Aalto University
School of Science

Relations Between the Generalizations of Differential and Linear Cryptanalysis

Céline Blondeau

November 14, 2014

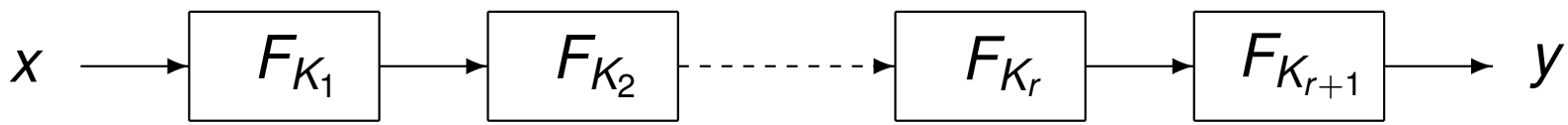
Université de Rennes

Introduction

Block cipher :

$$\begin{array}{rccc} E_K & : & \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ & & x & \mapsto & y \end{array}$$

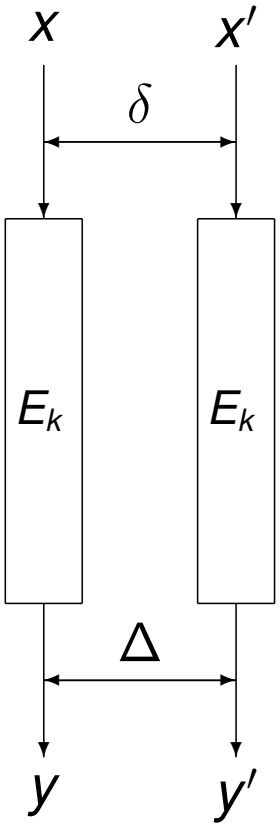
Iterative block cipher :



Statistical attacks: Attacks that take advantage of a non-uniform behaviour of the cipher

Differential Cryptanalysis [Biham Shamir 90]

Difference between plaintext and ciphertext pairs



Input difference : δ
Output Difference : Δ

Differential Probability :

$$\mathbf{P}[\delta \rightarrow \Delta] = P_x[\, E_k(x) \oplus E_k(x \oplus \delta) = \Delta]$$

Generalisations of Differential Cryptanalysis

Set of input differences : $\delta \in A$
Set of output differences : $\Delta \in B$

$$\mathbf{P}[A \to B] = \frac{1}{|A|} \sum_{\delta \in A} \sum_{\Delta \in B} P[\delta \to \Delta]$$

Truncated Differential (TD) [Knudsen 94] :
Set A and B generally with structure : linear, affine spaces

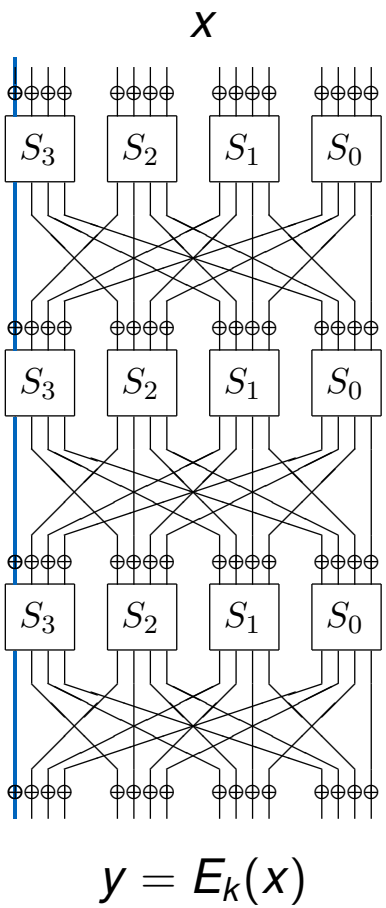
Impossible Differential (ID) [Knudsen 99] :
Truncated differential distinguisher with probability 0

Multiple Differential [Blondeau Gérard 11] :
Sets A and B without structure

Multiple Differential using LLR or $\chi 2$ [Blondeau Gérard Nyberg 12]

Linear Cryptanalysis [Tardy Gilbert 91] [Matsui 93]

Linear relation involving plaintext, key and ciphertext bits



Input mask : u
Output mask : v

Bias :

$$\varepsilon = 2^{-n}\#\{x \in \mathbb{F}_2^n |\ u \cdot x \oplus v \cdot y = 0\} - \frac{1}{2}$$

Correlation :

$$\begin{aligned} \mathbf{cor}_x(u,v) &= 2 \cdot P_x\left[u \cdot x \oplus v \cdot E_k(x) = 0\right] - 1 \\ &= 2 \cdot \varepsilon \end{aligned}$$

Generalizations of Linear Cryptanalysis

Set of masks $(u, v) \in U \times V \setminus \{0, 0\}$

Capacity :

$$C = \sum_{u \in U \setminus \{0\}} \sum_{v \in V \setminus \{0\}} \mathbf{cor}_x^2(u, v)$$

Multiple Linear [Biryukov et al 04] :
Set U and V without structure

Multidimensional Linear (ML) [Hermelin et al 08] :
Set U and V are linear or affine spaces

Zero-Correlation Linear (ZC) [Bogdanov et al 10] :
(Multidimensional) linear distinguisher with capacity 0

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2 (u, v)$$

- Used to show that AB functions are APN
  (In general used for vector-Boolean functions)

Recent Links Between

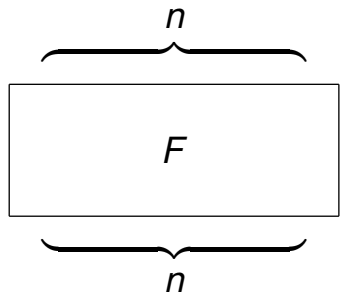
The Statistical Attacks

Outline

Outline

Computation

Chabaud-Vaudenay's link:

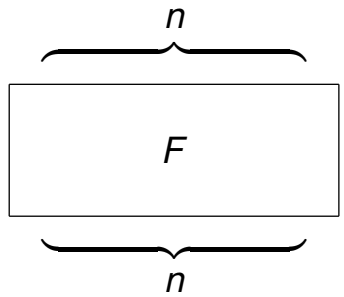


$$\mathbf{P}[\delta \xrightarrow{F} \Delta] = 2^{-n} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2 (u, v)$$

Complexity: Computation of 2^{2n} correlations!!!

