Aalto University
School of Science

On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-type Ciphers

Céline Blondeau and Andrey Bogdanov and Meiqin Wang

Thursday June 12, 2014

ACNS

Outline

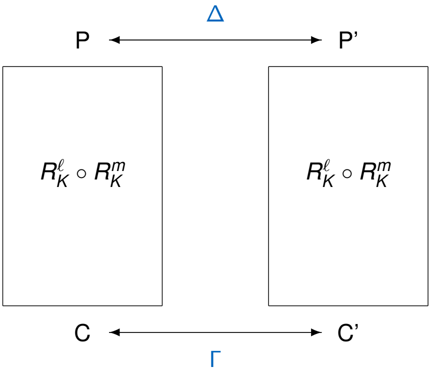
Outline

Impossible Differential (ID) Cryptanalysis

[Knudsen 1997]

ID distinguishers :

- Differentials which never occur
- Truncated differential (Δ, Γ) with probability 0



$$(0,0) \notin (\Delta, \Gamma)$$

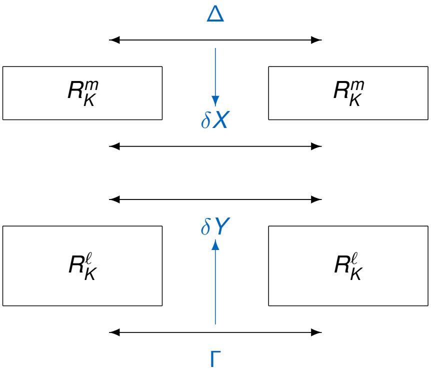
$$\mathbf{Pr}[\Delta \to \Gamma] = 0$$

Impossible Differential (ID) Cryptanalysis

[Knudsen 1997]

ID distinguishers :

- Differentials which never occur
- Truncated differential (Δ, Γ) with probability 0



$\mathbf{Pr}[\Delta \to \delta X] = 1$

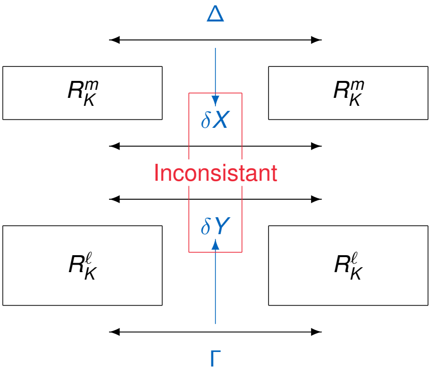
$\mathbf{Pr}[\Gamma \to \delta Y] = 1$

Impossible Differential (ID) Cryptanalysis

[Knudsen 1997]

ID distinguishers :

- Differentials which never occur
- Truncated differential (Δ, Γ) with probability 0



$\mathbf{Pr}[\Delta \to \delta X] = 1$

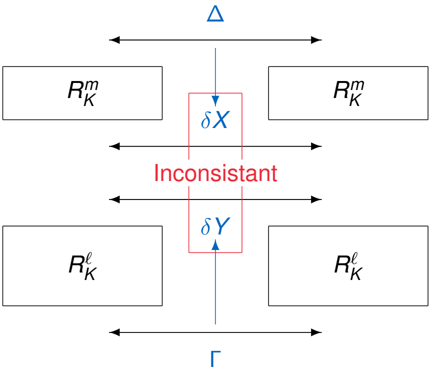
$\mathbf{Pr}[\Gamma \to \delta Y] = 1$

Impossible Differential (ID) Cryptanalysis

[Knudsen 1997]

ID distinguishers :

- Differentials which never occur
- Truncated differential (Δ, Γ) with probability 0



$$\mathbf{Pr}[\Delta \to \delta X] = 1$$

$$\mathbf{Pr}[\Delta \to \Gamma] = 0$$

$$\mathbf{Pr}[\Gamma \to \delta Y] = 1$$

Zero-Correlation (ZC) Linear Cryptanalysis

[Bogdanov et al 2012]

