Feistel-like Structures Revisited: Classification and Cryptanalysis

Bing Sun, Zejun Xiang, Zhengyi Dai, Guoqiang Liu, Xuan Shen, Longjiang Qu, and Shaojing Fu

National University of Defense Technology
Hubei University

Overview

Iteration structures for block ciphers

- Encryption is similar to decryption?
  - SPN structure, Feistel-like structure.
- Feistel-like structure
  - Feistel structure, Lai-Massey structure, Source-Heavy Generalised Feistel Structure, Target-Heavy Generalised Feistel Structure.
  - Source-Heavy Generalised Feistel Structure (SH GFS): SM4 structure.
  - Target-Heavy Generalised Feistel Structure (TH GFS): Mars structure.

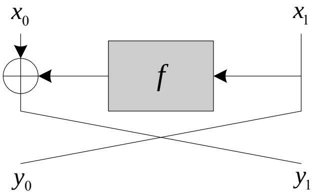

Figure: The Feistel structure

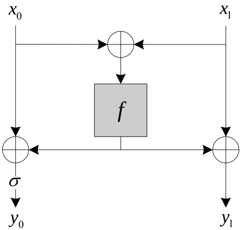

Figure: The Lai-Massey structure

Unified structure

- The condition that encryption and decryption are similar:

$$A_0B_0 \oplus A_1B_1 \oplus \cdots \oplus A_{d-1}B_{d-1} = 0.$$

- π is a branch permutation.

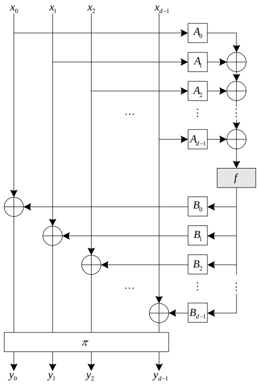

Figure: The unified structure

Numerous Feistel-like structures

The link among different structures

- If permutations π are different, some cryptographic properties remain the same for some Feistel-like structures.
- SM4-like and Mars-like structures cover the same number of rounds for the longest impossible differentials and the longest zero correlation linear hulls.
- The generic results of the meet-in-the-middle attacks against both SH GFS and TH GFS are the same.

Question 1:

Is there any equivalence for the universal cases between different structures?

- SM4-like and Mars-like structures
- SH GFS and TH GFS

Cryptanalysis of Iterative Structures

- Known cryptanalytic vectors.
- Provable security.

Links of impossible differentials, zero correlation linear hulls and integral distinguishers.

- The impossible differential of a structure is equivalent to the zero correlation linear hull of its dual structure.
- A zero correlation linear hull always implies the existence of an integral distinguisher.
- The matrix representation and mirror function link these three distinguishers of Feistel-like structures.

Question 2:

For what kind of structures are the impossible differentials equivalent to the zero correlation linear hulls?

Full-Diffusion Round and the Provable Security

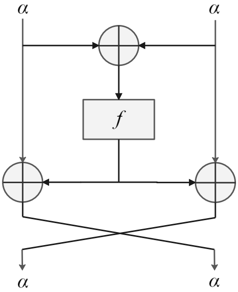

Figure: Insecure structure

There is a probability 1 differential which covers any rounds.

Question 3:

Is it possible to redefine the full-diffusion round such that the provable security evaluations of the unified structures against impossible differentials and zero correlation linear cryptanalysis can also be covered?

A Compact Description for the Unified Structure

Notations

- $A, B : \mathbb{F}_2^{nd} \mapsto \mathbb{F}_2^t$, $f : \mathbb{F}_2^t \mapsto \mathbb{F}_2^t$, $\mathbb{B}(t)$: all the mappings over $\mathbb{F}_2^t$, π is a branch permutation.
- A mapping from $\mathbb{F}_2^{nd}$ to $\mathbb{F}_2^{nd}$: $F_{A,B,\pi}(f)(X) = \pi\left(X \oplus B^{\mathrm{T}} f(AX)\right)$.
- The Unified Structure: $\mathcal{F}_{A,B,\pi} = \{F_{A,B,\pi}(f) | f \in \mathbb{B}(t)\}$.
- r-round iteration of $\mathcal{F}_{A,B,\pi}$:
  $\mathcal{F}_{A,B,\pi}^{(r)} = \{\pi^{-1} \circ F_{A,B,\pi}(f_r) \circ \cdots \circ F_{A,B,\pi}(f_1) | f_1, \ldots, f_r \in \mathbb{B}(t)\}$.

