}$ and for all $r \geq 0$, $A_r = B^r$

Expanded equivalence of even-odd permutations

Number of classes

There are $k!$ expanded equivalence classes of even-odd permutations of $2k$ elements.
Each of theses classes contains $k!$ permutations.

Expanded equivalence of even-odd permutations

Number of classes

There are $k!$ expanded equivalence classes of even-odd permutations of $2k$ elements.
Each of theses classes contains $k!$ permutations.

For 32 branches: from $231 \times 16! \simeq 2^{52}$ to $16! \simeq 2^{44}$.

The cycle structure of $R^{-1}L$ is invariant in the equivalence class of (L,R).
It is also true for all the $R^{-i}L^{i}$.
It is more interesting to describe an even-odd permutation (L, R) by $R^{-1}L$ and R.

Expanded equivalence of even-odd permutations

Number of classes

There are $k!$ expanded equivalence classes of even-odd permutations of $2k$ elements.
Each of theses classes contains $k!$ permutations.

For 32 branches: from $231 \times 16! \simeq 2^{52}$ to $16! \simeq 2^{44}$.

The cycle structure of $R^{-1}L$ is invariant in the equivalence class of (L,R).
It is also true for all the $R^{-i}L^i$.
It is more interesting to describe an even-odd permutation (L, R) by $R^{-1}L$ and R.

Table of Contents

1 - Reduction of candidates

Source & Topic	Size of the list	Nb of extended expanded equivalence classes
[CGT19] Best-known permutations for GFNs with 32,64 or 128 branches regarding diffusion (extended 1-round equivalence classes)	32	10
[Der+19] Optimal permutations for even-odd GFNs with 28 to 34 branches (1-round equivalence classes)	19	9
[Shi+18] Alternative permutations to improve the resistance of `LBlock` against DS MitM attack.	64	2
[Shi+18] Alternative permutations to improve the resistance of `TWINE` against DS MitM attack.	12	1

2 - WARP [Ban+20]

How to find a good 32-branch permutation?

The designers found 152 permutations with $DR = 10$ and among them 8 permutations with $AS = 66 \geq 64$ after 19 rounds.

2 - WARP [Ban+20]

How to find a good 32-branch permutation?

The designers found 152 permutations with $DR = 10$ and among them 8 permutations with $AS = 66 \geq 64$ after 19 rounds. But:

- *The attack characteristics for other attacks (...) are identical for all of them.*
- The designers say that these 8 permutations are not isomorphic.

2 - WARP [Ban+20]

How to find a good 32-branch permutation?

The designers found 152 permutations with $DR = 10$ and among them 8 permutations with $AS = 66 \geq 64$ after 19 rounds. But:

- *The attack characteristics for other attacks (...) are identical for all of them.*
- The designers say that these 8 permutations are not isomorphic.

They are (extended) expanded-equivalent.

2 - WARP [Ban+20]

How to find a good 32-branch permutation?

The designers found 152 permutations with $DR = 10$ and among them 8 permutations with $AS = 66 \geq 64$ after 19 rounds. But:

- *The attack characteristics for other attacks (...) are identical for all of them.*
- The designers say that these 8 permutations are not isomorphic.