(Multidimensional) ZC distinguishers :

- Linear approximations with probability 1/2
- Multidimensional linear approximation (U, V) with capacity 0

$$u \cdot P$$

$$R_K^{\ell} \circ R_K^{m}$$

$$v \cdot C$$

$$(0,0) \notin (U, V)$$

$$\forall u \in U, \quad \forall v \in V,$$

$$\mathbf{Pr}[u \cdot P \oplus v \cdot C = 0] = \frac{1}{2}$$

Or equivalently,

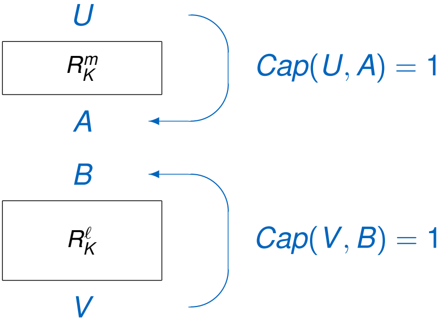
$$Cap(U, V) = 0$$

Zero-Correlation (ZC) Linear Cryptanalysis

[Bogdanov et al 2012]

(Multidimensional) ZC distinguishers :

- Linear approximations with probability 1/2
- Multidimensional linear approximation (U, V) with capacity 0

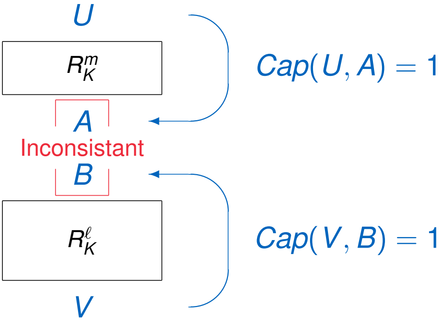


Zero-Correlation (ZC) Linear Cryptanalysis

[Bogdanov et al 2012]

(Multidimensional) ZC distinguishers :

- Linear approximations with probability 1/2
- Multidimensional linear approximation (U, V) with capacity 0

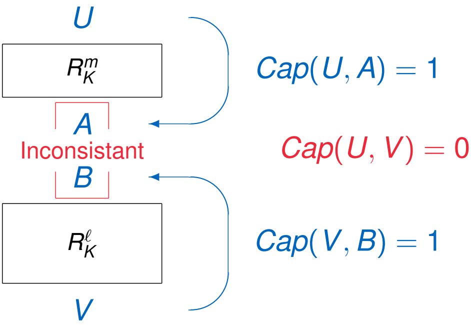


Zero-Correlation (ZC) Linear Cryptanalysis

[Bogdanov et al 2012]

(Multidimensional) ZC distinguishers :

- Linear approximations with probability 1/2
- Multidimensional linear approximation (U, V) with capacity 0

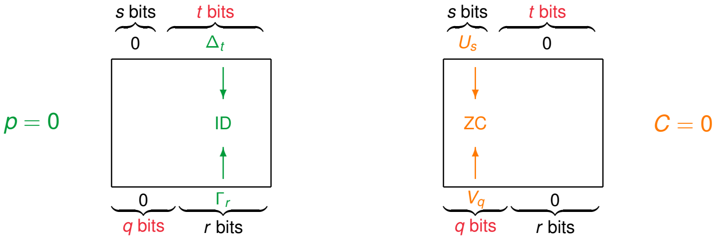


Mathematical Relation between ID and ZC

[Blondeau Nyberg 2013]

- TD : $[(0, \Delta_t), (0, \Gamma_r)]_{\Delta_t \in \mathbb{F}_2^t \setminus \{0\},\ \Gamma_r \in \mathbb{F}_2^r}$ with probability p
- ML : $[(U_s, 0), (V_q, 0)]_{U_s \in \mathbb{F}_2^s \setminus \{0\},\ V_q \in \mathbb{F}_2^q}$ with capacity C