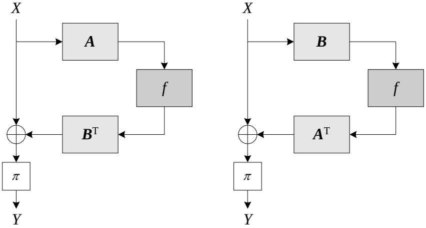

Figure: The Unified Structure $\mathcal{F}_{A,B,\pi}$ and Its Dual Structure $\mathcal{F}_{A,B,\pi}^{\perp}$

Examples: SM4-like Structure and Mars-like Structure

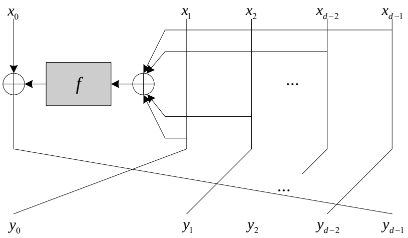

Figure: The SM4-like structure

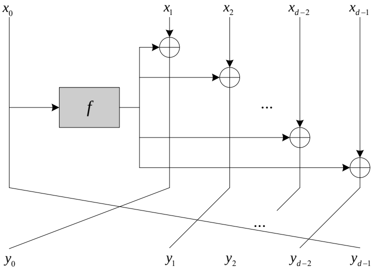

Figure: The Mars-like structure

SM4 structure and Mars structure

- SM4 structure: $A_{\rm S} = [O, I, I, I]$, $B_{\rm S} = [I, O, O, O]$.
- Mars structure: $A_{\rm M} = [I, O, O, O]$, $B_{\rm M} = [O, I, I, I]$,

$$\pi_{\rm M} = \pi_{\rm S} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}.$$

Dual structure

Definition: Dual structure

The dual structure of $\mathcal{F}_{A,B,\pi}^{(r)}$ is defined as $\mathcal{F}_{A,B,\pi}^{(r)\perp} = \mathcal{F}_{B,A,\pi}^{(r)}$.

Proposition 1

The dual structure of SM4 structure is Mars structure, and vice versa.

Denote:

$$\mathcal{A}^r = \begin{pmatrix} A \\ A\pi \\ \vdots \\ A\pi^{r-1} \end{pmatrix}, \quad \mathcal{B}^r = \begin{pmatrix} B \\ B\pi \\ \vdots \\ B\pi^{r-1} \end{pmatrix}.$$

Some conclusions for $\mathcal{F}_{A,B,\pi}$

Proposition 2

Let $\mathcal{F}_{A,B,\pi}$ be the unified structure with d n-bit branches. The following conclusions hold.

- $\mathcal{F}_{A,B,\pi}$ is invertible if and only if $AB^{\mathrm{T}} = 0$.
- There exists an integer r such that

  $$\mathrm{rank}\,(\mathcal{A}^r) = \mathrm{rank}\,(\mathcal{B}^r) = nd.$$

  Otherwise, there always exists a differential characteristic with probability 1 for an arbitrary number of rounds.
- $\alpha \to \beta$ is an r-round impossible differential of $\mathcal{F}^{(r)}_{A,B,\pi}$ if and only if $\alpha \to \beta$ is an r-round zero correlation linear hull of $\mathcal{F}^{(r)}_{B,A,\pi}$.

Research objective

Definition: Regular Unified Structure

A unified structure $\mathcal{F}_{A,B,\pi}$ with d n-bit branches is said to be regular if the following 5 conditions are satisfied:

- $AB^{\mathrm{T}} = 0$;
- sizes of the round functions equal the size of the branch;
- the round functions are permutations;
- the order of π equals the number of branches, i.e., $\mathrm{ord}(\pi) = d$;
- $\mathrm{rank}(\mathcal{A}^d) = \mathrm{rank}(\mathcal{B}^d) = nd$, i.e., both $\mathcal{A}^d$ and $\mathcal{B}^d$ are invertible matrices.

Affine equivalence between ciphers

Definition: Affine Equivalence between Ciphers

Let $E_1(\cdot, k)$ and $E_2(\cdot, k)$ be two block ciphers. If there are bijective affine mappings P and Q, such that for any X and k,

$$E_2(X, k) = QE_1(P(X), k),$$

the two ciphers $E_1(\cdot, k)$ and $E_2(\cdot, k)$ are defined to be affine equivalent.

Remark:

1. If $c = E_2(m, k)$, then $Q^{-1}(c) = E_1(P(m), k)$.
2. The security of DES is independent of the initial permutation IP.

