Extended Generalized Feistel Networks using Matrix Representation

Thierry P. Berger[1], Marine Minier[2], Gaël Thomas[1]

[1]XLIM (UMR CNRS 7252), Université de Limoges
123 avenue Albert Thomas, 87060 Limoges Cedex
thierry.berger@unilim.fr
gael.thomas@unilim.fr

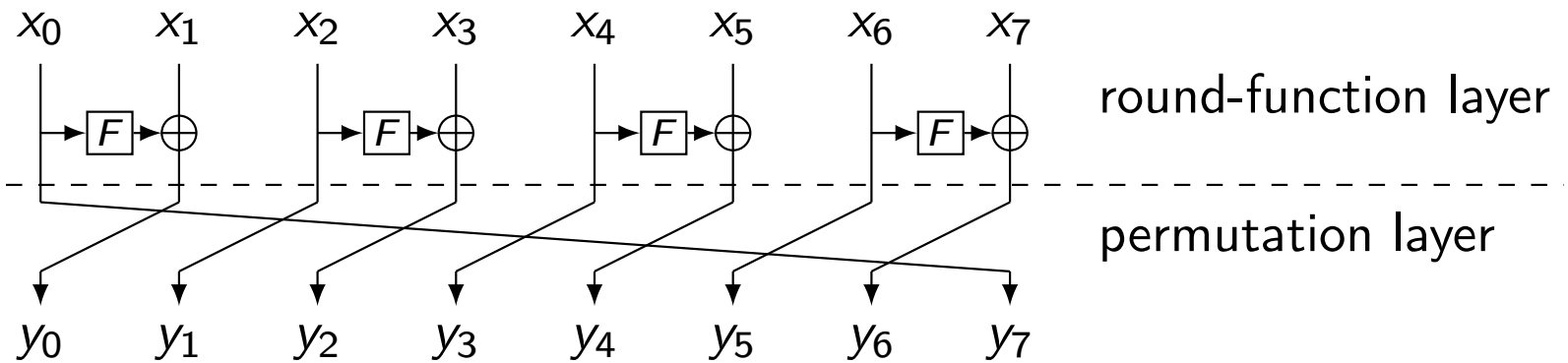
[2]Université de Lyon, INRIA
INSA-Lyon, CITI, F-69621, Villeurbanne
marine.minier@insa-lyon.fr

SAC 2013, August 15, 2013

This work was partially supported by the French National Agency of Research: ANR-11-INS-011.

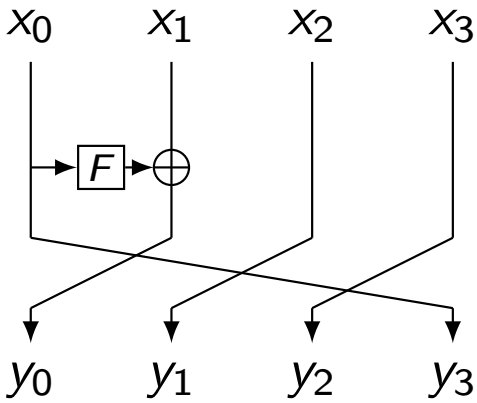
Generalized Feistel Networks

- Introduced by Zheng, Matsumoto, and Imai at CRYPTO'89
- Splits the message into $k \geq 2$ n-bit-long blocks
- Made of two consecutive layers: round-function layer and block-permutation layer
- Different flavors of GFNs, according to the round-function layer

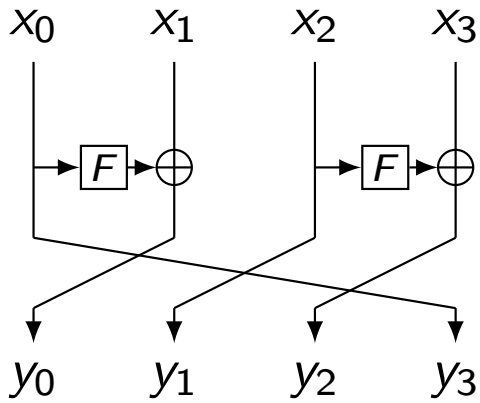


- Pro: fitted for small scale implementation (Block size = Sbox size)
- Con: "diffusion" between blocks gets poorer as k grows

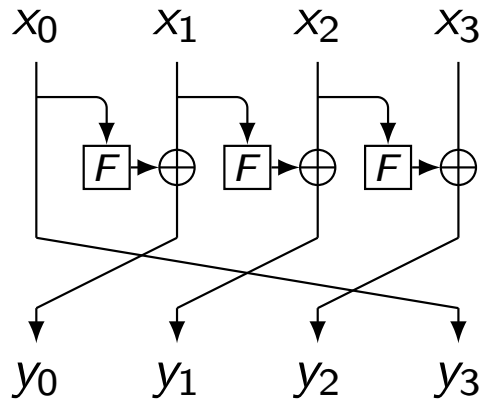
The Generalized Feistel Flavors



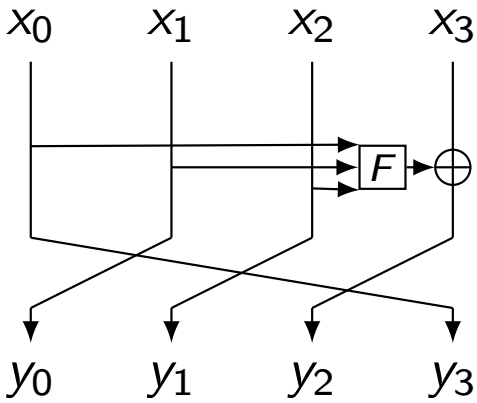
Type-1 (CAST-256, Lesamnta)