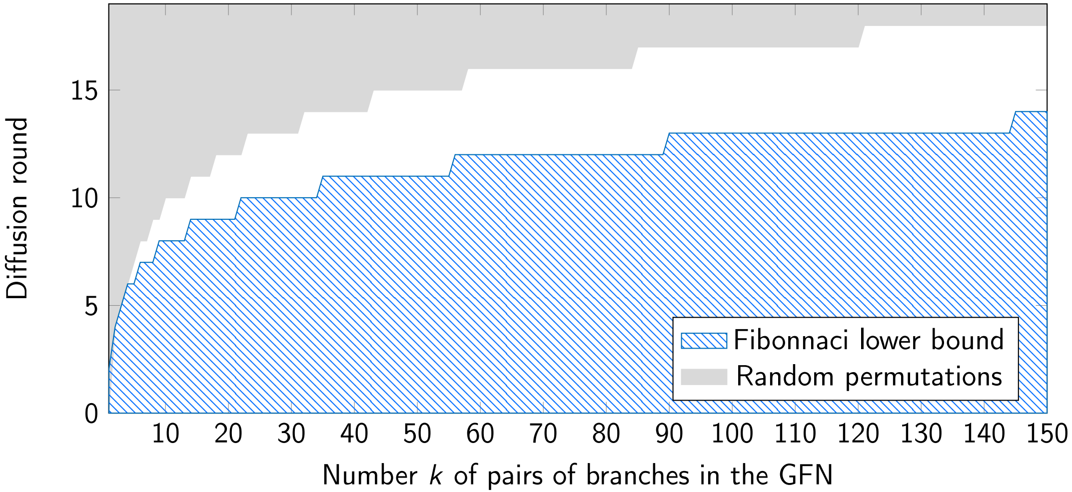
They are (extended) expanded-equivalent.

$\hookrightarrow$ Regrouping the 152 permutations with $DR = 10$ before computing the AS leads to 7 classes. The AS computation takes one hour instead of two days.

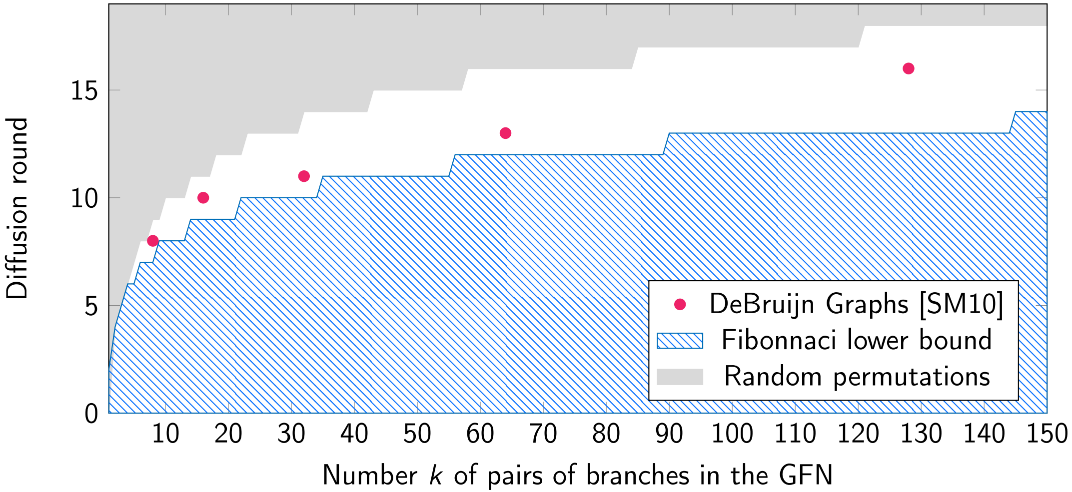
A better permutation?

We evaluated the DR/AS for a larger space of permutations (which reduced to 184 classes of permutations with $DR = 10$) and found 5 classes of permutations with $DR = 10$ and $AS \geq 64$ after 18 rounds.

