Diffusion dans les schémas de Feistel généralisés

Gaël Thomas[1]
Travail en collaboration avec Thierry P. Berger[1] et Marine Minier[2]

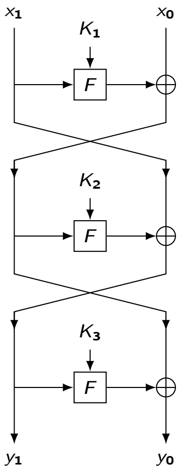
[1]XLIM (UMR CNRS 7252), Université de Limoges
123 avenue Albert Thomas, 87060 Limoges Cedex - France

[2]Université de Lyon, INRIA
INSA-Lyon, CITI, F-69621, Villeurbanne

JC2 2014-03-27

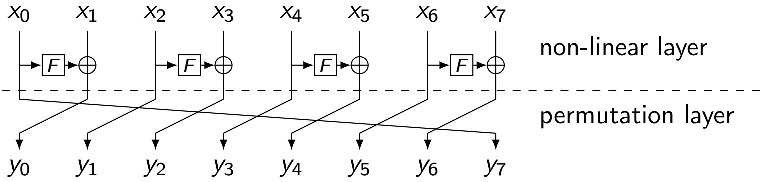
The Original Feistel Structure

- Designed by Horst Feistel at IBM in the 1970's
- Used in DES, Camellia, Simon,...
- Build $2n$-bit permutation from n-bit to n-bit (Feistel) functions
- Similar encryption and decryption up to round keys order



Generalized Feistel Networks

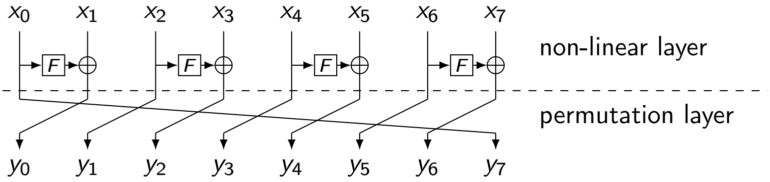
- Introduced by Zheng, Matsumoto, and Imai at CRYPTO'89
- Splits the message into $k \geq 2$ n-bit-long blocks



- Permutation layer : usually the cyclic shift
- Different flavors of GFNs according to the non-linear layer

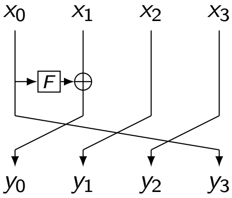
Generalized Feistel Networks

- Introduced by Zheng, Matsumoto, and Imai at CRYPTO‘89
- Splits the message into $k \geq 2$ n-bit-long blocks

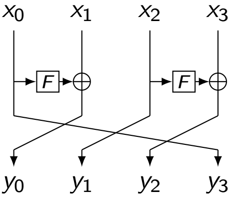


- Permutation layer : usually the cyclic shift
- Different flavors of GFNs according to the non-linear layer
- Pro: Simpler Feistel functions (fitted for small scale implementation)
- Con: "diffusion" between blocks gets poorer as k grows

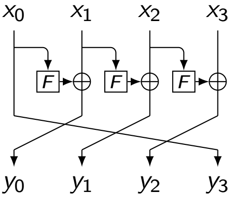
The Generalized Feistel Flavors



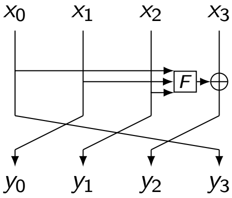
Type-1 (CAST-256, Lesamnta)



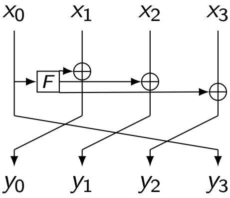
Type-2 (RC6, CLEFIA)



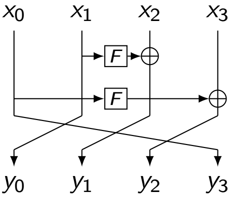
Type-3



Source Heavy (RC2, SHA-1)

