Diffusion dans les schémas de Feistel généralisés

Gaël Thomas\textsuperscript{1}
Travail en collaboration avec Thierry P. Berger\textsuperscript{1} et Marine Minier\textsuperscript{2}

\textsuperscript{1}XLIM (UMR CNRS 7252), Université de Limoges
123 avenue Albert Thomas, 87060 Limoges Cedex - France

\textsuperscript{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

\[ x_0 \ x_1 \ x_2 \ x_3 \ x_4 \ x_5 \ x_6 \ x_7 \]

\[ y_0 \ y_1 \ y_2 \ y_3 \ y_4 \ y_5 \ y_6 \ y_7 \]

- 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

\[
\begin{array}{cccccccc}
X_0 & X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & X_7 \\
\downarrow & F & \oplus & F & \oplus & F & \oplus & F \\
Y_0 & Y_1 & Y_2 & Y_3 & Y_4 & Y_5 & Y_6 & Y_7
\end{array}
\]

- 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)
\[ d = (k - 1)^2 + 1 \]

Type-2 (RC6, 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 $k \leq 8$
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

\[ \mathbf{M} = \begin{pmatrix} F & 1 \\ 1 & F \\ F & 1 \\ 1 & F \\ 1 & 1 \\ F & 1 \end{pmatrix} \]

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

\[ M = \begin{pmatrix} F & 1 \\ 1 & F \\ F & 1 \\ 1 & F & 1 \end{pmatrix} \quad P = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \quad F = \begin{pmatrix} \frac{1}{F} & 1 & 1 \\ F & 1 & 1 \\ 1 & F & 1 \end{pmatrix} \]

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

\[ M = \begin{pmatrix}
F & 1 & \cdots & \cdots & \cdots \\
\cdot & 1 & \cdots & \cdots & \cdots \\
\cdot & \cdot & F & 1 & \cdots \\
\cdot & \cdot & \cdot & 1 & \cdots \\
\cdot & \cdot & \cdot & \cdot & F & 1
\end{pmatrix} \quad M^2 = \begin{pmatrix}
F^2 & F & 1 & \cdots & \cdots & \cdots \\
\cdot & F & 1 & \cdots & \cdots & \cdots \\
\cdot & \cdot & F & 1 & \cdots & \cdots \\
\cdot & \cdot & \cdot & F & 1 & \cdots \\
\cdot & \cdot & \cdot & \cdot & F & 1 \\
\cdot & \cdot & \cdot & \cdot & \cdot & F^2 & F
\end{pmatrix} \quad \ldots
\]

- Computations done in \( \mathbb{Z}[F] \)
Depth of diffusion

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

- 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

\[
\mathcal{M} = \begin{pmatrix} F & 1 & \ldots & \ldots & \ldots \\ \ldots & 1 & \ldots & \ldots & \ldots \\ \ldots & \ldots & 1 & \ldots & \ldots \\ \ldots & \ldots & \ldots & 1 & \ldots \\ \ldots & \ldots & \ldots & \ldots & 1 \end{pmatrix}
\quad \mathcal{M}^2 = \begin{pmatrix} F^2 & F & 1 & \ldots & \ldots \\ \ldots & F & 1 & \ldots & \ldots \\ \ldots & \ldots & F & 1 & \ldots \\ \ldots & \ldots & \ldots & F & 1 \\ \ldots & \ldots & \ldots & \ldots & F \end{pmatrix} \quad \ldots
\]

- 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 \(\ell\) 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 dependences

- Linked with resistances to \textit{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

![Diagram of not a Feistel network]
Graph of the non-linear layer

\[
\begin{pmatrix}
0 & F & 0 & 0 & \cdots & 0 & (0) \\
F & 0 & F & 0 & \cdots & 0 & 0 \\
0 & F & 0 & F & \cdots & 0 & 0 \\
0 & 0 & F & 0 & \cdots & 0 & (0) \\
(0) & 0 & 0 & F & \cdots & 0 & 0 \\
(0) & (0) & 0 & F & \cdots & 0 & 0 \\
(0) & (0) & (0) & F & \cdots & 0 & 0 \\
(0) & (0) & (0) & (0) & \cdots & F & 0 \\
\end{pmatrix}
\]

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 $F$
- 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 $\ell$ and column $\ell$ cannot both have an $F$ coefficient
  - $F^{-1} = 2I - F$ (i.e. $F^{-1} = F \mod 2$)
- Not the case for Type-3 GFN
Exhaustive Search of GFNs

- We investigated all the quasi-involutive GFNs with $k = 8$ blocks up to block reindexing equivalence.
Exhaustive 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, $c = d \times s$. 

---

Diffusion dans les schémas de Feistels généralisés  
Gaël Thomas  
JC2 2014-03-27  
14/18
Exhaustive 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 $c$:

<table>
<thead>
<tr>
<th>$d$</th>
<th>1, 2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s$</td>
<td>$\infty$</td>
<td>16</td>
<td>7</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>$c$</td>
<td>$\infty$</td>
<td>48</td>
<td>28</td>
<td>30</td>
<td>24</td>
<td>28</td>
<td>32</td>
<td>27</td>
<td>30</td>
<td>33</td>
<td>24</td>
</tr>
</tbody>
</table>
How to Further Increase Diffusion?

