Type 1.x Generalized Feistel Structures

Shingo Yanagihara and Tetsu Iwata
Nagoya University, Japan
WCC 2013,
April 15-19, 2013, Bergen (Norway)
Generalized Feistel Structure (GFS)

- The same computation of the nonlinear functions in encryption and decryption

- Poor diffusion property
  - It requires many rounds to be secure.
• Generally, GFS has the sub-block-wise cyclic shift ($\pi_s$).
- Generally, GFS has the sub-block-wise cyclic shift ($\pi_s$).
Previous work
[FSE 2010, Suzaki, Minematsu]

• Changing the permutation of Type 2 GFS from $\pi_S$
• There are permutations such that
  – the diffusion property and
  – the security against several attacks
    are better than $\pi_S$.  

The diffusion property and
the security improve.
Previous work

[IEICE 2013, Yanagihara, Iwata]

• FD (full diffusion): every output sub-blocks depend on all input sub-blocks

• For Type 1 GFS
  – $\pi_s$: the worst permutation in terms of the diffusion property among permutations archive FD.
  – The construction of the best permutation
Previous work
[IEICE 2013, Yanagihara, Iwata]

• For Type 3 GFS,
  – The condition of a permutation which cannot archive FD with any number of rounds.

• For Source-Heavy and Target-Heavy GFSs
  – $\pi_s$ : the best permutation in terms of the diffusion property.
Example of unclassified types of GFS

• Key schedule function of TWINE [SAC 2012]
  – Two nonlinear functions in $\mathcal{F}$-Layer
Our work

• Propose Type 1.x GFS
  – covers Type 1 and Type 2 GFSs as special cases
• Propose a construction of a permutation for Type 1.x GFS with two nonlinear functions in F-Layer
• Present analysis of Type 1.x GFS with $\pi_s$
  – compare proposed construction with $\pi_s$
• Show experimental results for Type 1.x GFS for $3 \leq d \leq 8$
Type 1.x \((d, \eta)\) GFS

d sub-blocks \((d \geq 3)\)

\[ \eta \text{ nonlinear functions} \quad (1 \leq \eta \leq \lfloor d/2 \rfloor) \]

- Type 1.x \((d, 1)\) GFS ⇔ Type 1 GFS
- Type 1.x \((d, d/2)\) GFS (\(d\) is even) ⇔ Type 2 GFS
Notation

- $\pi_s = (d - 1, 0, 1, \ldots, d - 2)$ (left cyclic shift)
- $\pi(i)$: the sub-block after applying $\pi$ to the $i$-th sub-block.
- $r_{ij}$: the smallest number $r$ such that $\pi^r(i) = j$. 

\[\pi = (5, 0, 1, 2, 3, 4) = \pi_s\]
DRmax
[Suzaki, Minematsu, FSE 2010]

- $\text{DRmax}^{(d, \eta)}(\pi)$: The smallest round such that every output sub-blocks depend on all input sub-blocks.
DRmax
[Suzaki, Minematsu, FSE 2010]

- $\text{DR}_{\text{max}}^{(d, \eta)}(\pi)$: The smallest round such that every output sub-blocks depend on all input sub-blocks.

$\text{DR}_{\text{max}}^{(3,1)}_{E,0}(\pi_s) = 2$

$\text{DR}_{\text{max}}^{(3,1)}_{E,1}(\pi_s) = 3$

$\text{DR}_{\text{max}}^{(3,1)}_{E,2}(\pi_s) = 4$
\( \text{DR}_{D,0}^{(3,1)}(\pi_s) = 3 \)

\( \text{DR}_{D,1}^{(3,1)}(\pi_s) = 5 \)

\( \text{DR}_{D,2}^{(3,1)}(\pi_s) = 4 \)