Affine equivalence between structures

Definition: Affine Equivalence between Structures

Two unified structures $\mathcal{E}_1$ and $\mathcal{E}_2$ are said to be affine equivalent if there exist two affine mappings P and Q that establish a one-to-one correspondence between sets of all instances of $\mathcal{E}_1$ and $\mathcal{E}_2$ in the following manner:

- For any instance $E_1 \in \mathcal{E}_1$, the transformation $Q \circ E_1 \circ P$ results in an instance within $\mathcal{E}_2$.
- Conversely, for any instance $E_2 \in \mathcal{E}_2$, the transformation $Q^{-1} \circ E_2 \circ P^{-1}$ results in an instance within $\mathcal{E}_1$.

This relationship is denoted by $\mathcal{E}_1 \sim \mathcal{E}_2$ and can be expressed as $\mathcal{E}_2 = Q \circ \mathcal{E}_1 \circ P$.

Remark: The affine equivalence between structures forms an equivalent relation.

Normalized form

Lemma 1: $\mathscr{X}$-type normalized form

Let $\mathcal{F}_{A,B,\pi}^{(r)}$ be an r-round d-branch regular unified structure. Then, $\mathcal{F}_{A,B,\pi}^{(r)}$ is affine equivalent to $\mathcal{F}_{\dot{A},\dot{B},\dot{\pi}}^{(r)}$, where

$$\begin{cases} \dot{A} = [I, O, O, \cdots, O], \\ \dot{B} = \left[O, \left(A\pi B^{\mathrm{T}}\right)^{\mathrm{T}}, \left(A\pi^2 B^{\mathrm{T}}\right)^{\mathrm{T}}, \cdots, \left(A\pi^{d-1} B^{\mathrm{T}}\right)^{\mathrm{T}}\right], \\ \dot{\pi} = \begin{pmatrix} 0 & 1 & 2 & \cdots & d-2 & d-1 \\ d-1 & 0 & 1 & \cdots & d-3 & d-2 \end{pmatrix}. \end{cases}$$

To be specific, for any $f_1, \ldots, f_r \in \mathbb{B}(n)$, we have

$$F_{A,B,\pi}(f_r, \ldots, f_1) = \left(\mathcal{A}^d\right)^{-1} \circ F_{\dot{A},\dot{B},\dot{\pi}}(f_r, \ldots, f_1) \circ \mathcal{A}^d.$$

Moreover, $\mathcal{F}_{\dot{A},\dot{B},\dot{\pi}}^{(r)}$ is called the $\mathscr{X}$-type normalized form of $\mathcal{F}_{A,B,\pi}^{(r)}$.

Normalized form

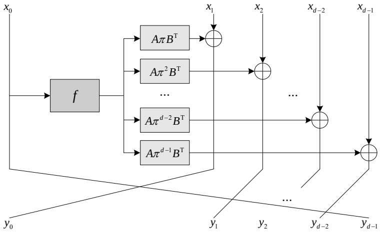

Figure: The $\mathscr{X}$-type Normalized Form of $\mathcal{F}_{A,B,\pi}$

Corollary 1

Let $\mathcal{F}^{(r)}_{A_1,B_1,\pi_1}$ and $\mathcal{F}^{(r)}_{A_2,B_2,\pi_2}$ be two r-round d-branch regular unified structures. Then, $\mathcal{F}^{(r)}_{A_1,B_1,\pi_1} \sim \mathcal{F}^{(r)}_{A_2,B_2,\pi_2}$ if the following equation holds for $i = 1, 2, \ldots, d-1$:

$$A_1\pi_1^i B_1^{\mathrm{T}} = A_2\pi_2^i B_2^{\mathrm{T}}.$$

Example

Example: SM4 structure and Mars structure are equivalent.

$$\mathcal{E}_{\mathrm{SM4}} = \begin{pmatrix} O & I & I & I \\ I & O & I & I \\ I & I & O & I \\ I & I & I & O \end{pmatrix} \circ \mathcal{E}_{\mathrm{Mars}} \circ \begin{pmatrix} O & I & I & I \\ I & O & I & I \\ I & I & O & I \\ I & I & I & O \end{pmatrix}.$$

Remark: SM4 and Mars ciphers are affine equivalent if these two ciphers use the same round function and round keys.