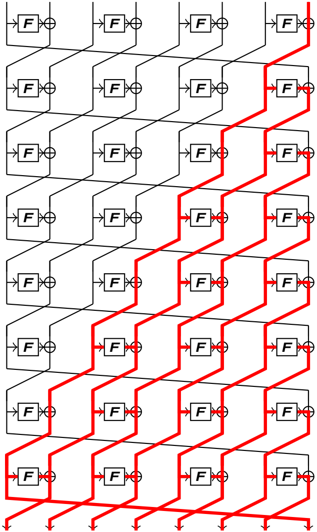


Target Heavy (MARS)



Nyberg's

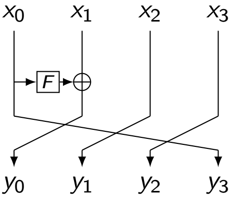
Full Diffusion Delay



- Introduced by Suzaki and Minematsu at FSE'10
- Minimum number of rounds d^+ for every inputs to influence every outputs
- Depends solely on the structure of the network, not on the Feistel functions used
- d^-: similarly defined when performing decryption
- We consider encryption *and* decryption important, thus we look at:

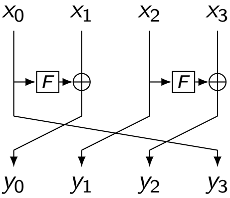
$$d = \max(d^+, d^-).$$

Full Diffusion Delay of Generalized Feistel Networks



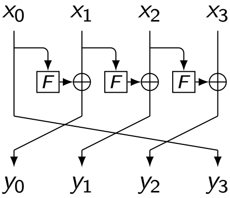
Type-1 (CAST-256, Lesamnta)

$\mathbf{d} = (\mathbf{k}-\mathbf{1})^2 + \mathbf{1}$



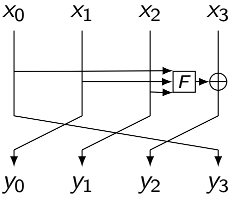
Type-2 (RC6, CLEFIA)

$\mathbf{d} = \mathbf{k}$



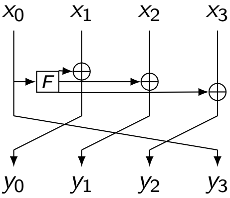
Type-3

$\mathbf{d} = \mathbf{k}$



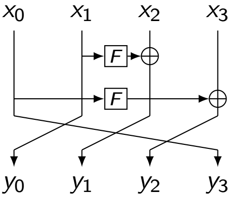
Source Heavy (RC2, SHA-1)

$\mathbf{d} = \mathbf{k}$



Target Heavy (MARS)

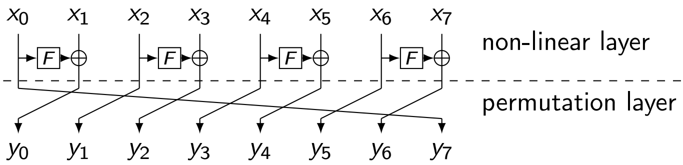
$\mathbf{d} = \mathbf{k}$



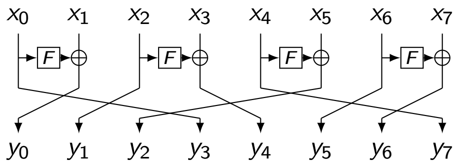
Nyberg's

$\mathbf{d} = \mathbf{k}$

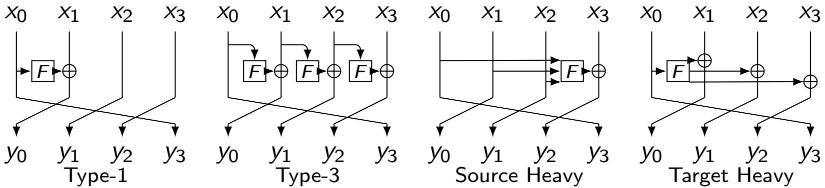
An Improvement of Type-2



- Proposed by Suzaki and Minematsu at FSE'10
- Idea: Replace the cyclic shift of the permutation layer by any block-wise permutation
- Includes Nyberg's GFNs
- Full diffusion delay d goes from k to $2\log_2 k$ for optimum permutations

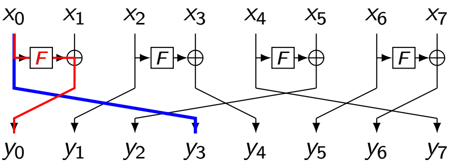


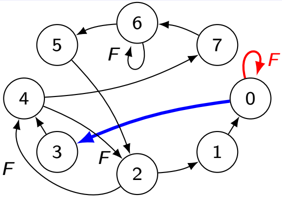
Improve Type-1, Type-3, Source-Heavy and Target-Heavy?