\( \text{DR}_{D}^{(3,1)}(\pi_s) = 5 \)
Proposed construction for $\eta = 2$

Let $d \geq 5$ and $a$ be an integer such that $1 \leq a \leq d - 3$

$$\pi_p = \begin{cases} 
(1, 3, 4, 2, 5, 6, \ldots, d - 1, 0) & \text{if } a = 1 \\
(1, 4, 0, 2, 5, 6, \ldots, d - 1, 3) & \text{if } a = d - 3 \\
(1, 4, a + 3, 2, 5, 6, \ldots, a + 2, 3, a + 4, a + 5, \ldots, d - 1, 0) & \text{otherwise}
\end{cases}$$

Type 1.x (9,2) GFS with $\pi_p$ when $a = 1$
Properties of the proposed construction $\pi_p$

\[ r_{01} = r_{32} = 1,\ r_{13} = a,\ r_{20} = d - 2 - a \]
DRmax of the proposed construction

Lemma Let $d \geq 5$. Then we have $\text{DRmax}^{(d,2)}(\pi_p) = 2d - 4$.

• Brief overview of the proof:
Using the property,

– The largest DRmax for encryption is
  \[ \text{DRmax}_{E,\pi_p(2)}^{(d,2)}(\pi_p) = 2(r_{13} + r_{20}) = 2d - 4 \]
– The largest DRmax for decryption is $2d - 4$, because the structures of encryption and decryption are equivalent.
Equivalence of the structure

0 \quad 1 \quad 2 \quad 3

\[ F_0 \quad F_1 \]

\[ a \text{ rounds} \quad d - 2 - a \text{ rounds} \]
Equivalence of the structure

\[ F_0 \rightarrow F_1 \]

\[ a \text{ rounds} \quad d - 2 - a \text{ rounds} \]
Equivalence of the structure

\[ F_1 \]

\[ F_0 \]

\[ a \text{ rounds} \]

\[ d - 2 - a \text{ rounds} \]
Equivalence of the structure
**Lemma**: For any \( d \geq 3 \) and \( 1 \leq \eta \leq \lfloor d/2 \rfloor \), we have

\[
\text{DRmax}_{D, 2\eta-3}^{(d, \eta)}(\pi_s) = \max\{\text{DRmax}_{D, 2\eta-3}^{(d, \eta)}(\pi_s), \text{DRmax}_{D, 2\eta-1}^{(d, \eta)}(\pi_s)\},
\]

where

\[
\text{DRmax}_{D, 2\eta-3}^{(d, \eta)}(\pi_s) = \begin{cases} \left(\frac{d-2}{\eta}\right)(d-\eta) + 2 & \text{if } (d-2) \text{ mod } \eta = 0 \\ \left\lfloor\frac{d-2}{\eta}\right\rfloor(d-2\eta) + 2(d-\eta) & \text{otherwise} \end{cases}
\]

and

\[
\text{DRmax}_{D, 2\eta-1}^{(d, \eta)}(\pi_s) = \begin{cases} \left(\frac{d-1}{\eta}\right)(d-\eta) + 1 & \text{if } (d-1) \text{ mod } \eta = 0 \\ \left\lfloor\frac{d-1}{\eta}\right\rfloor(d-2\eta) + 2(d-\eta) & \text{otherwise}. \end{cases}
\]
Brief overview of the proof

• For encryption
Brief overview of the proof

• For encryption
Brief overview of the proof

• For encryption
Brief overview of the proof

- For encryption

\[ d - 1 \text{ rounds} \]
Brief overview of the proof

• For encryption

\[ d - 1 \text{ rounds} \]
Brief overview of the proof

• For encryption

\[ d - 1 \text{ rounds} \quad DR_{\text{max}}^{(d, \eta)}_{E, d-1}(\pi_s) = 2d - 2\eta \]

\[ d - 2\eta + 1 \text{ rounds} \]
Brief overview of the proof

• For decryption direction

\[
\text{DR}_{D,2\eta-3}^{(d,\eta)}(\pi_s) \geq 2d - 2\eta
\]

\[
\text{DR}_{D,2\eta-1}^{(d,\eta)}(\pi_s) \geq 2d - 2\eta
\]

\[
\text{DR}_{D}^{(d,\eta)}(\pi_s) = \max\{\text{DR}_{D,2\eta-3}^{(d,\eta)}(\pi_s), \text{DR}_{D,2\eta-1}^{(d,\eta)}(\pi_s)\}
\]
A comparison of two lemmas

Good

Bad

diffusion property

\[ \text{DR}_{\text{max}}(d,2)(\pi) \]

\[ \pi_s \]

\[ \pi_p \]
Experimental results

• Compute $\text{DR}_{\text{max}}^{(d, \eta)}(\pi)$ for all $3 \leq d \leq 8$ and $1 \leq \eta \leq \lfloor d/2 \rfloor$.