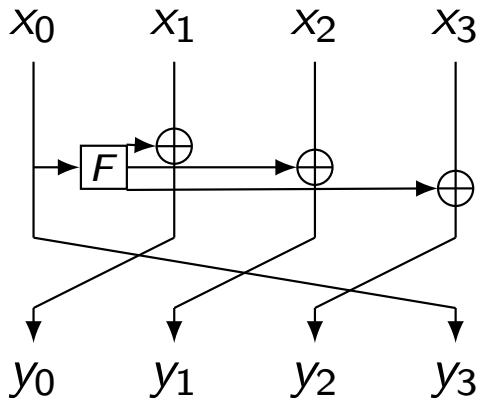
Type-2 (HIGHT, CLEFIA)



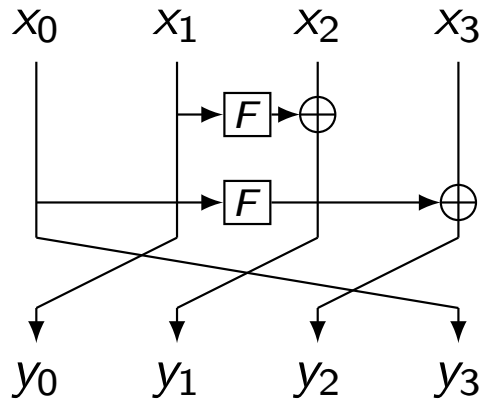
Type-3



Source Heavy (RC2, SHA-1)



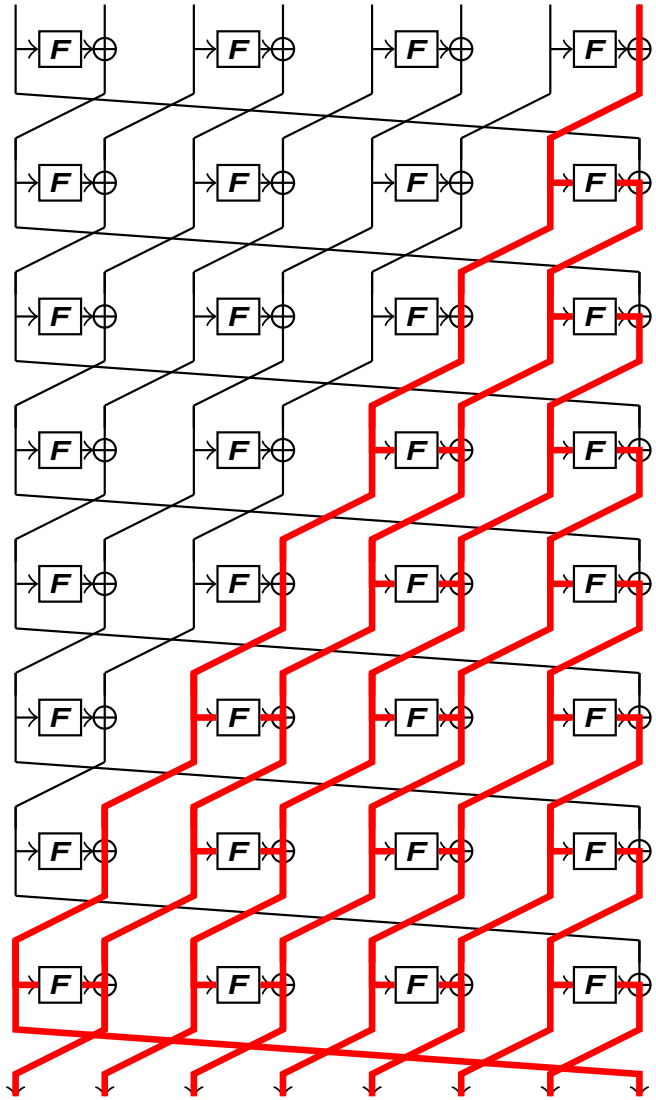
Target Heavy (MARS)



Nyberg's

Table of Contents

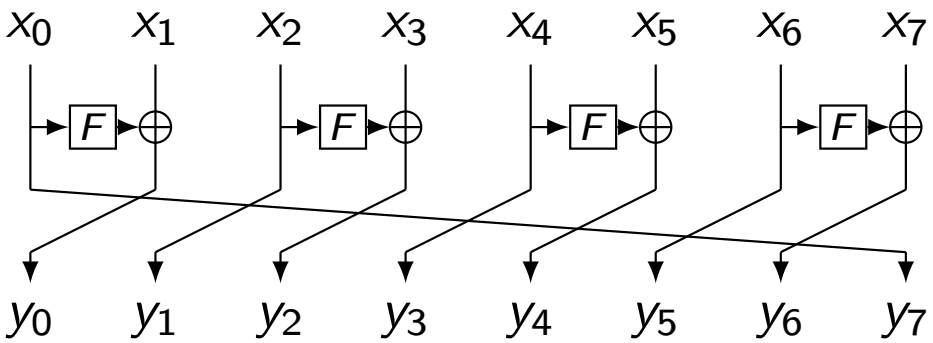
Full Diffusion Delay

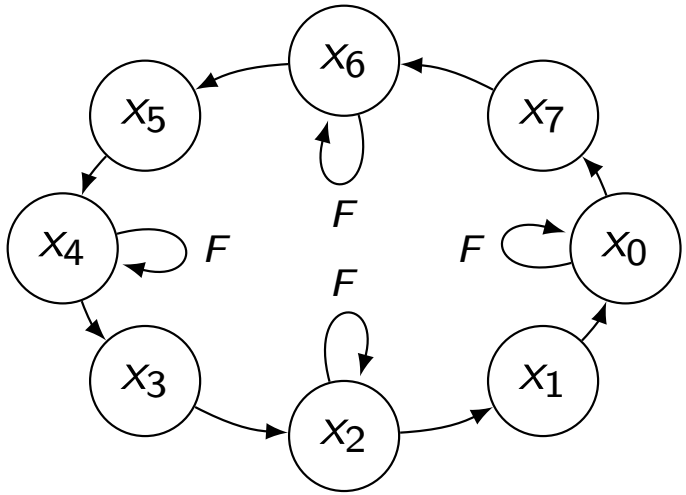


- Introduced by Suzaki and Minematsu at FSE'10
- Minimum number of rounds d^+ for every inputs to influence every outputs
- Depends solely on the structure of the network, not on the round-functions used
- d^-: similarly defined when performing decryption
- We consider encryption *and* decryption important,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