- Studied by Yanagihara and Iwata at IEICE Trans. 2013
- Same idea as Suzaki and Minematsu: allow any block permutation $\mathcal{P}$
- Source Heavy and Target-Heavy cannot be improved
- Full diffusion delay of Type-1 drops from $(k-1)^2+1$ to $k(k+2)/2-2$
- No general construction for Type-3 but found permutations with $d \leq 4$ for $k \leq 8$

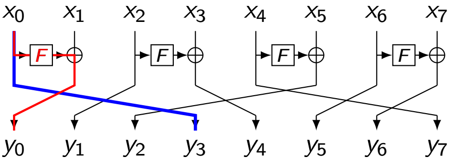
Graph and Matrix Representations

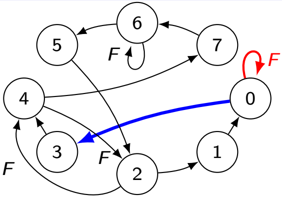




- d^+ smallest distance such that for all vertices couple (u, v) there exists a path of length d^+ going from u to v

Graph and Matrix Representations

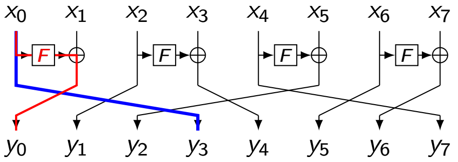


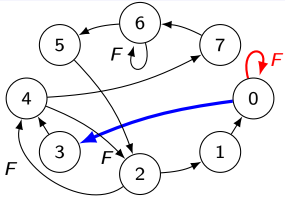


$$\mathcal{M} = \begin{pmatrix} {\color{red}F} & 1 & & & & & & \\ & & 1 & & & & & \\ & & & & F & 1 & & \\ {\color{blue}1} & & & & & & & \\ & & F & 1 & & & & \\ & & & & & & 1 & \\ & & & & & & F & 1 \\ & & & & 1 & & & \end{pmatrix}$$

- d^+ smallest distance such that for all vertices couple (u, v) there exists a path of length d^+ going from u to v
- $\mathcal{M}$: adjacency matrix of the graph associated to the GFN
- $\Rightarrow d^+$: smallest integer such that $\mathcal{M}^{d^+}$ has no zero coefficient

Graph and Matrix Representations





$$\mathcal{M} = \begin{pmatrix} {\color{red}F} & 1 & & & & & & \\ & & 1 & & & & & \\ & & & & F & 1 & & \\ {\color{blue}1} & & & & & & & \\ & & F & 1 & & & & \\ & & & & & & 1 & \\ & & & & & & F & 1 \\ & & & & 1 & & & \end{pmatrix} \quad \mathcal{P} = \begin{pmatrix} & 1 & & & & & & \\ & & 1 & & & & & \\ & & & & & 1 & & \\ 1 & & & & & & & \\ & & & 1 & & & & \\ & & & & & & 1 & \\ & & & & & & & 1 \\ & & & & 1 & & & \end{pmatrix} \quad \mathcal{F} = \begin{pmatrix} {\color{blue}1} & & & & & & & \\ {\color{red}F} & 1 & & & & & & \\ & & 1 & & & & & \\ & & F & 1 & & & & \\ & & & & 1 & & & \\ & & & & F & 1 & & \\ & & & & & & 1 & \\ & & & & & & F & 1 \end{pmatrix}$$

- d^+ smallest distance such that for all vertices couple (u, v) there exists a path of length d^+ going from u to v
- $\mathcal{M}$: adjacency matrix of the graph associated to the GFN
- $\Rightarrow d^+$: smallest integer such that $\mathcal{M}^{d^+}$ has no zero coefficient
- $\mathcal{M}$ cut into two matrices : $\mathcal{P}$ for the permutation layer and $\mathcal{F}$ for the non-linear layer : $\mathcal{M} = \mathcal{P}\mathcal{F}$.