• List $\pi_s$ and all optimum permutations in terms of the diffusion property.

• Present only the lexicographically first permutations in the equivalent classes.

• Result for $\eta = 1$ is analyzed in [IEICE 2013]
Result for $\eta = 2$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\pi$</th>
<th>DRmax</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$(1, 3, 0, 2)_p^1$</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 1, 2)_s$</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>$(1, 3, 4, 2, 0)_p^1$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 0, 2, 3)_p^2$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 4, 2, 1)_s$</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>$(1, 3, 4, 2, 5, 0)_p^1$</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 0, 2, 5, 3)_p^3$</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 5, 2, 3, 0)_p^2$</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 4, 2, 5, 1)_s$</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$(3, 4, 5, 0, 2, 1)$</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>$(1, 3, 4, 2, 5, 6, 0)_p^1$</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 0, 2, 5, 6, 3)_p^4$</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 5, 2, 3, 6, 0)_p^2$</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 5, 2, 6, 0, 3)_p^3$</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 4, 2, 5, 6, 1)_s$</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>$(1, 3, 4, 2, 5, 6, 7, 0)_p^1$</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 0, 2, 5, 6, 7, 3)_p^3$</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 5, 2, 3, 6, 7, 0)_p^2$</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 5, 2, 6, 0, 7, 3)_p^4$</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$(1, 4, 5, 2, 6, 7, 3, 0)_p^3$</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 4, 2, 5, 6, 7, 1)_s$</td>
<td>24</td>
</tr>
</tbody>
</table>

- **Subscript**
  - $s$: it is equivalent to $\pi_s$.
  - $p$: it is equivalent to $\pi_p$.

- **Superscript**
  - the integer $\alpha$ for $\pi_p$.

- For $d \geq 5$, there are better permutations than $\pi_s$. 

33
• Permutations in green are analyzed in [FSE 2010].
Result for $\eta = 4$

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\pi$</th>
<th>DRmax</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>$(1, 2, 4, 0, 7, 6, 5, 3)$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(1, 2, 5, 0, 3, 6, 7, 4)$</td>
<td>6 [FSE 2010]</td>
</tr>
<tr>
<td></td>
<td>$(1, 2, 5, 6, 7, 4, 3, 0)$</td>
<td>6 [FSE 2010]</td>
</tr>
<tr>
<td></td>
<td>$(1, 2, 5, 7, 3, 0, 4, 6)$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(1, 3, 5, 6, 7, 4, 0, 2)$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(1, 3, 5, 7, 0, 2, 4, 6)$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(2, 4, 7, 5, 1, 0, 3, 6)$</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 1, 4, 7, 2, 5, 6)$</td>
<td>6 [FSE 2010]</td>
</tr>
<tr>
<td></td>
<td>$(3, 0, 5, 2, 7, 4, 1, 6)_s$</td>
<td>8</td>
</tr>
</tbody>
</table>

- Some permutations do not exist in [FSE 2010] results.
  - Because [FSE 2010] paper observed “even-odd shuffles”. (instead of all permutations)
Conclusion

• Proposed Type 1.x GFS
  – covers Type 1 and Type 2 GFSs
• Proposed a construction $\pi_p$ for Type 1.x GFS
• Analysis of Type 1.x GFS with $\pi_s$
  – compared $\pi_p$ to $\pi_s$ in terms of the diffusion property
• Showed experimental results for Type 1.x GFS for $3 \leq d \leq 8$
Future work

• Analyze the security against various attacks
  – differential, linear, impossible differential, and saturation attacks
• Design optimum permutations for $\eta \geq 3$. 