$\Rightarrow$ Impossible in practice

Computation



Chabaud-Vaudenay's link:

$$\mathbf{P}[\delta \xrightarrow{F} \Delta] = 2^{-n} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^n} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$

Complexity: Computation of 2^{2n} correlations!!!

$\Rightarrow$ Impossible in practice

How to reduce the complexity:

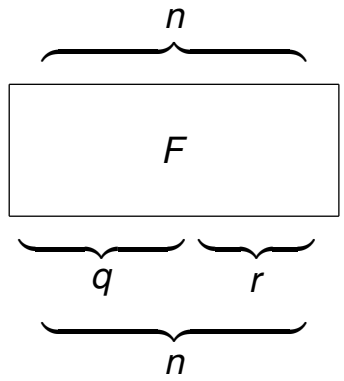
- Using truncated output differences

  $\Rightarrow$ Reduce the sum over v

- Assuming δ of small weight

  $\Rightarrow$ Reduce the sum over u

Truncated Output Difference

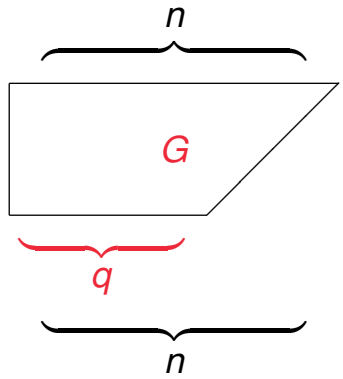


Setting:

- Affine space $\Delta_q \oplus \mathbb{F}_2^r$
- Let G be a projection of F

$$\mathbf{P}[\delta \xrightarrow{F} (\Delta_q \oplus \mathbb{F}_2^r)] = \mathbf{P}[\delta \xrightarrow{G} \Delta_q]$$

Truncated Output Difference

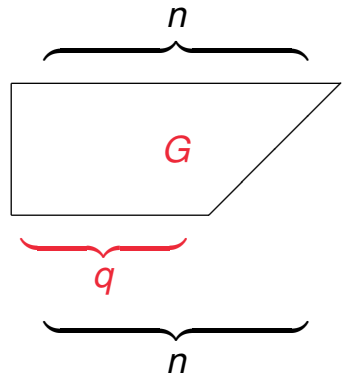


Setting:

- Affine space $\Delta_q \oplus \mathbb{F}_2^r$
- Let G be a projection of F

$$\mathbf{P}[\delta \xrightarrow{F} (\Delta_q \oplus \mathbb{F}_2^r)] = \mathbf{P}[\delta \xrightarrow{G} \Delta_q]$$

Truncated Output Difference



Setting:

- Affine space $\Delta_q \oplus \mathbb{F}_2^r$
- Let G be a projection of F

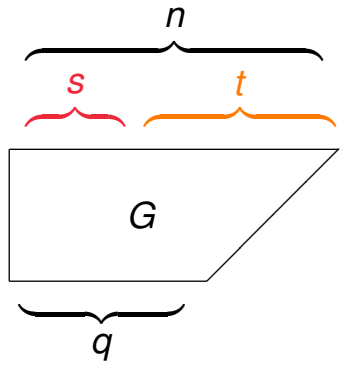
$$\mathbf{P}[\delta \xrightarrow{F} (\Delta_q \oplus \mathbb{F}_2^r)] = \mathbf{P}[\delta \xrightarrow{G} \Delta_q]$$

Link:

$$\mathbf{P}[\delta \xrightarrow{G} \Delta_q] = 2^{-q} \sum_{u \in \mathbb{F}_2^n} \sum_{v_q \in \mathbb{F}_2^q} (-1)^{u \cdot \delta \oplus v_q \cdot \Delta_q} \mathbf{cor}_x^2 (u, v_q)$$

Complexity: Computation of 2^{n+q} correlations

Assuming δ of Small Weight

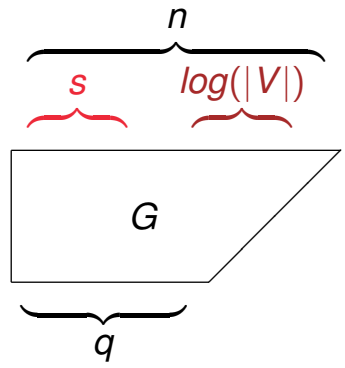


Assumption: $\delta = (\delta_s, \delta_t) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $\delta_t = 0$

Fundamental Theorem [Nyberg 93]:

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot \delta} \mathbf{cor}_x^2(u, v_q) = 2^{-t} \sum_{x_t \in \mathbb{F}_2^t} \sum_{u_s \in \mathbb{F}_2^s} (-1)^{u_s \cdot \delta_s} \mathbf{cor}_{x_s}^2(u_s, v_q)$$

Assuming δ of Small Weight



Assumption: $\delta = (\delta_s, \delta_t) \in \mathbb{F}_2^s \times \mathbb{F}_2^t$ with $\delta_t = 0$

Fundamental Theorem [Nyberg 93]:

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot \delta} \mathbf{cor}_x^2(u, v_q) = 2^{-t} \sum_{x_t \in \mathbb{F}_2^t} \sum_{u_s \in \mathbb{F}_2^s} (-1)^{u_s \cdot \delta_s} \mathbf{cor}_{x_s}^2(u_s, v_q)$$

Approximation:

$$\sum_{u \in \mathbb{F}_2^n} (-1)^{u \cdot \delta} \mathbf{cor}_x^2(u, v_q) \approx \frac{1}{|A|} \sum_{x_t \in A} \sum_{u_s \in \mathbb{F}_2^s} (-1)^{u_s \cdot \delta_s} \mathbf{cor}_{x_s}^2(u_s, v_q)$$

Method of Computation

Estimated Truncated Differential Probability:

$$\mathbf{P}[\delta \xrightarrow{G} \Delta_q] \approx \frac{2^{-q}}{|A|} \sum_{x_t \in A} \sum_{u_s \in \mathbb{F}_2^s} \sum_{v_q \in \mathbb{F}_2^q} (-1)^{u_s \cdot \delta_s \oplus v_q \cdot \Delta_q} \mathbf{cor}^2_{x_s}(u_s, v_q)$$

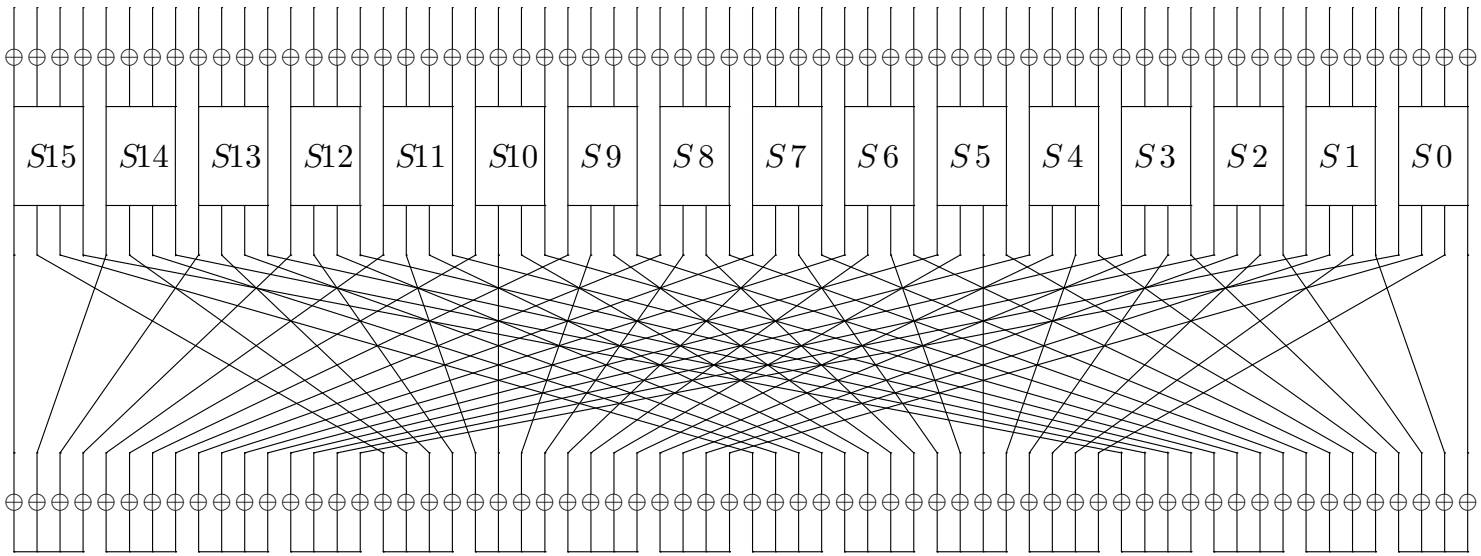
Complexity: Computation of $2^{s+q}|A|$ correlations

Accuracy: Depends on the choice of s and A

PRESENT

[Bogdanov et al 08]

- 64-bit cipher
- 80-bit (128-bit) key
- 31 rounds



Setting of Experiments on PRESENT

PRESENT:

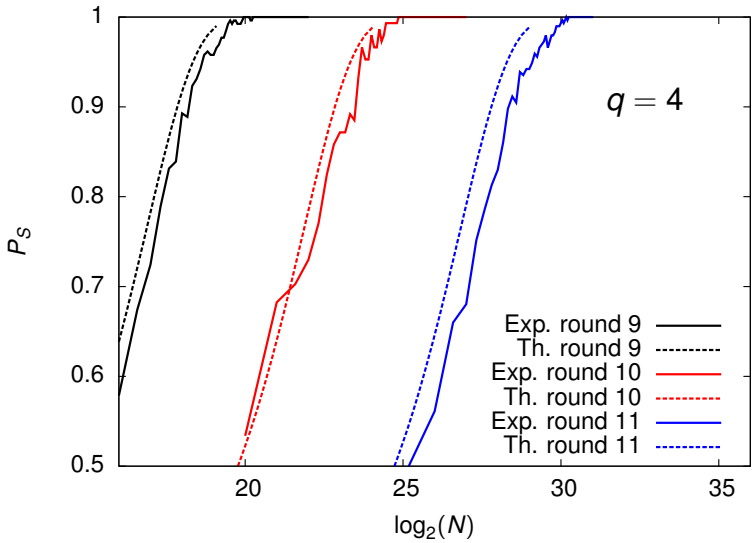
- Single-bit linear trails are dominant
- Computation of correlations using transition matrices
  as for instance in [Cho 10]