Depth of diffusion

$$\mathcal{M} = \begin{pmatrix} F & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & . & F & 1 & . & . \\ 1 & . & . & . & . & . & . & . \\ . & . & F & 1 & . & . & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & F & 1 \\ . & . & . & . & 1 & . & . & . \end{pmatrix} \quad \mathcal{M}^2 = \begin{pmatrix} F^2 & F & 1 & . & . & . & . & . \\ . & . & . & . & F & 1 & . & . \\ . & . & F^2 & F & . & . & 1 & . \\ F & 1 & . & . & . & . & . & . \\ 1 & . & . & . & F^2 & F & . & . \\ . & . & . & . & . & . & F & 1 \\ . & . & . & . & 1 & . & F^2 & F \\ . & . & F & 1 & . & . & . & . \end{pmatrix} \quad \cdots$$

- Computations done in $\mathbb{Z}[F]$

Depth of diffusion

$$\mathcal{M} = \begin{pmatrix} F & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & . & F & 1 & . & . \\ 1 & . & . & . & . & . & . & . \\ . & . & F & 1 & . & . & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & F & 1 \\ . & . & . & . & 1 & . & . & . \end{pmatrix} \quad \mathcal{M}^2 = \begin{pmatrix} F^2 & F & 1 & . & . & . & . & . \\ . & . & . & . & F & 1 & . & . \\ . & . & F^2 & F & . & . & 1 & . \\ F & 1 & . & . & . & . & . & . \\ 1 & . & . & . & F^2 & F & . & . \\ . & . & . & . & . & . & F & 1 \\ . & . & . & . & 1 & . & F^2 & F \\ . & . & F & 1 & . & . & . & . \end{pmatrix} \quad \cdots$$

- Computations done in $\mathbb{Z}[F]$
- Degree of coefficient (i, j) : number of Feistel functions gone through from x_j to y_i

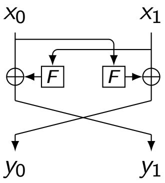
Depth of diffusion

$$\mathcal{M} = \begin{pmatrix} F & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & . & F & 1 & . & . \\ 1 & . & . & . & . & . & . & . \\ . & . & F & 1 & . & . & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & F & 1 \\ . & . & . & . & 1 & . & . & . \end{pmatrix} \quad \mathcal{M}^2 = \begin{pmatrix} F^2 & F & 1 & . & . & . & . & . \\ . & . & . & . & F & 1 & . & . \\ . & . & F^2 & F & . & . & 1 & . \\ F & 1 & . & . & . & . & . & . \\ 1 & . & . & . & F^2 & F & . & . \\ . & . & . & . & . & . & F & 1 \\ . & . & . & . & 1 & . & F^2 & F \\ . & . & F & 1 & . & . & . & . \end{pmatrix} \quad \cdots$$

- Computations done in $\mathbb{Z}[F]$
- Degree of coefficient (i, j) : number of Feistel functions gone through from x_j to y_i
- Generalize diffusion delay : r-depth of diffusion d_r^+
- d_r^+ : minimum number of rounds ℓ such as the coefficients of $\mathcal{M}^\ell$ are of degree at least r.
- e.g. $d_0^+ = d^+$; d_1^+ : no more linear-only dependances
- Linked with resistances to *structural* attacks as impossible differentials or integral attacks

Characterizing GFN Matrices

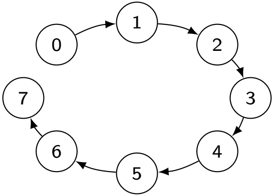
- GFNs transforms non-invertible F functions into a permutation,
- Hence decryption mode matrix $\mathcal{M}^{-1}$ should not have coefficients with F at denominator
- $\Rightarrow \det(\mathcal{M})$ independent of $F \Rightarrow \det(\mathcal{M}) = \pm 1$.
- Goal : Find condition on where to put the Feistel functions

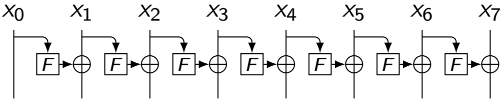


Not a Feistel network

Graph of the non-linear layer

$$\begin{pmatrix} 0 & & & & & & & \\ F & 0 & & & & & & \\ & F & 0 & & & & (0) & \\ & & F & 0 & & & & \\ & & & F & 0 & & & \\ & & & & F & 0 & & \\ & (0) & & & & F & 0 & \\ & & & & & & F & 0 \end{pmatrix}$$