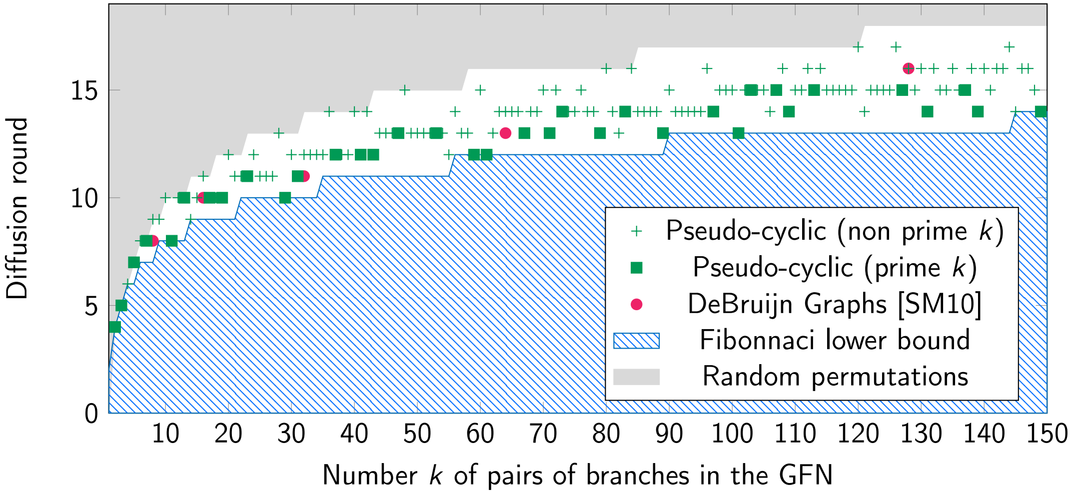
3 - New family of GFNs with good diffusion



3 - New family of GFNs with good diffusion



3 - New family of GFNs with good diffusion



Conclusion and open questions

- A better understanding of the fundamental structure of type-II GFNs
- New GFN candidates (diffusion, AS, ...)

Conclusion and open questions

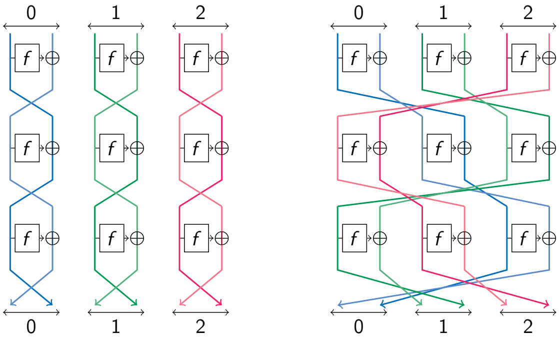
IRISA

- A better understanding of the fundamental structure of type-II GFNs
- New GFN candidates (diffusion, AS, ...)

Open questions

- Non even-odd case: $\dfrac{(2k)!}{k!} = \binom{2k}{k} k!$ equivalence classes?
- Finding good permutations to help designers.
  - $\hookrightarrow$ Analysis of the family which diffuses well?
  - $\hookrightarrow$ Any other good families?
- Cryptanalysis / Security analysis
  - $\hookrightarrow$ Can we find an equivalent GFN which is vulnerable to some attacks?
  - $\hookrightarrow$ Can we prove that all the equivalent GFNs are resistant?

Invariant subspace attacks



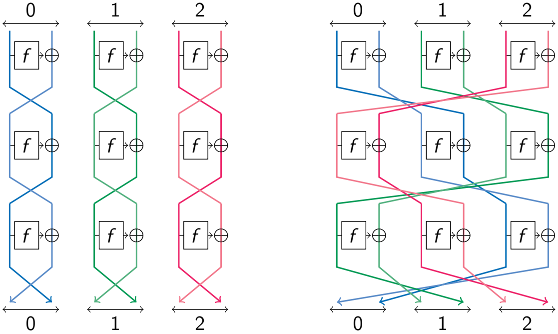
(a) 0 is invariant

(b) 0 is not invariant
$0 \to 1 \to 2 \to 0$ is a subspace trail.

Invariant subspaces are not preserved by expanded equivalence.

Can we find all subspace trails by finding invariant subspaces in an equivalent GFNs?

Invariant subspace attacks



(a) 0 is invariant

(b) 0 is not invariant
$0 \to 1 \to 2 \to 0$ is a subspace trail.

Invariant subspaces are not preserved by expanded equivalence.

Can we find all subspace trails by finding invariant subspaces in an equivalent GFNs?

Thank you for your attention