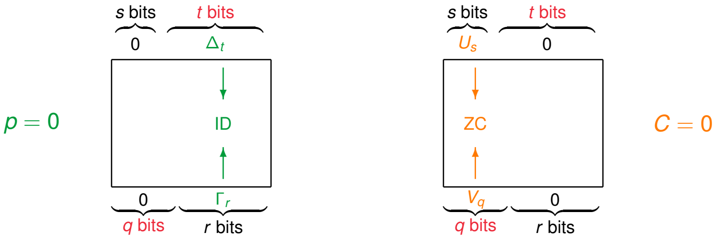
$$\frac{2^t - 1}{2^t} \cdot p = 2^{-q} \cdot (C + 1) - 2^{-t}$$



If $t = q$: ZC and ID distinguishers are mathematically equivalent

Mathematical Relation between ID and ZC

[Blondeau Nyberg 2013]



If $t = q$: ZC and ID distinguishers are mathematically equivalent

Observation :

- Independent of the cipher and its structure

However: $(2^t - 1)(2^{n-t} - 1) \approx 2^n$ IDs are involved

- In practice, the considered spaces are smaller

Outline

ID and ZC Distinguishers

Number of Rounds of the Distinguisher:

Ciphers	ID	ZC
LBlock / TWINE	14	14
MARS	11	11
SMS4	11	11
Skipjack	24	17
Skipjack (only rule A)	16	16
Four-Cell	18	12

ID and ZC Distinguishers

Number of Rounds of the Distinguisher:

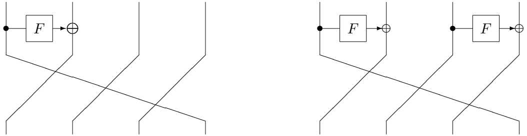
Ciphers	ID	ZC
LBlock / TWINE	14	14
MARS	11	11
SMS4	11	11
Skipjack	24	17
Skipjack (only rule A)	16	16
Four-Cell	18	12

Example of Patterns (for LBlock) :

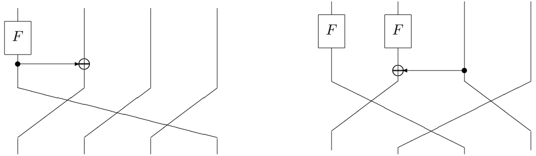
- Impossible differential :
  $(00000000, 00\Delta00000) \nrightarrow (0\Gamma000000, 00000000)$
- Zero correlation approximation :
  $(000U0000, 00000000) \nrightarrow (00000000, 0V000000)$

Example of Constructions

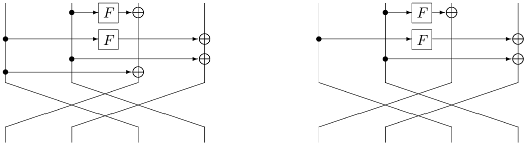
Feistel-Type



Skipjack-Type

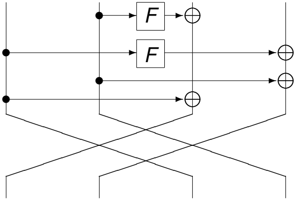


EGNF-Type



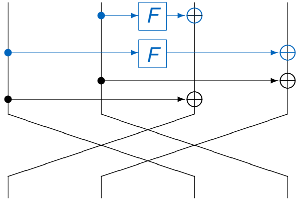
Representation of the Round Function

- F-layer
- X-layer
- P-layer



Representation of the Round Function

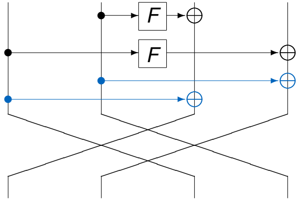
- F-layer
- X-layer
- P-layer



$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix},$$

Representation of the Round Function

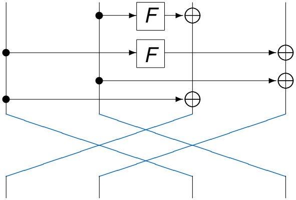
- F-layer
- X-layer
- P-layer



$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Representation of the Round Function