- Graph with adjacency matrix $\mathcal{F} - \mathcal{I}$
- Shows order the Feistel functions must be evaluated for decryption
- Possible if and only if Graph is *acyclic*
- If and only if $\mathcal{F}$ is lower triangular up to block reindexing

An interesting subfamily : Quasi-involutive GFNs

- Stronger requirement for matrix $\mathcal{F}$
- Non-linear layer must be the same for encryption *and* decryption
- Holds when any of the following (equivalent) conditions holds :
  - A block cannot both emit and receive through a Feistel function
  - for all $0 \leq \ell \leq k-1$, row ℓ and column ℓ cannot both have an F coefficient
  - $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$ (i.e. $\mathcal{F}^{-1} = \mathcal{F} \mod 2$)
- Not the case for Type-3 GFN

Exhautive Search of GFNs

- We investigated all the quasi-involutive GFNs with $k = 8$ blocks up to block reindexing equivalence.

Exhautive Search of GFNs

- We investigated all the quasi-involutive GFNs with $k = 8$ blocks up to block reindexing equivalence.
- We consider three parameters :
  - the full diffusion delay d,
  - the number of Feistel functions (per round) s,
  - the total cost, i.e. the number of Feistel functions required for full diffusion, $c = d \times s$.

Exhautive Search of GFNs

- We investigated all the quasi-involutive GFNs with $k = 8$ blocks up to block reindexing equivalence.
- We consider three parameters :
  - the full diffusion delay d,
  - the number of Feistel functions (per round) s,
  - the total cost, i.e. the number of Feistel functions required for full diffusion, $c = d \times s$.
- No GFN with cost $c < 24$. GFN with cost $c = 24$ includes the Type-2 of Suzaki and Minematsu ($s = 4$, $d = 6$)
- Minimum number s of Feistel functions per round required to have a full diffusion in d rounds and corresponding total cost c:

d	1, 2	3	4	5	6	7	8	9	10	11	12
s	∞	16	7	6	4	4	4	3	3	3	2
c	∞	48	28	30	24	28	32	27	30	33	24

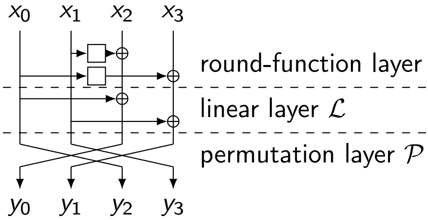
How to Further Increase Diffusion?

How to Further Increase Diffusion?

- Generalize the permutation layer $\mathcal{P}$ beyond block-permutation

How to Further Increase Diffusion?

- Generalize the permutation layer $\mathcal{P}$ beyond block-permutation
- We propose: a GFN-like linear mapping $\mathcal{G}$ with identity as round-function, i.e. $\mathcal{G} = \mathcal{P}\mathcal{L}$ with
    - $\mathcal{P}$ is a block-wise permutation matrix
    - $\mathcal{L}$ is similar to $\mathcal{F}$ but with I instead of F, called the linear layer

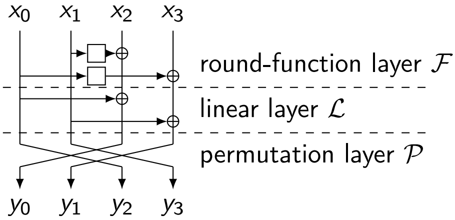


$$\mathcal{P} = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}$$

$$\mathcal{L} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ I & & 1 & \\ & I & & 1 \end{pmatrix} \qquad \mathcal{F} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & F & 1 & \\ F & & & 1 \end{pmatrix}$$

How to Further Increase Diffusion?