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

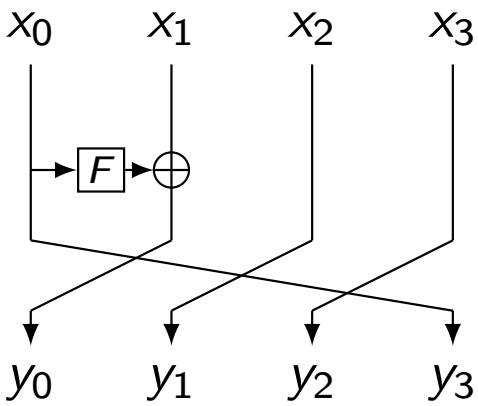
Graph Point of View





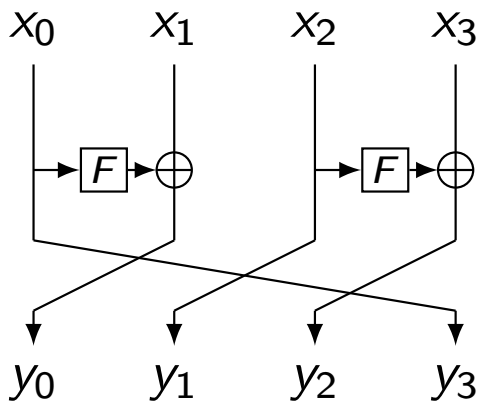
- Graph of a Feistel Network: obtained by folding outputs onto the corresponding inputs
- Represents the structure of the Network
- Full diffusion delay d^+: smallest distance such that for all vertices couple (u, v) there exists a path of length d^+ going from u to v

Full Diffusion Delay of Generalized Feistel Networks



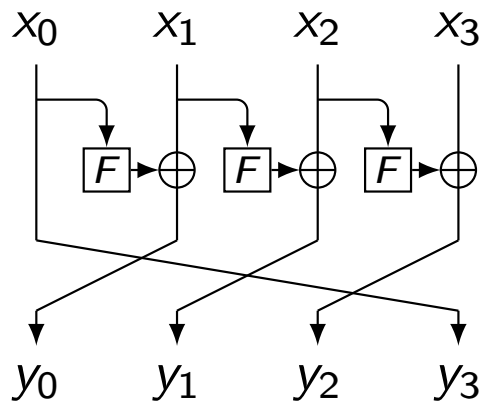
Type-1 (CAST-256, Lesamnta)

$d = (k-1)^2 + 1$



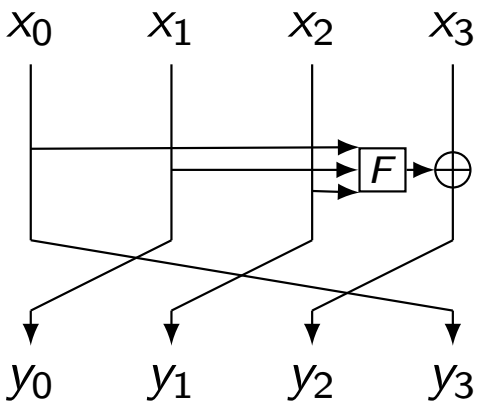
Type-2 (HIGHT, CLEFIA)

$d = k$



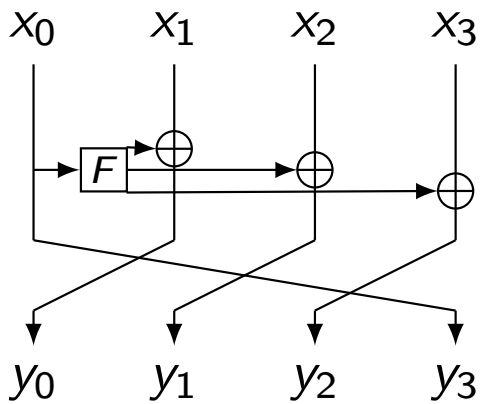
Type-3

$d = k$



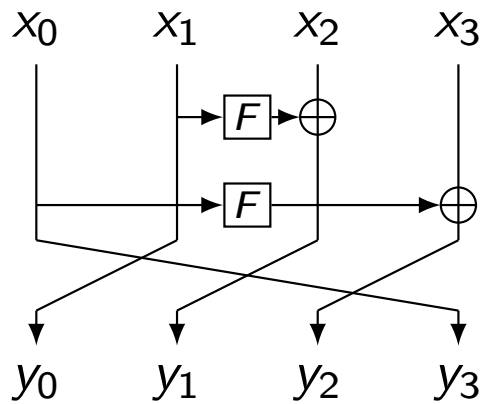
Source Heavy (RC2, SHA-1)

$d = k$



Target Heavy (MARS)