- F-layer
- X-layer
- P-layer

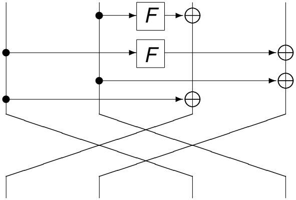


$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\mathcal{P} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

Representation of the Round Function

- F-layer
- X-layer
- P-layer

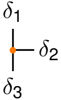


$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

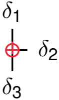
$$\mathcal{P} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$ and $\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$

Rules to find ZC and ID distinguishers

Differential Context :



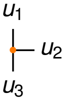
$\delta_3 = \delta_1 = \delta_2$



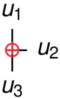
$\delta_3 = \delta_1 \oplus \delta_2$

$\delta_1 = \delta_2 = 0$
$\delta_1 \neq 0$ and $\delta_2 \neq 0$

Linear Context :



$u_3 = u_1 \oplus u_2$

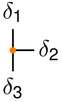


$u_3 = u_1 = u_2$

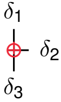
$u_1 = u_2 = 0$
$u_1 \neq 0$ and $u_2 \neq 0$

Rules to find ZC and ID distinguishers

Differential Context :



$\delta_3 = \delta_1 = \delta_2$

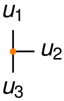


$\delta_3 = \delta_1 \oplus \delta_2$

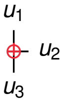
$\delta_1 = \delta_2 = 0$

$\delta_1 \neq 0$ and $\delta_2 \neq 0$

Linear Context :



$u_3 = u_1 \oplus u_2$



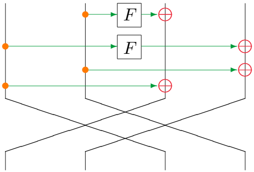
$u_3 = u_1 = u_2$

$u_1 = u_2 = 0$

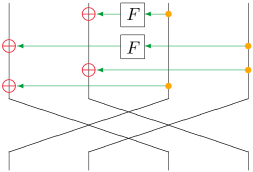
$u_1 \neq 0$ and $u_2 \neq 0$

$\oplus$ and • ”play orthogonal roles”

Mirror Round Function



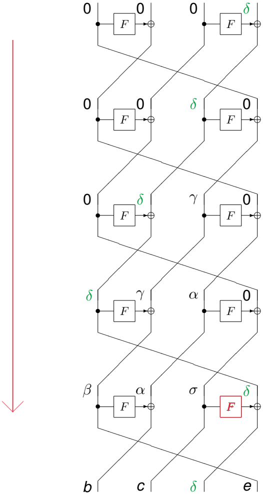
$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

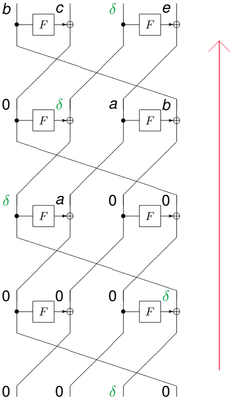


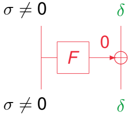
$$\mathcal{M} = \mathcal{P} \cdot \mathcal{X}^T \cdot \mathcal{F}^T$$

- $\mathcal{M}$ is the matrix representation of the mirror round function
- In general $\mathcal{M}^T \neq \mathcal{R}$
- Used to find ZC distinguishers [Soleimany Nyberg 2013]

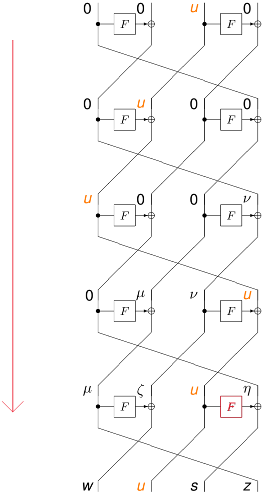
Example of ID distinguisher

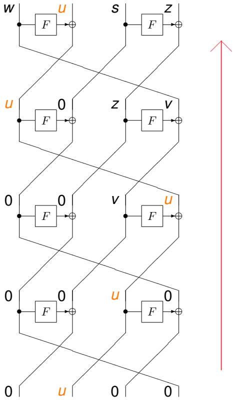


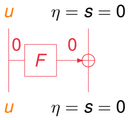




Example of ZC distinguisher







Matrix Method

Impossible Differential Context :