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

Extended Generalized Feistel Networks: $M = PLF$ $L$ and $F$ have common structure $\rightarrow$ regrouped into matrix $N = LF$ 

Matrix $N$ has two formal parameters: $F$: non-linear functions $\rightarrow$ cryptographic security $I$: idendity functions $\rightarrow$ quick diffusion

$x_0$ $y_0$ $x_1$ $y_1$ $x_2$ $y_2$ $x_3$ $y_3$ round-function layer $F$ linear layer $L$ permutation layer $P$ $M$ = \[
\begin{bmatrix}
I & F & 1 & F \\
I & 1 & F & 1 \\
1 & I & 1 & I \\
1 & 1 & I & 1
\end{bmatrix}
\]

$P$ = \[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1
\end{bmatrix}
\]

$L$ = \[
\begin{bmatrix}
1 & 1 & I & 1 \\
1 & I & 1 & I
\end{bmatrix}
\]

$F$ = \[
\begin{bmatrix}
1 & 1 & F & 1 \\
1 & 1 & F & 1
\end{bmatrix}
\]
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

\[
\begin{align*}
\mathcal{P} &= \begin{pmatrix}
1 & 1 \\
1 & 1
\end{pmatrix} \\
\mathcal{L} &= \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1
\end{pmatrix} \\
\mathcal{F} &= \begin{pmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1
\end{pmatrix}
\end{align*}
\]
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: $\mathcal{M} = \mathcal{P}\mathcal{L}\mathcal{F}$

\[
\begin{align*}
\mathcal{P} &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & F & 1 & 1 \\ F & 1 & 1 & 1 \end{pmatrix} \\
\mathcal{L} &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & F & 1 & 1 \\ F & 1 & 1 & 1 \end{pmatrix} \\
\mathcal{F} &= \begin{pmatrix} 1 & F & 1 & 1 \\ 1 & F & 1 & 1 \\ 1 & F & 1 & 1 \\ 1 & F & 1 & 1 \end{pmatrix}
\end{align*}
\]
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. $\mathcal{G} = \mathcal{PL}$ 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: $\mathcal{M} = \mathcal{PLF}$
- $\mathcal{L}$ and $\mathcal{F}$ have common structure $\rightarrow$ regrouped into matrix $\mathcal{N} = \mathcal{LF}$
- Matrix $\mathcal{N}$ has two formal parameters:
  - $F$: non-linear functions $\rightarrow$ cryptographic security
  - $I$: idendity functions $\rightarrow$ quick diffusion

\[
\begin{align*}
\mathcal{M} &= \begin{pmatrix} I & F \\ I & F \end{pmatrix}, \\
\mathcal{P} &= \begin{pmatrix} 1 & F \\ I & F \end{pmatrix}, \\
\mathcal{L} &= \begin{pmatrix} 1 & I \\ I & I \end{pmatrix}, \\
\mathcal{F} &= \begin{pmatrix} 1 & I \\ I & F \end{pmatrix}
\end{align*}
\]
An Interesting Example

\[ \mathcal{F} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & F & 1 \\ F & F & 1 \end{pmatrix} \]

\begin{align*}
&x_0 \quad x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7 \\
&\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \\
&\oplus \quad \oplus \quad \oplus \quad \oplus \quad \oplus \quad \oplus \quad \oplus \quad \oplus \\
\end{align*}
An Interesting Example

\[ \mathcal{L} = \begin{pmatrix}
1 & 1 & 1 \\
1 & 1 & \vdots \\
\vdots & \ddots & 1 \\
\vdots & \vdots & \ddots & 1 \\
1 & 1 & 1
\end{pmatrix} \]
An Interesting Example

\[ N = \begin{pmatrix} 
1 & 1 & 1 \\
F & 1 & \\
F & F & 1 \\
F & F & F & 1 \\
\end{pmatrix} \]

\[ \begin{array}{cccccccc}
X_0 & X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & X_7 \\
\end{array} \]

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/linearly active S-boxes ranges from 26 to 42 as \( P \) varies.
An Interesting Example

\[ \mathcal{N} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & F & 1 \\ F & I & 1 \\ F & I & I & 1 \end{pmatrix} \]

- \( \mathcal{P} \): Swap emitters and receivers

\[ \mathcal{P} = \begin{pmatrix} 0 & P_1 \\ P_2 & 0 \end{pmatrix} \]

If \( \mathcal{P} \) swaps \( k_{i-1} \) and \( k_{i+1} \) then \( d = 4 \).

Choose \( \mathcal{P}'_1 \) and \( \mathcal{P}'_2 \) to best resist attacks not (directly) related to \( d \). E.g. for \( k = 16 \) and 20 rounds, minimum number of differentially/lineally actives S-boxes ranges from 26 to 42 as \( \mathcal{P} \) varies.
An Interesting Example

\[ \mathcal{N} = \begin{pmatrix} 1 & 1 & 1 \\ F & 1 \\ F & F & 1 & 1 \end{pmatrix} \]

- \( \mathcal{P} \) : Swap emitters and receivers

\[ \mathcal{P} = \begin{pmatrix} 0 & P'_1 & 0 \\ 0 & \ddots & \ddots \\ 0 & 0 & 1 \end{pmatrix} \]

- If \( \mathcal{P} \) swaps \( k - 1 \) and \( \frac{k}{2} - 1 \) then \( d = 4 \).
An Interesting Example

\[ \mathcal{N} = \begin{pmatrix} 1 & 1 & 1 \\ F & 1 & 1 \\ F & F & 1 & 1 \end{pmatrix} \]

- \( \mathcal{P} \): Swap emitters and receivers

\[ \mathcal{P} = \begin{pmatrix} 0 & P'_1 & \cdots & 0 \\ 0 & \cdots & 1 \end{pmatrix} \]

- 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.
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?