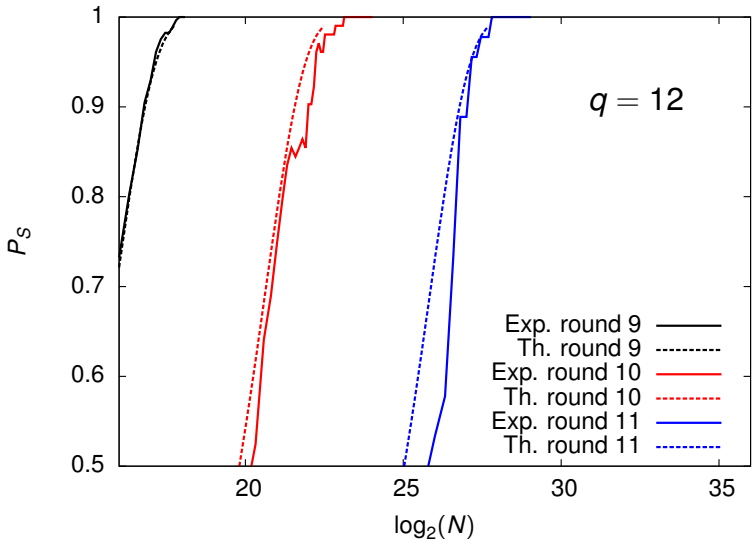
Setting:

- Truncated differential distribution cryptanalysis
  Using *LLR* statistical test [Blondeau Gérard Nyberg 12]

Truncated Differential Distribution Cryptanalysis

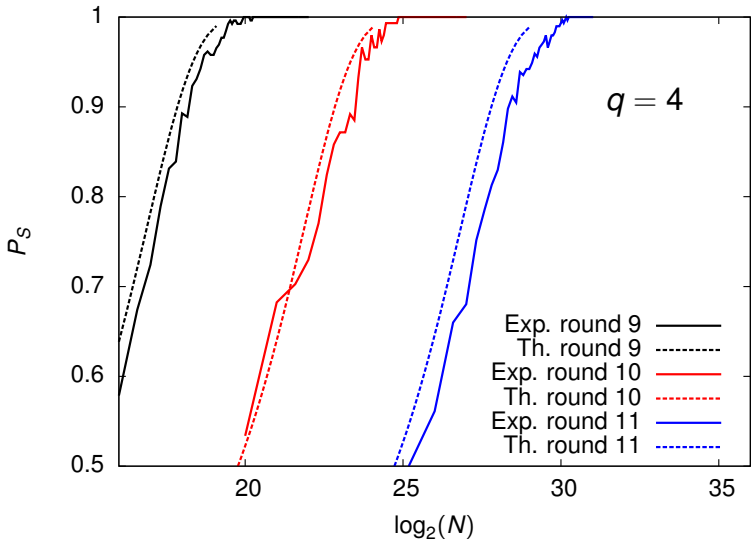
Experiments on PRESENT :

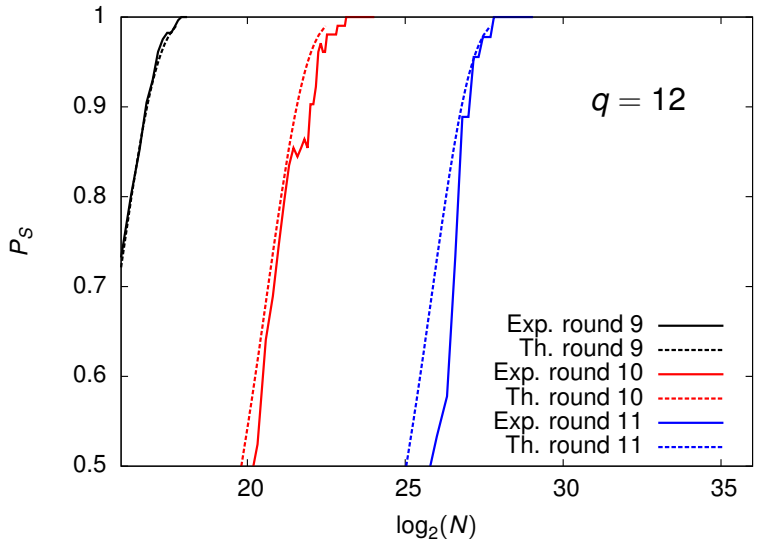




Truncated Differential Distribution Cryptanalysis

Experiments on PRESENT :





Cryptanalysis:

- On 19 rounds

Previously:

- Multiple differential cryptanalysis: 18 rounds
- Multidimensional linear cryptanalysis: 26 rounds

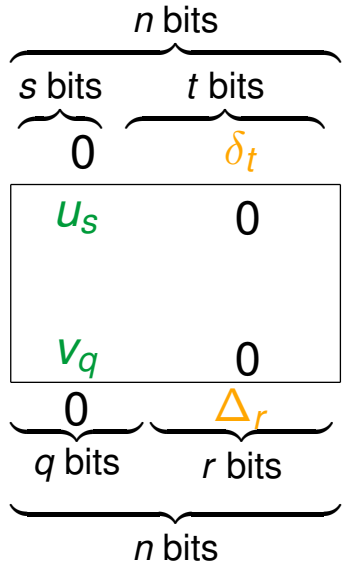
Outline

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$

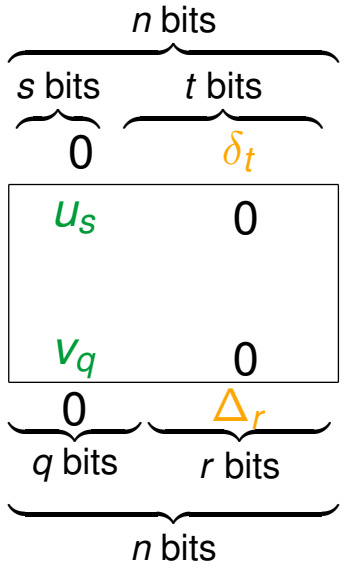


Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$



Generalization [Blondeau Nyberg 14]:

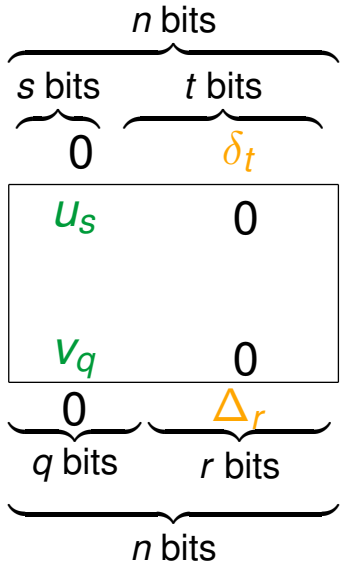
- ML : $[(u_s, 0), (v_q, 0)]_{u_s \in \mathbb{F}_2^s \setminus \{0\},\ v_q \in \mathbb{F}_2^q}$ with capacity C
- TD : $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t,\ \Delta_r \in \mathbb{F}_2^r}$ with probability p

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$



Generalization [Blondeau Nyberg 14]:

- 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
- TD : $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t,\ \Delta_r \in \mathbb{F}_2^r}$ with probability p

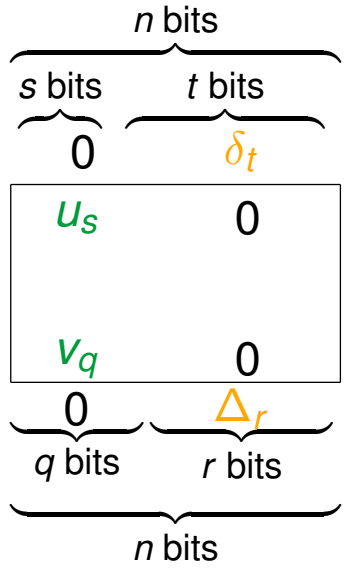
$$p = 2^{-q}(C + 1)$$

Link between Differential and Linear Cryptanalysis

[Chabaud Vaudenay 94] :

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$\mathbf{P}[\delta \to \Delta] = 2^{-m} \sum_{u \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^m} (-1)^{u \cdot \delta \oplus v \cdot \Delta} \mathbf{cor}_x^2(u, v)$$



Generalization [Blondeau Nyberg 14]:

- 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
- TD : $[(0, \delta_t), (0, \Delta_r)]_{\delta_t \in \mathbb{F}_2^t,\ \Delta_r \in \mathbb{F}_2^r}$ with probability p

$$p = 2^{-q}(C + 1)$$

- TD is a chosen plaintext (CP) attack
- ML is a known plaintext (KP) attack

Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

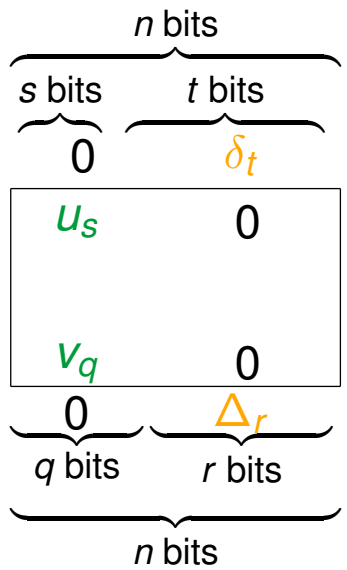
- Multidimensional Linear :

$$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- Truncated Differential :

$$N^{TD} = \frac{2^{-q+1}}{M \cdot (p - 2^{-q})^2} \cdot \varphi_a^2,$$

where M is the size of a structure (usually $M = 2^t$)



Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

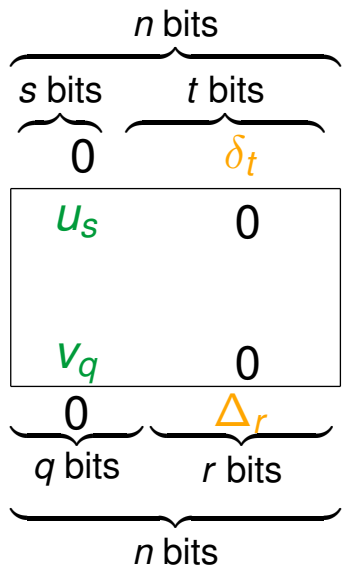
- Multidimensional Linear :

$$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- Truncated Differential :

$$N^{TD} = \frac{2^{-q+1}}{M \cdot (p - 2^{-q})^2} \cdot \varphi_a^2,$$

where M is the size of a structure (usually $M = 2^t$)



- For $p = 2^{-q}(C + 1)$:

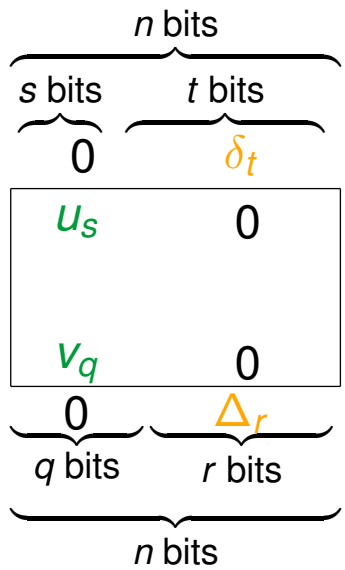
$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$

Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

- $$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- For $p = 2^{-q}(C+1)$:
$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$