- Truncated input difference Δ
- Truncated output difference Γ

- If there is an inconsistency between $\mathcal{R}^m \cdot \Delta$ and $\mathcal{R}^{-\ell} \cdot \Gamma$, we have an ID on $m + \ell$ rounds

Zero-Correlation Context :

- Truncated input mask U
- Truncated output mask V

- If there is an inconsistency between $\mathcal{M}^m \cdot U$ and $\mathcal{M}^{-\ell} \cdot V$, we have a ZC on $m + \ell$ rounds

Equivalence between ID and ZC distinguishers

If it exists a linear relation between $\mathcal{M}$ and $\mathcal{R}$ or $\mathcal{R}^{-1}$,
the existence of an ID distinguisher involving *M* differentials is equivalent to the existence of a ZC distinguisher involving *M* linear masks.

Given $\mathcal{Q}$ a permutation matrix, the relation is

- Feistel-type ($\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$) :

$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$$

- Skipjack-type ($\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$) :

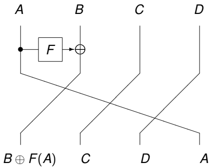
$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{F} \cdot \mathcal{P} \cdot \mathcal{X} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$$

- EGFN-type ($\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$) :

$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{R} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{F} \cdot \mathcal{P} \cdot \mathcal{X} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$$

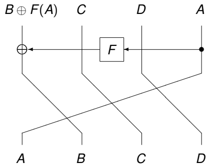
Illustration of the Proof for a Type-I Feistel

Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$$

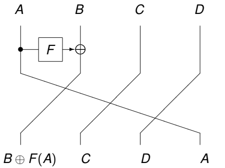
Inverse function



$$\begin{aligned}\mathcal{R}^{-1} &= \mathcal{P}^{-1} \cdot \mathcal{F}^{-1} \\ &= \mathcal{P}^{-1} \cdot (\mathcal{P} \cdot \mathcal{F}^{-1} \cdot \mathcal{P}^{-1})\end{aligned}$$

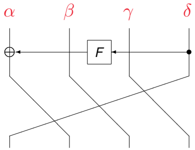
Illustration of the Proof for a Type-I Feistel

Round function



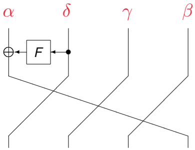
$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$$

Inverse function



$$\mathcal{R}^{-1} = \mathcal{P}^{-1} \cdot \mathcal{F}^{-1}$$

Permutation of the branches

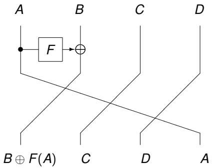


$$\mathcal{Q} \cdot \mathcal{R}^{-1} \cdot \mathcal{Q}^{-1}$$

$$(\alpha, \beta, \delta, \gamma) \rightarrow (\alpha, \delta, \gamma, \beta)$$

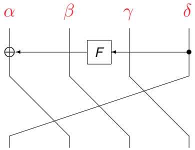
Illustration of the Proof for a Type-I Feistel

Round function



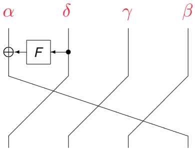
$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$$