- Generalize the permutation layer $\mathcal{P}$ beyond block-permutation
- We propose: a GFN-like linear mapping $\mathcal{G}$ with identity as round-function, i.e. $\mathcal{G} = \mathcal{P}\mathcal{L}$ with
    - $\mathcal{P}$ is a block-wise permutation matrix
    - $\mathcal{L}$ is similar to $\mathcal{F}$ but with I instead of F, called the linear layer
- Extended Generalized Feistel Networks: $\mathcal{M} = \mathcal{P}\mathcal{L}\mathcal{F}$

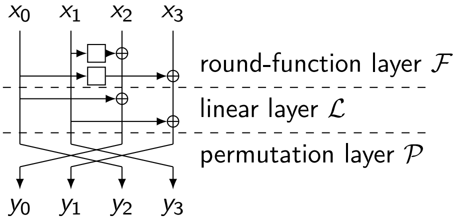


$$\mathcal{M} = \begin{pmatrix} I & F & 1 & \\ F & I & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix} \qquad \mathcal{P} = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}$$

$$\mathcal{L} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ I & & 1 & \\ & I & & 1 \end{pmatrix} \qquad \mathcal{F} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & F & 1 & \\ F & & & 1 \end{pmatrix}$$

How to Further Increase Diffusion?

- Generalize the permutation layer $\mathcal{P}$ beyond block-permutation
- We propose: a GFN-like linear mapping $\mathcal{G}$ with identity as round-function, i.e. $\mathcal{G} = \mathcal{P}\mathcal{L}$ with
  - $\mathcal{P}$ is a block-wise permutation matrix
  - $\mathcal{L}$ is similar to $\mathcal{F}$ but with I instead of F, called the linear layer
- Extended Generalized Feistel Networks: $\mathcal{M} = \mathcal{P}\mathcal{L}\mathcal{F}$
- $\mathcal{L}$ and $\mathcal{F}$ have common structure $\rightarrow$ regrouped into matrix $\mathcal{N} = \mathcal{L}\mathcal{F}$
- Matrix $\mathcal{N}$ has two formal parameters:
  - F: non-linear functions $\rightarrow$ cryptographic security
  - I: idendity functions $\rightarrow$ quick diffusion

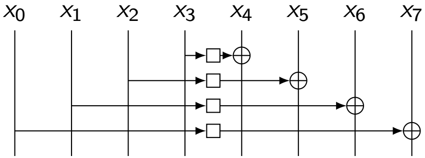


$$\mathcal{M} = \begin{pmatrix} I & F & 1 & \\ F & I & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix} \qquad \mathcal{P} = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}$$

$$\mathcal{L} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ I & & 1 & \\ & I & & 1 \end{pmatrix} \qquad \mathcal{F} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & F & 1 & \\ F & & & 1 \end{pmatrix}$$

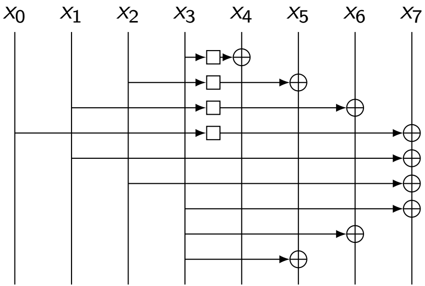
An Interesting Example

$$\mathcal{F} = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & F & 1 & & & \\ & & F & & & 1 & & \\ & F & & & & & 1 & \\ F & & & & & & & 1 \end{pmatrix}$$



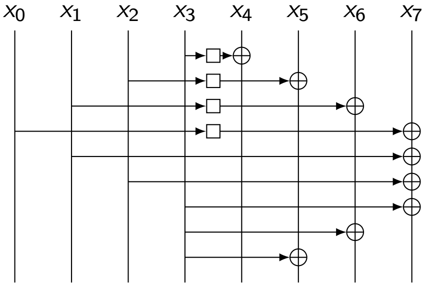
An Interesting Example

$$\mathcal{L} = \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & I & & 1 & & \\ & & & I & & & 1 & \\ & I & I & I & & & & 1 \end{pmatrix}$$



An Interesting Example

$$\mathcal{N} = \left(\begin{array}{cccc|cccc}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & 1 & & & & & \\
 & & & 1 & & & & \\
\hline
 & & & F & 1 & & & \\
 & & F & I & & 1 & & \\
 & F & & I & & & 1 & \\
F & I & I & I & & & & 1
\end{array}\right)$$

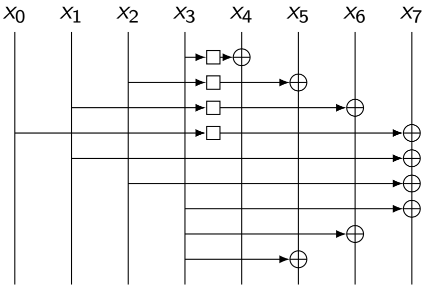


An Interesting Example

$$\mathcal{N} = \left(\begin{array}{cccc|cccc} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ \hline & & & F & 1 & & & \\ & & F & I & & 1 & & \\ & F & & I & & & 1 & \\ F & I & I & I & & & & 1 \end{array}\right)$$