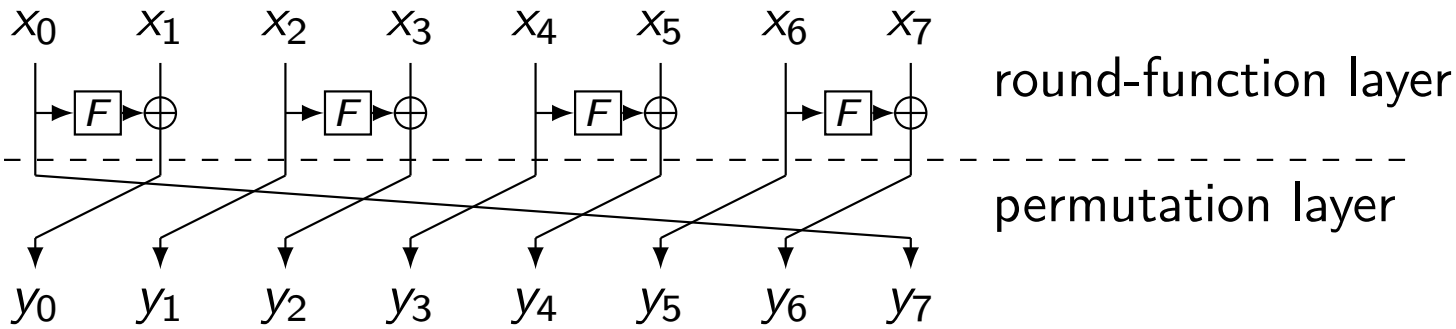
$d = k$



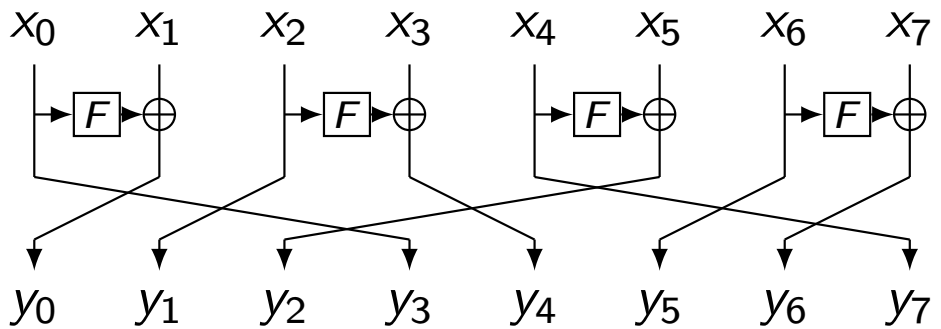
Nyberg's

$d = k$

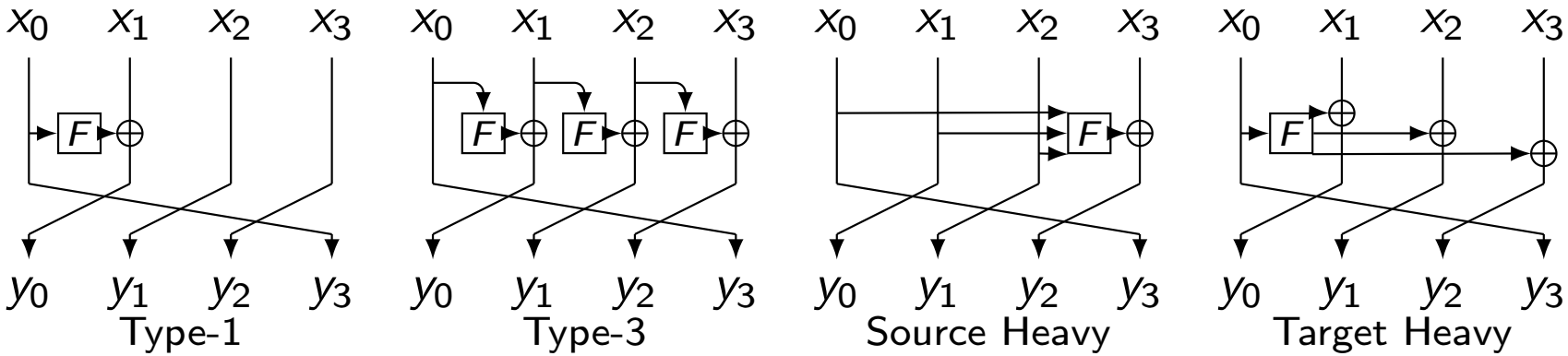
An Improvement of Type-2



- 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

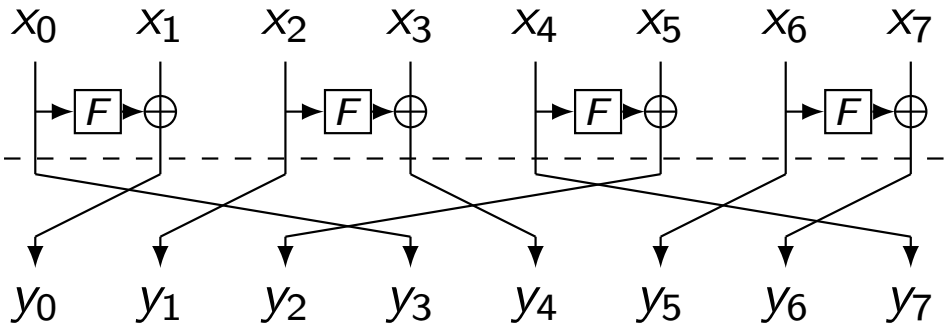


Improve Type-1, Type-3, Source-Heavy and Target-Heavy?



- 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 $k \leq 8$

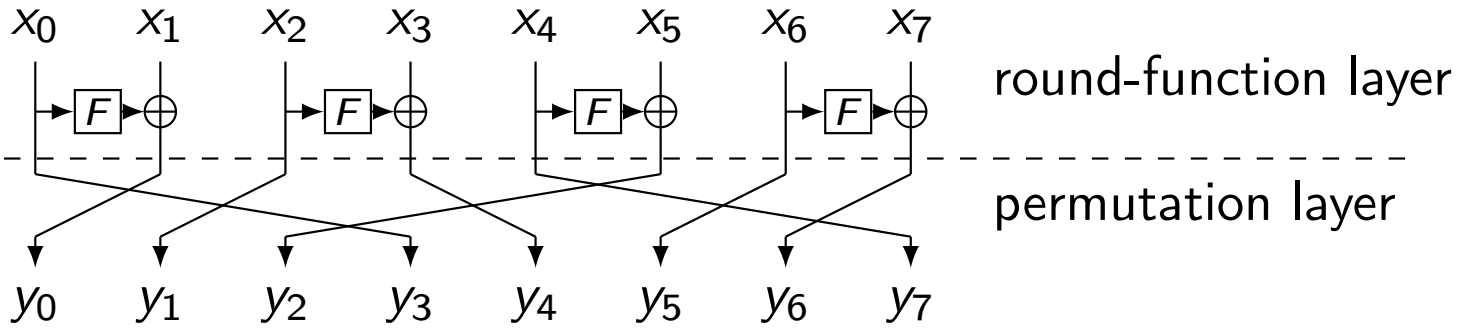
Matrix of a Feistel Network



- a GFN is made of a round-function layer and a permutation layer
- The permutation layer can be represented by a permutation matrix $\mathcal{P}$