Inverse function



$$\mathcal{R}^{-1} = \mathcal{P}^{-1} \cdot \mathcal{F}^{-1}$$

Permutation of the branches



$$\mathcal{Q} \cdot \mathcal{R}^{-1} \cdot \mathcal{Q}^{-1}$$

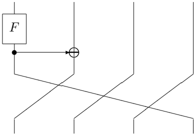
$$(\alpha, \beta, \delta, \gamma) \rightarrow (\alpha, \delta, \gamma, \beta)$$

$$\mathcal{M} = \mathcal{Q} \cdot \mathcal{R}^{-1} \cdot \mathcal{Q}^{-1}$$

$$\underbrace{\mathcal{M}^{m} \cdot U \not\equiv \mathcal{M}^{-\ell} \cdot V}_{\text{ZC on } m+\ell \text{ rounds}} \iff \underbrace{\mathcal{Q} \cdot \mathcal{R}^{-m} \cdot \mathcal{Q}^{-1} \cdot \Delta \not\equiv \mathcal{Q} \cdot \mathcal{R}^{\ell} \cdot \mathcal{Q}^{-1} \cdot \Gamma}_{\text{ID on } \ell+m \text{ rounds}}$$

Illustration for Proof for Skipjack Rule-A

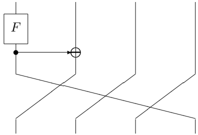
Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

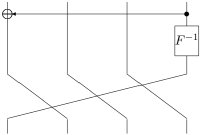
Illustration for Proof for Skipjack Rule-A

Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

Inverse function



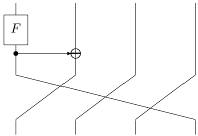
$$\begin{aligned} \mathcal{R}^{-1} &= \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \\ &= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1} \end{aligned}$$

$$\mathcal{F}_*^{-1} = \mathcal{P} \cdot \mathcal{F} \cdot \mathcal{P}^{-1}$$

$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

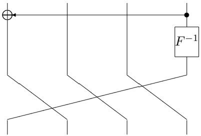
Illustration for Proof for Skipjack Rule-A

Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

Inverse function

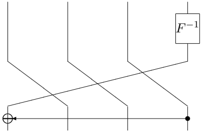


$$\mathcal{R}^{-1} = \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1}$$
$$= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}$$

$$\mathcal{F}_*^{-1} = \mathcal{P} \cdot \mathcal{F} \cdot \mathcal{P}^{-1}$$

$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

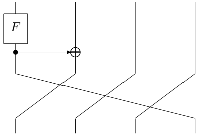
Exchange the order of the operations



$$\mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1}$$

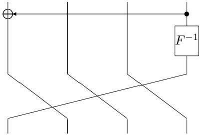
Illustration for Proof for Skipjack Rule-A

Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

Inverse function

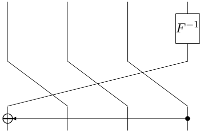


$$\begin{aligned}\mathcal{R}^{-1} &= \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \\ &= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}\end{aligned}$$

$$\mathcal{F}_*^{-1} = \mathcal{P} \cdot \mathcal{F} \cdot \mathcal{P}^{-1}$$

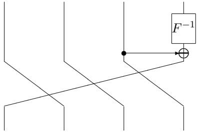
$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

Exchange the order of the operations



$$\mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1}$$

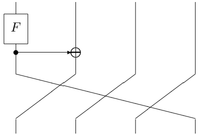
Equivalent formulation



$$\mathcal{P}^{-1} \cdot (\mathcal{P} \cdot \mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1}) \cdot \mathcal{F}_*^{-1}$$

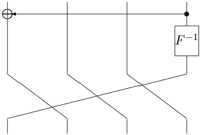
Illustration for Proof for Skipjack Rule-A

Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

Inverse function

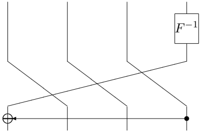


$$\begin{aligned}\mathcal{R}^{-1} &= \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \\ &= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}\end{aligned}$$

$$\mathcal{F}_*^{-1} = \mathcal{P} \cdot \mathcal{F} \cdot \mathcal{P}^{-1}$$

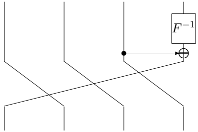
$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

Exchange the order of the operations



$$\mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1}$$

Equivalent formulation



$$\mathcal{P}^{-1} \cdot (\mathcal{P} \cdot \mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1}) \cdot \mathcal{F}_*^{-1}$$