Data Complexity of a Distinguishing Attack

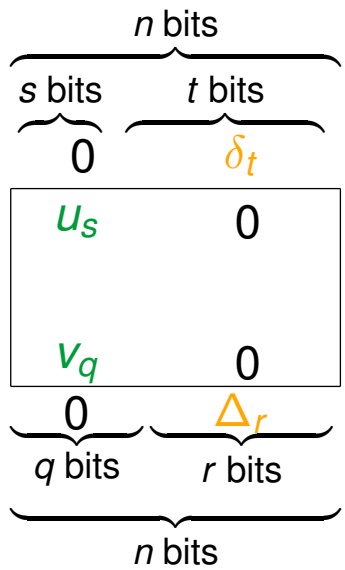
[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

- $$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$

- For $p = 2^{-q}(C+1)$:

$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$

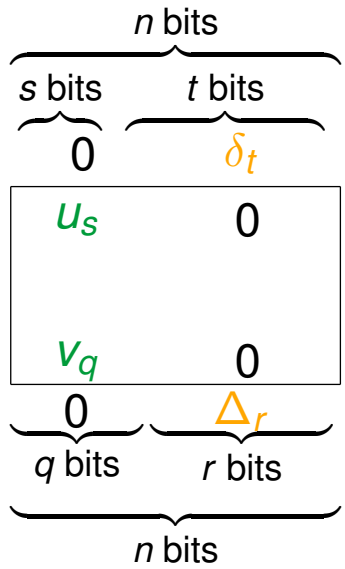
$$N^{TD} = \frac{1}{2^n} \cdot (N^{ML})^2$$



Data Complexity of a Distinguishing Attack

[Selçuk 07] $P_S = 50\%$ and $\varphi_a = \Phi^{-1}(1 - 2^{-a})$, with a the advantage

- $$N^{ML} = \frac{2^{(s+q+1)/2}}{C} \cdot \varphi_a$$



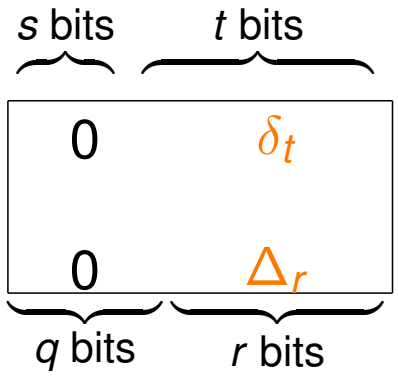
- For $p = 2^{-q}(C + 1)$:

$$N^{TD} = \frac{2^{q+1}}{2^t \cdot C^2} \cdot {\varphi_a}^2$$

$$N^{TD} = \frac{1}{2^n} \cdot (N^{ML})^2$$

$N^{TD} \leq N^{ML}$ with equality when using the full codebook

Truncated Differential Distinguisher



$x = (x_s, x_t)$

$y = (y_q, y_r)$

M : size of a structure
S : number of structures

$$N^{TD} = S \cdot M$$

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
  Create a table T of size M
  for M values of $x_t \in \mathbb{F}_2^t$ **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[x_t] = y_q$
  for all pairs (x_t, x_t') **do**
    if $(T[x_t] \oplus T[x_t']) == 0$ **then**
      $D \mathrel{+}= 1$

For S structures

For all elements in a structure

Store the partial ciphertexts

Count the number of pairs which have no difference on the q bits

Truncated Differential Distinguisher

Time Complexity : Verifying all pairs

$$Time \approx S \cdot M^2/2$$

Memory Complexity : Storing all ciphertexts inside a structure

$$Memory \approx M$$

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
  Create a table T of size M
  for M values of $x_t \in \mathbb{F}_2^t$ **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[x_t] = y_q$
  for all pairs (x_t, x_t') **do**
    if $(T[x_t] \oplus T[x_t']) == 0$ **then**
      $D \mathrel{+}= 1$

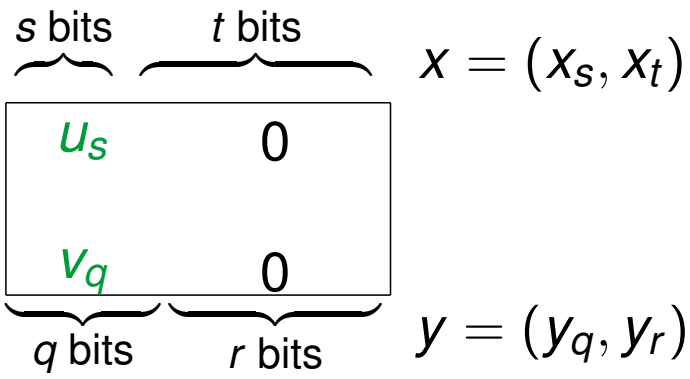
For S structures

For all elements in a structure

Store the partial ciphertexts

Count the number of pairs which have no difference on the q bits

Multidimensional Linear Distinguisher



Set a counter D to 0
Create a table T of size 2^{q+s}
for N^{ML} plaintexts **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[(x_s, y_q)] \mathrel{+}= 1$
for all (x_s, y_q) **do**
    $D \mathrel{+}= (T[(x_s, y_q)] - N/2^{q+s})^2$

For N^{ML} plaintexts
  Count the number of occurrences of each pair (x_s, y_q)

Compute the statistic

Multidimensional Linear Distinguisher

Time Complexity : Reading all messages

$$Time \approx N^{ML}$$

Memory Complexity : Storing the number of occurrences of $(x_s^i, y_q^j)_{i,j}$

$$Memory \approx 2^{s+q}$$

Set a counter D to 0
Create a table T of size 2^{q+s}
for N^{ML} plaintexts **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[(x_s, y_q)] \mathrel{+}= 1$
for all (x_s, y_q) **do**
    $D \mathrel{+}= (T[(x_s, y_q)] - N/2^{q+s})^2$

For N^{ML} plaintexts
  Count the number of occurrences of each pair (x_s, y_q)