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

Matrix of a Feistel Network

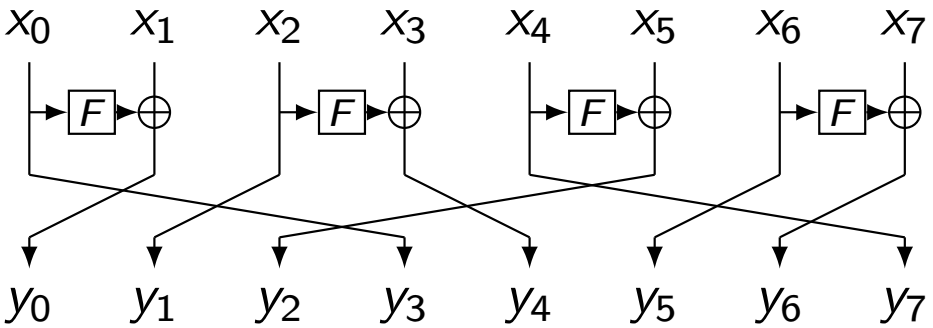


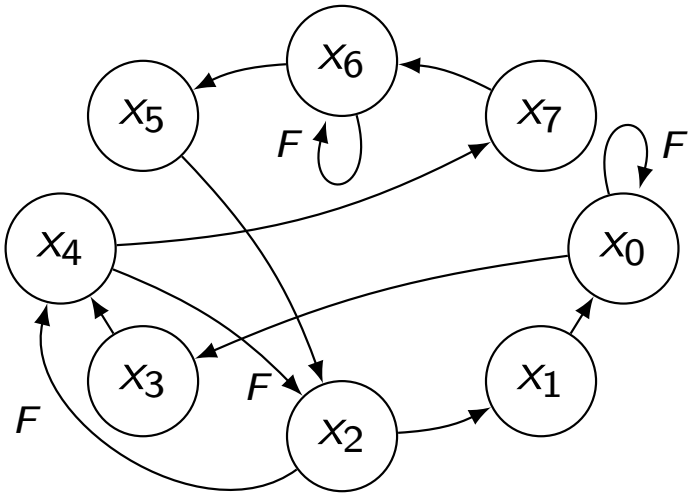
- a GFN is made of a round-function layer and a permutation layer
- The permutation layer can be represented by a permutation matrix $\mathcal{P}$
- Idea: Represent the round-function layer by a matrix $\mathcal{F}$ with:
  - an all-one diagonal
  - a parameter F at position (i, j) when $y_{\mathcal{P}(i)} = F(x_j) \oplus x_i$
- F is a formal parameter merely indicating the presence of a round-function
- Matrix of the whole GFN defined as $\mathcal{M} = \mathcal{P} \times \mathcal{F}$

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

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

Type-2 Feistel Network and its corresponding Matrix



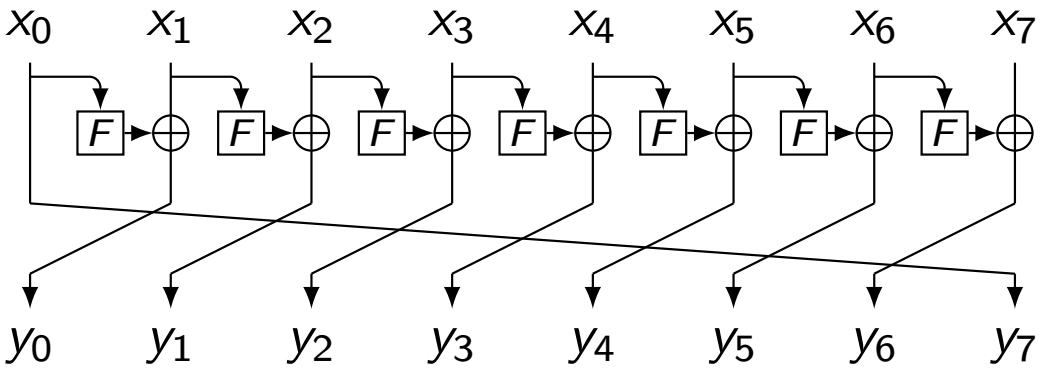


$$\mathcal{M} = \begin{pmatrix} F & 1 & & & & & & \\ & 1 & & & & & & \\ & & F & 1 & & & & \\ 1 & & & & & & & \\ & & F & 1 & & & & \\ & & & & & & 1 & \\ & & & & & & F & 1 \\ & & & & 1 & & & \end{pmatrix} \quad \mathcal{P} = \begin{pmatrix} & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & & & 1 & \\ 1 & &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

- $\mathcal{M}$ is the adjacency matrix of the graph associated to the GFN
- d^+ is the smallest integer such that $\mathcal{M}^{d^+}$ has no zero coefficient

Properties we require from GFNs

- GFNs transforms round-functions into a permutation, hence decryption mode matrix $\mathcal{M}^{-1}$ should not contain any "F^{-1}"
  $\Rightarrow \det(\mathcal{M}) = \pm 1$.
  $\rightarrow$ verified for all classical GFNs
- GFNs are quasi-involutive: encryption/decryption is the same process up to using direct/inverse permutation layer $\mathcal{P}$.
  $\rightarrow$ verified for all classical GFNs except Type-3



We choose to focus on GFNs that are quasi-involutive:

Definition

A matrix $\mathcal{M} = \mathcal{P}\mathcal{F}$ is a GFN matrix if $\mathcal{P}$ is a permutation matrix and $\mathcal{F}$ is with:

1. an all-one diagonal
2. either 0 or F in off-diagonal positions
3. a block cannot both emit and receive through a round-function, i.e.: $\forall i \leq k-1$, row i and column i cannot both have an F coefficient

Quasi-involutiveness

$\mathcal{F}$ is invertible and $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$.