Permutation of the branches

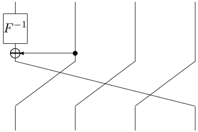
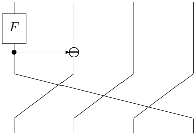


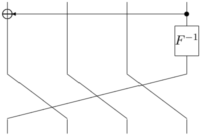
Illustration for Proof for Skipjack Rule-A

Round function



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

Inverse function

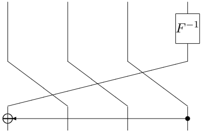


$$\mathcal{R}^{-1} = \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} = \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}$$

$$\mathcal{F}_*^{-1} = \mathcal{P} \cdot \mathcal{F} \cdot \mathcal{P}^{-1}$$

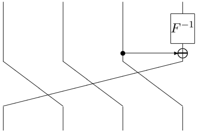
$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

Exchange the order of the operations



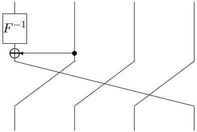
$$\mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1}$$

Equivalent formulation



$$\mathcal{P}^{-1} \cdot (\mathcal{P} \cdot \mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1}) \cdot \mathcal{F}_*^{-1}$$

Permutation of the branches

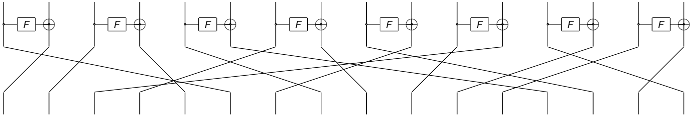


The inverse function is “equivalent” to the mirror function

Outline

Example of Equivalence

Round Function of the Twine Block Cipher:



$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F} \text{ with } \mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ F & 1 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 1 & & 0 & 0 & 0 \\ & & \cdots & & & & \\ 0 & 0 & 0 & & 0 & 1 & 0 \\ 0 & 0 & 0 & & 0 & F & 1 \end{pmatrix},$$

$\mathcal{P}$ defined from $\pi = \{5, 0, 1, 4, 7, 12, 3, 8, 13, 6, 9, 2, 15, 10, 11, 14\}$

We have $\mathcal{M} = \mathcal{Q} \cdot \mathcal{R} \cdot \mathcal{Q}^{-1}$ for $\mathcal{Q}$ defined from

$$\gamma = \{16, 15, 12, 11, 14, 13, 10, 9, 8, 7, 4, 3, 6, 5, 2, 1\}$$

Example of Inequivalence

- Some of the Feistels of [Suzaki et al 2010]
  - For instance $\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$ with $\mathcal{F} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ F & 1 & & 0 & 0 \\ & & \cdots & & \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & & F & 1 \end{pmatrix}$

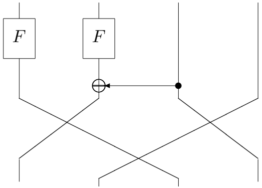
    and $\mathcal{P}$ is defined from $\pi = \{1, 2, 9, 4, 11, 6, 7, 8, 5, 12, 13, 10, 3, 0\}$

Example of Inequivalence

- Some of the Feistels of [Suzaki et al 2010]
  - For instance $\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$ with $\mathcal{F} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ F & 1 & & 0 & 0 \\ & & \cdots & & \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & & F & 1 \end{pmatrix}$

    and $\mathcal{P}$ is defined from $\pi = \{1, 2, 9, 4, 11, 6, 7, 8, 5, 12, 13, 10, 3, 0\}$

- The original Skipjack (ID: 24 rounds, ZC: 17 rounds)
  - Rule-B followed by Rule-A is equivalent to



Conclusions

- We provide condition of equivalence between ID and ZC distinguishers for different cipher constructions (Feistel-type, Skipjack-type, EGFN-type, $\cdots$)
- The results can be generalized to other constructions
- This relation can be taken into consideration when designing a cipher

- Is there a link between the key-recovery attacks?