Compute the statistic

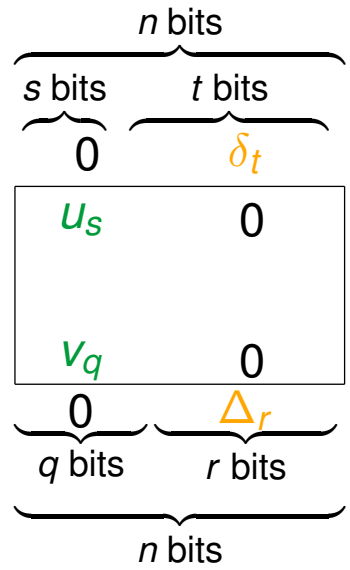
Complexities of TD and ML Attacks

- ML distinguisher :

$$Data = N^{ML}$$

$$Time \approx N^{ML}$$

$$Memory \approx 2^{s+q}$$



- TD distinguisher :

$$Data = N^{TD} = S \cdot 2^t < N^{ML}$$

$$Time \approx N^{TD} \cdot 2^{t-1}$$

$$Memory \approx 2^t$$

Question : Can we decrease the time complexity of a TD attack?

TD with Less Time Complexity

- Dominant part: Verifying the output difference for each pair of ciphertexts

Example :

- 4 ciphertexts : (y_1, b_1) (y_2, b_2) (y_1, b_3) (y_3, b_4)
  1 pair with equal y_i
- Previous algorithm : 6 comparisons

TD with Less Time Complexity

- Dominant part: Verifying the output difference for each pair of ciphertexts

Example :

- 4 ciphertexts : $(y_1, b_1)\ (y_2, b_2)\ (y_1, b_3)\ (y_3, b_4)$
  1 pair with equal y_i
- Previous algorithm : 6 comparisons

Improved Version :

- Count the occurrences of each y_i :

	y_1	y_2	y_3
$T[y_i]$	2	1	1

and compute $D = \sum_i T[y_i](T[y_i] - 1)/2 = 1$

TD with Less Time Complexity

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
  Create a table T of size 2^q
  for M values of $x_t \in \mathbb{F}_2^t$ **do**
    $(y_q, y_r) = E((x_s, x_t))$
    $T[y_q] \mathrel{+}= 1$
  for all $y_q \in \mathbb{F}_2^q$ **do**
    $D \mathrel{+}= T[y_q](T[y_q] - 1)/2$

For S structures

For all elements in a structure

Count the number of occurrences of the partial ciphertexts

Compute the statistic

$$Data = N^{TD} = S \cdot M < N^{ML}$$

$$Time \approx max(N^{TD}, S \cdot 2^q)$$

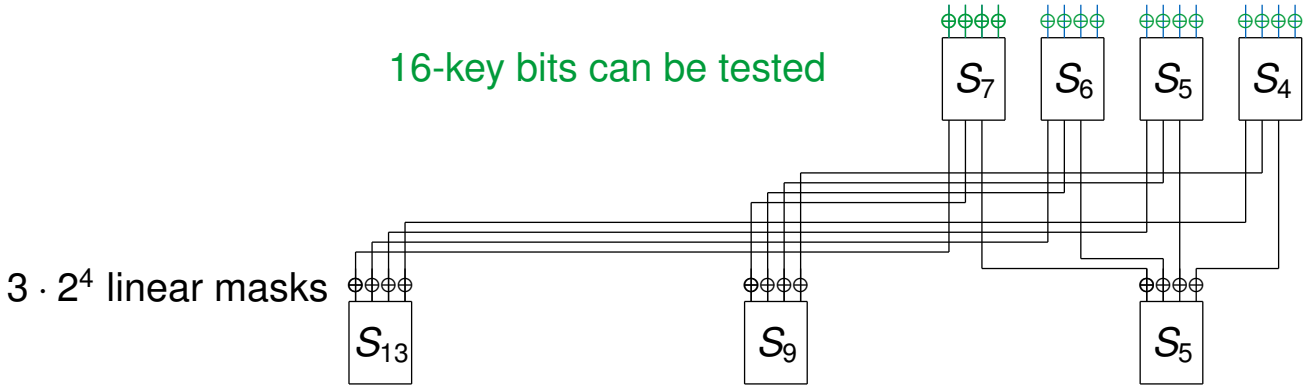
$$Memory \approx 2^q$$

KP ML and CP TD Attacks : An Example on PRESENT

[Cho 10] :

- ML distinguisher on 24 rounds
- KP ML attack on 26 rounds (inversion of the first and last round)

First round : (In Cho's ML characteristic)



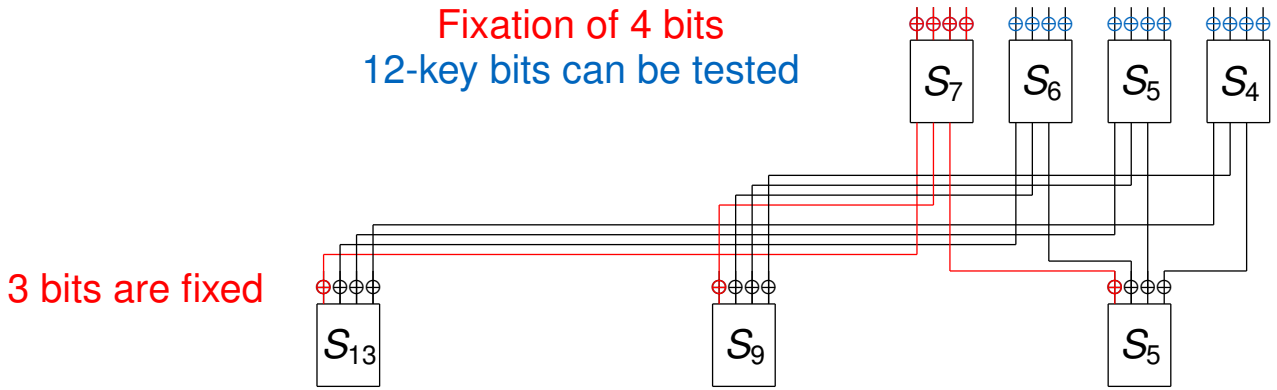
- KP ML $\Rightarrow$ Guess 16-key bits

KP ML and CP TD Attacks : An Example on PRESENT

[Cho 10] :