Normalized form

Lemma 2: $\mathscr{D}$-type normalized form

Let $\mathcal{F}_{A,B,\pi}^{(r)}$ be an r-round d-branch regular unified structure. Then, $\mathcal{F}_{A,B,\pi}^{(r)}$ is affine equivalent to $\mathcal{F}_{\mathring{A},\mathring{B},\mathring{\pi}}^{(r)}$, where

$$\begin{cases} \mathring{A} = \left[O, A\pi^{d-1}B^{\mathrm{T}}, A\pi^{d-2}B^{\mathrm{T}}, \cdots, A\pi B^{\mathrm{T}}\right], \\ \mathring{B} = [I, O, O, \cdots, O], \\ \mathring{\pi} = \begin{pmatrix} 0 & 1 & 2 & \cdots & d-2 & d-1 \\ d-1 & 0 & 1 & \cdots & d-3 & d-2 \end{pmatrix}. \end{cases}$$

Moreover, $\mathcal{F}_{\mathring{A},\mathring{B},\mathring{\pi}}^{(r)}$ is called the $\mathscr{D}$-type normalized form of $\mathcal{F}_{A,B,\pi}^{(r)}$.

Normalized form

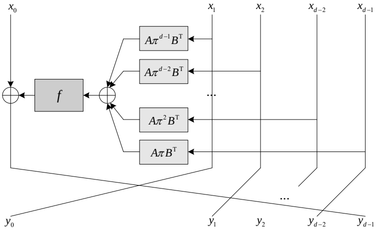

Figure: The $\mathscr{D}$-type Normalized Form of $\mathcal{F}_{A,B,\pi}$

Theorem 1: The equivalence between SH GFS and TH GFS

Every SH GFS corresponds to an affine equivalent TH GFS, and vice versa. This equivalence establishes that, from a security standpoint, the design of new ciphers can focus on either structure without losing better possibilities, as both provide equivalent cryptographic properties.

Self-equivalent structure

Definition: Self-Equivalent Structure

Let $\mathcal{E}$ be a structure and $\mathcal{E}^{\perp}$ be its dual structure. If $\mathcal{E} \sim \mathcal{E}^{\perp}$, $\mathcal{E}$ is called a self-equivalent structure.

Remark: Evaluating the security of $\mathcal{E}$ against zero correlation linear cryptanalysis is equivalent to evaluating the security of $\mathcal{E}^{\perp}$ against impossible differential cryptanalysis.

Corollary 2

Let $\mathcal{F}_{A,B,\pi}^{(r)}$ be an r-round d-branch regular unified structure. Then, $\mathcal{F}_{A,B,\pi}^{(r)}$ is a self-equivalent structure if the following equation holds for $i = 1, 2, \ldots, d-1$:

$$A\pi^i B^{\mathrm{T}} = B\pi^i A^{\mathrm{T}}.$$

Proposition 3

Both $\mathcal{E}_{\mathrm{SM4}}$ and $\mathcal{E}_{\mathrm{Mars}}$ are self-equivalent structures.

Self-equivalent structure

Theorem 2

Let $\mathcal{F}_{A,B,\pi}^{(r)}$ be an r-round d-branch regular unified structure, and both A and B are block matrices whose elements are either identity matrix I or zero matrix O. If $A \oplus B = [I, I, \ldots, I]$, $\mathcal{F}_{A,B,\pi}^{(r)}$ is a self-equivalent structure.

Lemma 3

There is a one-to-one correspondence between the impossible differentials and zero correlation linear hulls of a self-equivalent structure. Thus, for a self-equivalent structure, the longest impossible differential covers exactly the same rounds as the longest zero correlation linear hull.

Self-equivalent structure

$$
\begin{array}{ccccccc}
\alpha & & \alpha & & \alpha & & (P^{-1})^{\mathrm{T}}\alpha \\
\downarrow & & \downarrow & & \downarrow P & & \downarrow \\
\mathcal{E} & \Leftrightarrow & \mathcal{E}^{\perp} & \Leftrightarrow & \mathcal{E} & \Leftrightarrow & \mathcal{E} \\
\downarrow & & \downarrow & & \downarrow Q & & \downarrow \\
\beta & & \beta & & \beta & & Q^{\mathrm{T}}\beta \\
(\mathrm{ID}) & & (\mathrm{ZC}) & & (\mathrm{ZC}) & & (\mathrm{ZC})
\end{array}
$$

Theorem 3

Let $\mathcal{F}_{A,B,\pi}$ be a self-equivalent structure, and denote by R_I, R_{ID} and R_{ZC} the maximal rounds of the integral distinguisher, the impossible differential and zero correlation linear hull of $\mathcal{F}_{A,B,\pi}$, respectively. Then we have:

$$R_{ID} = R_{ZC} \leq R_I.$$

Remark: The security of a block cipher against integral attacks covers the security against impossible differential and zero correlation linear attacks.