In the case where X-ORs are used, this means $\mathcal{F}^{-1} = \mathcal{F}$.

Conversely

If $\mathcal{F}$ verifies (1) and (2) and $\mathcal{F}^{-1} = 2\mathcal{I} - \mathcal{F}$ then $\mathcal{F}$ also verifies (3).

Exhaustive Search of GFNs

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

Exhaustive Search of GFNs

- We investigated all the GFNs with $k = 8$ blocks, up to block-reindexation equivalence.
- We consider three parameters :
  - the full diffusion delay d,
  - the number of round-function (per round) s,
  - the total cost, i.e. the number of round function 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 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

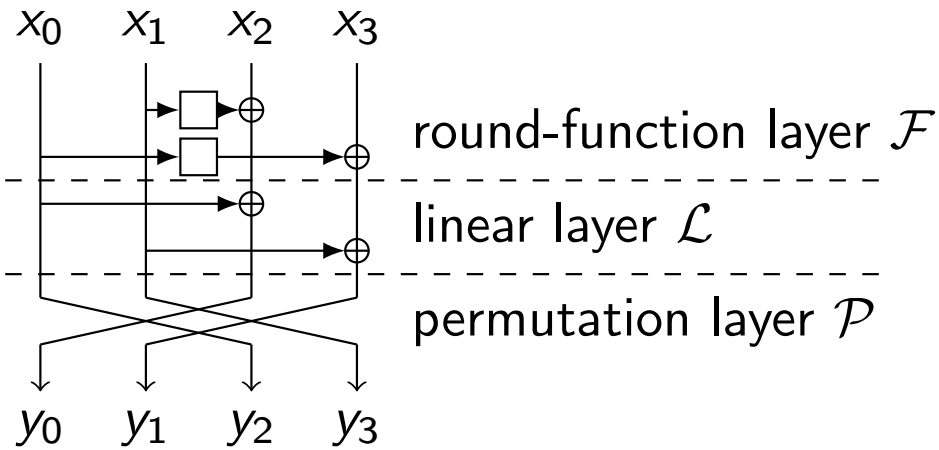
How to Further Increase Diffusion?

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

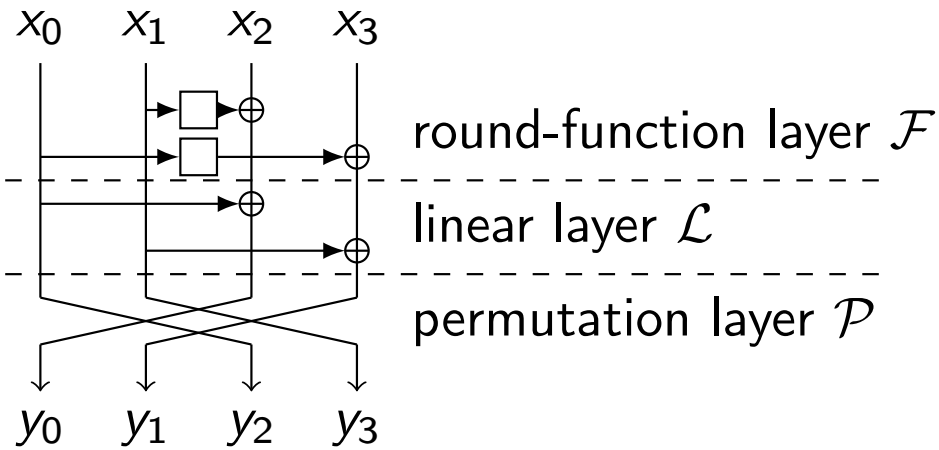


$$\mathcal{P} = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}$$

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

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: $\mathcal{M} = \mathcal{P}\mathcal{L}\mathcal{F}$

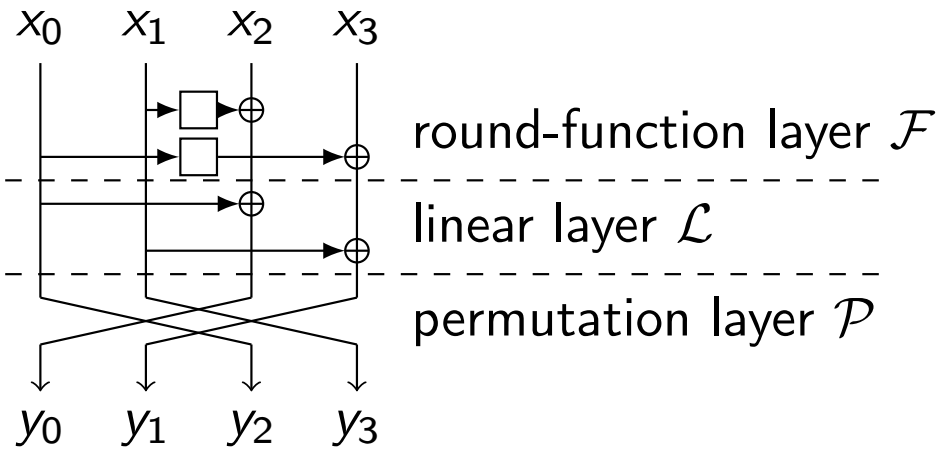


$$\mathcal{M} = \begin{pmatrix} I & F & 1 & \\ F & I & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix} \qquad \mathcal{P} = \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix}$$

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

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



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

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

Definition

A matrix $\mathcal{M} = \mathcal{P}\mathcal{N}$ is a EGFN matrix if $\mathcal{P}$ is a permutation matrix and $\mathcal{N}$ is with:

1. an all-one diagonal
2. either 0, F or I in off-diagonal positions
3. A block cannot both emit and receive through a round-function (either F or I)
4. Linear (I) receivers are also non-linear (F) receivers