- $\mathcal{P}$: Swap emitters and receivers

$$\mathcal{P} = \left(\begin{array}{c|c} 0 & P_1 \\ \hline P_2 & 0 \end{array}\right)$$



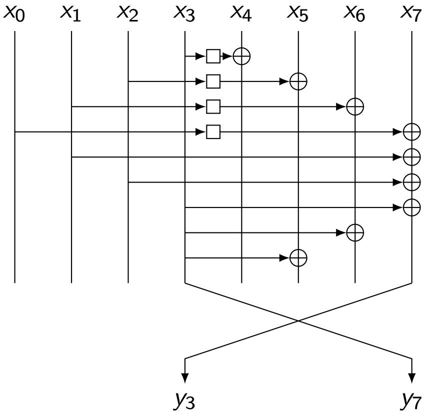
An Interesting Example

$$\mathcal{N} = \left(\begin{array}{cccc|cccc}
1 & & & & & & & \\
 & 1 & & & & & & \\
 & & 1 & & & & & \\
 & & & 1 & & & & \\
\hline
 & & & F & 1 & & & \\
 & & F & I & & 1 & & \\
 & F & & I & & & 1 & \\
F & I & I & I & & & & 1
\end{array}\right)$$

- $\mathcal{P}$: Swap emitters and receivers

$$\mathcal{P} = \left(\begin{array}{c|c}
0 & \begin{array}{cc} P'_1 & \begin{array}{c} 0 \\ \vdots \end{array} \\ 0 \; \cdots & 1 \end{array} \\
\hline
\begin{array}{cc} P'_2 & \begin{array}{c} 0 \\ \vdots \end{array} \\ 0 \; \cdots & 1 \end{array} & 0
\end{array}\right)$$

- If $\mathcal{P}$ swaps $k-1$ and $\frac{k}{2}-1$ then $d=4$.

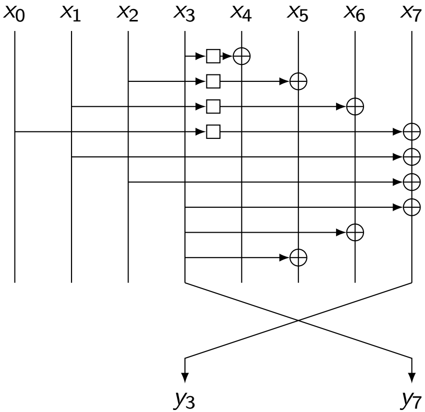


An Interesting Example

$$\mathcal{N} = \left(\begin{array}{cccc|cccc} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ \hline & & & F & 1 & & & \\ & & F & I & & 1 & & \\ & F & & I & & & 1 & \\ F & I & I & I & & & & 1 \end{array}\right)$$

- $\mathcal{P}$: Swap emitters and receivers

$$\mathcal{P} = \left(\begin{array}{c|c} 0 & \begin{array}{cc} P'_1 & \begin{array}{c} 0 \\ \vdots \end{array} \\ 0 \ \cdots & 1 \end{array} \\ \hline \begin{array}{cc} P'_2 & \begin{array}{c} 0 \\ \vdots \end{array} \\ 0 \ \cdots & 1 \end{array} & 0 \end{array}\right)$$



- If $\mathcal{P}$ swaps $k-1$ and $\frac{k}{2}-1$ then $d = 4$.
- Choose P'_1 and P'_2 to best resist attacks not (directly) related to d
- E.g. for $k = 16$ and 20 rounds, minimum number of differentially/linealy actives S-boxes ranges from 26 to 42 as $\mathcal{P}$ varies

Conclusion

We have:

- Matrix representation of a GFN
- used it to show some properties of GFNs (diffusion in particular)
- Introduced a new class of schemes called Extended Generalized Feistel Networks: add a diffusion layer to the GFN
- Instantiated this class into a well chosen example

Further work:

- Propose a blockcipher based on our proposals
- Further study resistance against linear/differential cryptanalysis

Thank you for your attention

Any Questions ?