Notations

Three types of differential propagations of the round functions for a regular unified structure.

- 0 difference always propagates to 0.
- A non-zero difference $\epsilon \in \mathbb{F}_2^n/\{0\}$ always propagates to $V_\epsilon = \mathbb{F}_2^n/\{0\}$.
- An undetermined difference $\delta \in \mathbb{F}_2^n$, which can be either zero or non-zero, always propagates to $V_\delta = \mathbb{F}_2^n$.

Refined full-diffusion round

Definition: Refined Full-Diffusion Round

Let $E^{(r)}$ be an r-round n-bit iterative block cipher. The maximal integer R satisfying the following condition is called the refined full-diffusion round of E: there is an input difference $\Delta_I \neq 0$, two matrices L_I and $L_O \neq O$, such that for any $\Delta_O^{(r)} \in \{E^{(R)}(x) \oplus E^{(R)}(x \oplus \Delta_I) | x \in \mathbb{F}_2^n\}$,

$$L_I \Delta_I \oplus L_O \Delta_O^{(r)} = O.$$

Let $\mathcal{E}$ be an n-bit iterative structure. The maximal integer R satisfying the following condition is called the refined full-diffusion round of $\mathcal{E}$: there is an input difference $\Delta_I \neq 0$, two matrices L_I and $L_O \neq O$, such that for any $\Delta_O^{(r)} \in \{E^{(R)}(x) \oplus E^{(R)}(x \oplus \Delta_I) | x \in \mathbb{F}_2^n, E^{(R)} \in \mathcal{E}^{(R)}\}$,

$$L_I \Delta_I \oplus L_O \Delta_O^{(r)} = 0.$$

Refined full-diffusion round

Proposition 4

The refined full-diffusion round of the structure deduced from AES is 2.

Theorem 4

Let $\mathcal{F}_{A,B,\pi}^{(r)}$ be an r-round d-branch regular unified structure. Then, the refined full-diffusion round of $\mathcal{F}_{A,B,\pi}$ is $2d-2$, provided $A\pi^i B^{\mathrm{T}}$'s are invertible for $i = 1, 2, \cdots, d-1$.

Refined full-diffusion round

Algorithm 1 Calculate refined full-diffusion round of $\mathcal{F}_{A,B,\pi}$

procedure RFDR(A, B, π, d) ▷ d is the number of branches
  matrix $Q \leftarrow [O, O, \cdots, O]^{\mathrm{T}}$
  $r \leftarrow d - 1$
  while $\mathrm{rank}(Q) < nd$ **do**
    if $r \bmod d = d - 1$ or $AQ \neq O$ **then**
      $Q \leftarrow [\pi Q \mid \pi B^{\mathrm{T}}]$
    else
      $Q \leftarrow \pi Q$
    end if
    $r \leftarrow r + 1$
  end while
  return $r - 1$
end procedure

Refined full-diffusion round

Proposition 5

The refined full-diffusion rounds of the Feistel, SM4 and Mars structures are 2, 6 and 6, respectively, if the round functions are permutations.

The number of rounds for the longest impossible differential

Theorem 6

Let $\mathcal{F}^{(r)}_{A,B,\pi}$ be an r-round d-branch regular unified structure. Denote by RFDR the refined full-diffusion round of $\mathcal{F}_{A,B,\pi}$. Then, the longest impossible differential of $\mathcal{F}_{A,B,\pi}$ covers exactly

$$\frac{3}{2}\mathrm{RFDR} + 2 = 3d - 1$$

rounds, provided $A\pi^i B^{\mathrm{T}}$'s are invertible for $i = 1, 2, \cdots, d - 1$.

Proposition 6

The longest impossible differential in a standard Feistel structure spans exactly five rounds, and in the SM4 structure, it spans exactly eleven rounds, assuming that the round functions operate as random permutations.

Conclusion

The results could give new guidelines for both the design and cryptanalysis of Feistel-like ciphers.

- A source-heavy generalised Feistel cipher is always affine equivalent to a target-heavy generalised Feistel cipher with the same round functions f and same round key k.
- For self-equivalent structure, there is a one-to-one correspondence between the impossible differentials and the zero correlation linear hulls.
- For self-equivalent structure, the longest integral covers at least the rounds of the longest impossible differentials/zero correlation linear hulls.
- Both the longest impossible differential and zero correlation linear hull of the d-branch SM4-like structures cover exactly $3d - 1$ rounds.

Thanks For Your Attention!