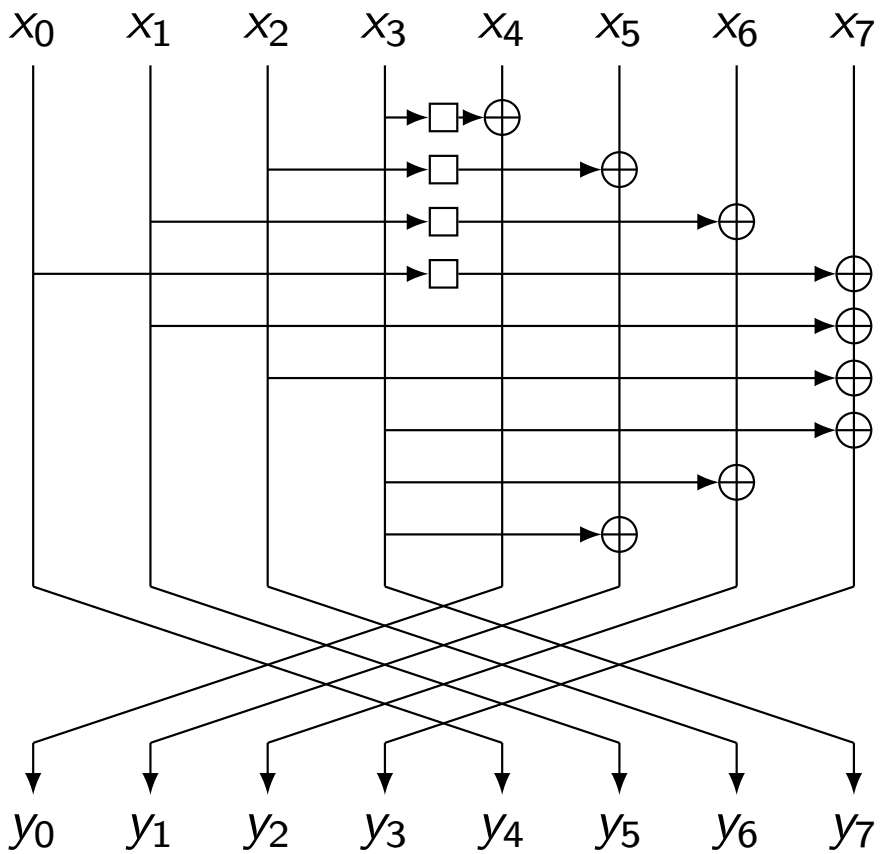
$\rightarrow$ Last condition is for the pseudorandomness proof to works

Quasi-involutiveness

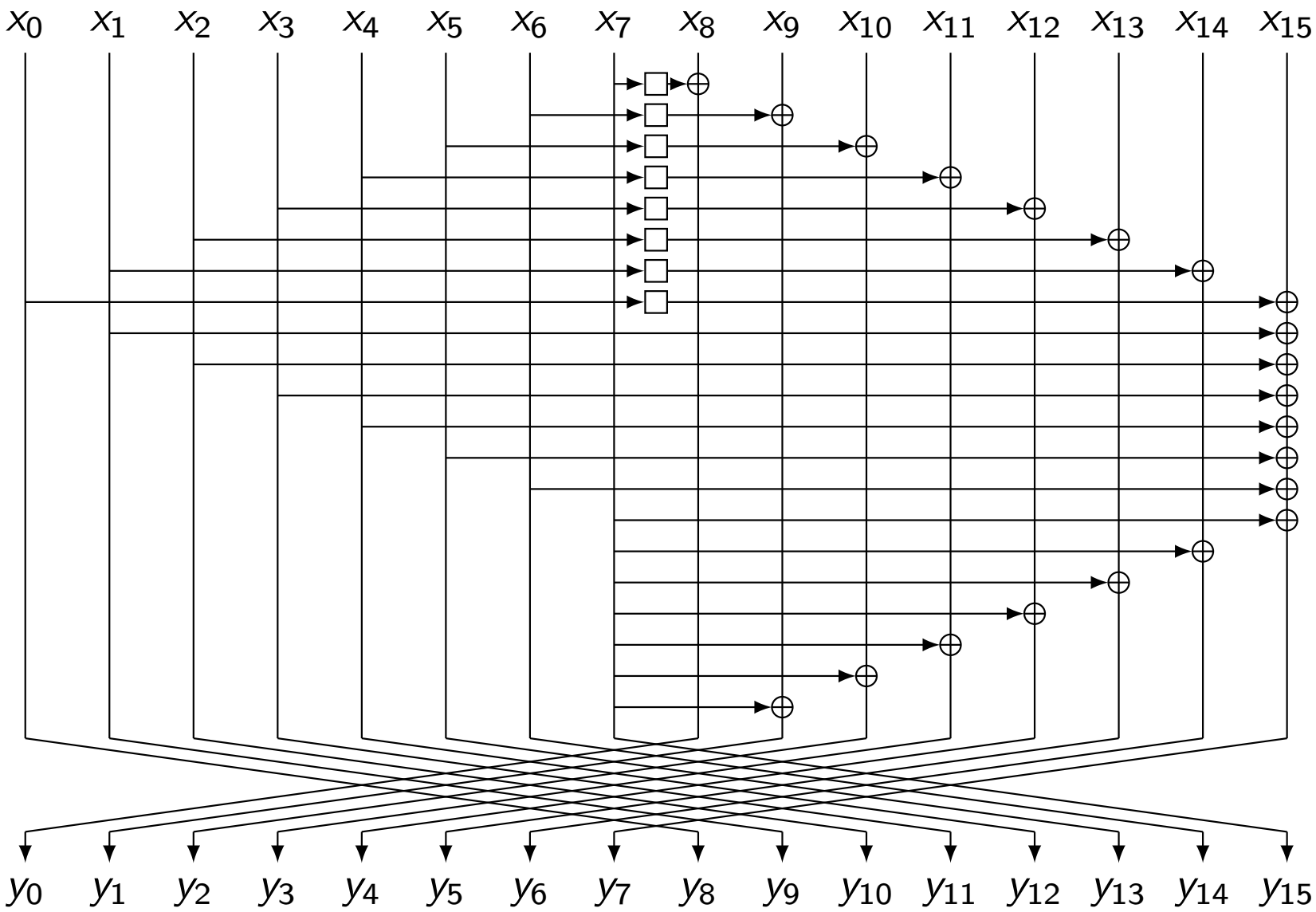
$\mathcal{N}$ is invertible and $\mathcal{N}^{-1} = 2\mathcal{I} - \mathcal{N}$.

An Efficient Example

$$\mathcal{M} = \begin{pmatrix} (0) & & F & I & 1 & & \\ & \ddots & & I & & \ddots & \\ & & & \vdots & & & \\ F & & (0) & \vdots & & & 1 \\ F & I \cdots I & & I & & & 1 \\ 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & (0) & \\ & & & 1 & & & \\ & & & & 1 & & \end{pmatrix}$$



- Order 2 block permutation
- Full diffusion delay $d = 4$ for $k \geq 4$.
- Number of round-functions $s = k/2$
- Total cost $c = d \times s = 2k \rightarrow$ cheaper than S. & M. ($c = k \log_2 k$)


x_0 x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9 x_{10} x_{11} x_{12} x_{13} x_{14} x_{15}
y_0 y_1 y_2 y_3 y_4 y_5 y_6 y_7 y_8 y_9 y_{10} y_{11} y_{12} y_{13} y_{14} y_{15}

Pseudorandomness

- Seminal work of Luby and Rackoff on the classical Feistel ($k = 2$):
  - 3 rounds is pseudorandom-permutation (prp)
  - 4 rounds is strong prp (sprp)
  - Advantage in $\mathcal{O}(\frac{q^2}{2^n})$
- Our Example:
  - $d + 2$ rounds is pseudorandom-permutation (prp): bound in $\mathcal{O}(\frac{kdq^2}{2^n})$
  - $2d + 2$ rounds is strong prp (sprp): bound in $\mathcal{O}(\frac{kdq^2}{2^{n-1}})$

Differential/Linear Cryptanalysis

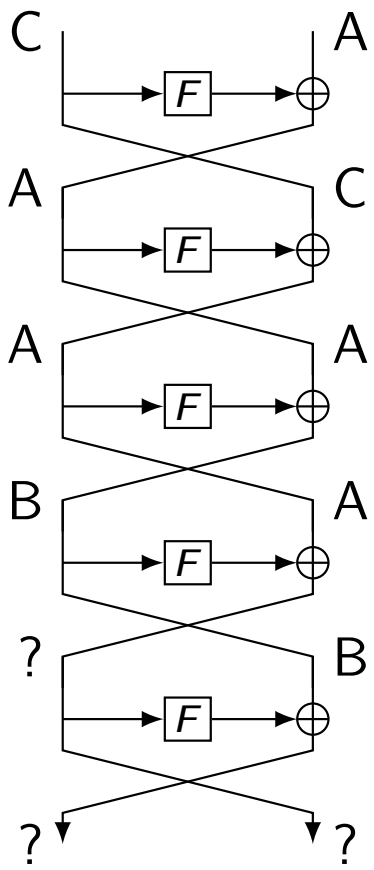
Number of active S-boxes for every round compared with results of Suzaki and Minematsu.

	Round	1	2	3	4	5	6	**7**	8	**9**	10
$k = 8$	S&M's	0	1	2	3	4	6	8	10	12	12
$k = 8$	Ours	0	1	2	6	9	9	**12**	14	15	19
$k = 16$	S&M's	0	1	2	3	4	6	8	11	14	19
$k = 16$	Ours	0	1	2	10	17	17	18	26	**33**	33

	Round	11	12	13	14	15	16	17	18	19	20
$k = 8$	S&M's	14	16	16	18	20	20	22	24	24	26
$k = 8$	Ours	19	22	24	25	29	29	32	34	35	39
$k = 16$	S&M's	21	24	25	27	30	31	33	36	37	39
$k = 16$	Ours	34	42	49	49	50	58	65	65	66	74

- We have more active S-boxes than Suzaki and Minematsu.
- For 64 bits plaintexts:
  - For block size $n = 8$ and block number $k = 8$, secure after **7** rounds
  - For block size $n = 4$ and block number $k = 16$, secure after **9** rounds

Integral Attack



A: All B: Balanced
C: Constant ?: Unknown

- Bijective round-function
- Given 2^n plaintexts
  - all different on one blocks (A)
  - constant on other blocks (C)
- Find an "integral" characteristic after some rounds: Sum of all values of a block is zero (B)
- Attack on the last round by guessing the key
- Forward characteristic for at most $d + 2$ rounds, confirmed experimentaly
- Can add up to d backward rounds, thus characteristic for at most $2d + 2$ rounds

Impossible Differential Attack

- Find differential characteristic $\alpha \not\to \beta$ such that $\Pr[E(x) \oplus E(x \oplus \alpha) = \beta] = 0$.
- Find the maximum number of rounds for that attack using the $\mathcal{U}$-method of Kim, Hong, Sung, Lee, Lim, and Sung:
- $\rightarrow$ at most $2d + 1$ rounds.

Impossible Differential Attack

- Find differential characteristic $\alpha \not\to \beta$ such that $\Pr[E(x) \oplus E(x \oplus \alpha) = \beta] = 0$.
- Find the maximum number of rounds for that attack using the $\mathcal{U}$-method of Kim, Hong, Sung, Lee, Lim, and Sung:
- $\rightarrow$ at most $2d + 1$ rounds.

Security Conclusion:

Construction secure against classical attacks after $2d + 3 = 11$ rounds.

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 two proposals + security arguments

Further work:

- Propose a blockcipher based on our proposals

Thank you for your attention.