- ML distinguisher on 24 rounds
- KP ML attack on 26 rounds (inversion of the first and last round)

First round : (In Cho's ML characteristic)



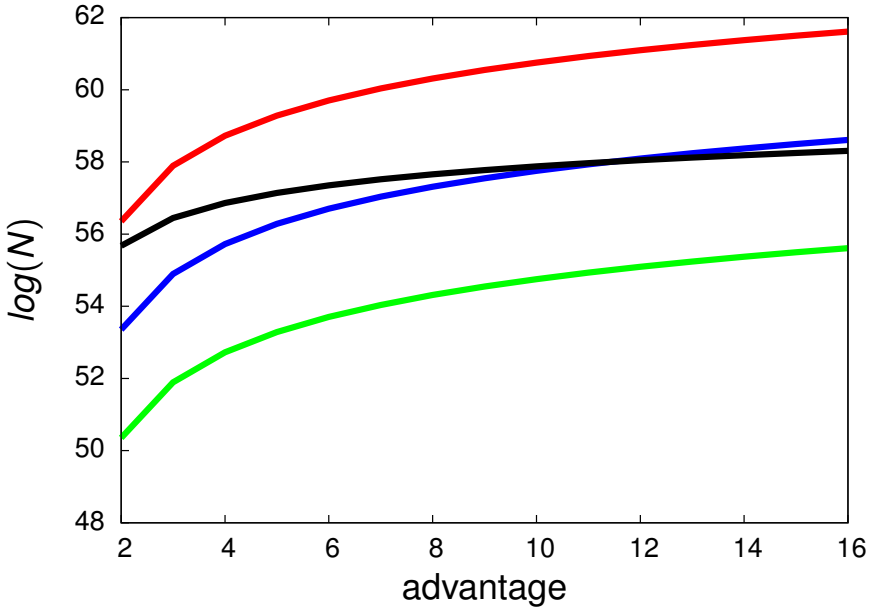
- KP ML $\Rightarrow$ Guess 16-key bits

Using the link between TD and ML

- CP TD $\Rightarrow$ Guess $4, 8, 12, 16$-key bits

Example of CP TD Attack on 24 Rounds of PRESENT

Data Complexity (*Data*) :



KP ML
CP TD fixing 4 bits
CP TD fixing 8 bits
CP TD fixing 12 bits

- The *Data* of a KP ML is proportional to $\varphi_a = \Phi^{-1}(1 - 2^{-a})$
- The *Data* of a CP TD is proportional to φ_a^2
- Depending of the size of the fixation, the data complexity of a CP ML attack can be smaller than for a KP ML attack

Example of CP TD Attack on 24 Rounds of PRESENT

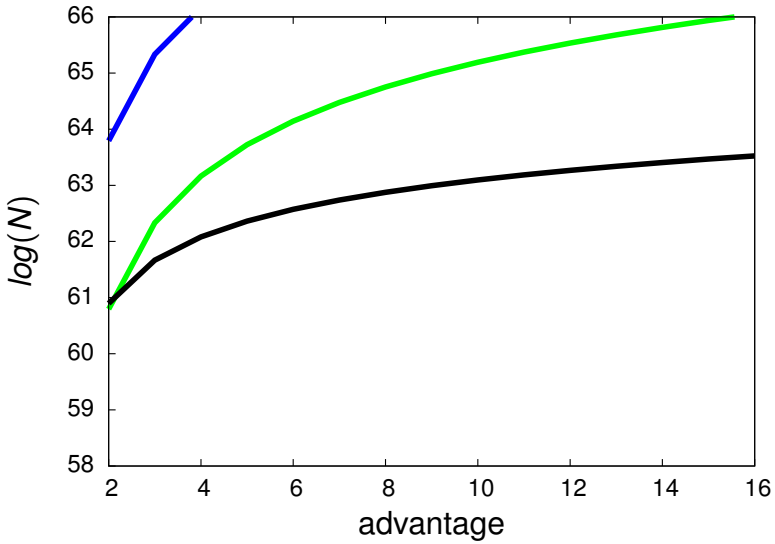
Fixing 4 bits :

Model	a	*Data*	*Memory*	$Time_1$	$Time_2$
CP TD	10	$2^{54.75}$	2^{29}	$2^{54.75}$	2^{70}
KP ML	5	$2^{57.14}$	2^{32}	$2^{57.14}$	2^{75}

$Time_1$: Complexity of the distillation phase
$Time_2$: Complexity of the search phase

- Data, time and memory complexities of the CP TD attack are smaller than those of a KP ML attack

Example of CP TD Attack on 26 Rounds of PRESENT



KP ML

CP TD fixing 4 bits

CP TD fixing 8 bits

Model	a	*Data*	*Memory*	$Time_1$	$Time_2$
CP TD	4	$2^{63.16}$	2^{29}	$2^{63.16}$	2^{76}
KP ML	4	$2^{62.08}$	2^{32}	$2^{62.08}$	2^{76}

- A CP TD attack on 26 rounds of PRESENT with less memory than the KP ML attack
- The previous differential-type attack was on 19 rounds

Outline

Statistical Saturation (SS) Attack [Collard Standaert 09]

Idea :

- “Dual” of the saturation attack
- Takes advantage of several plaintexts with some fixed bits while the others vary randomly
- We observe the diffusion of the fixed bits during the encryption process

Application on PRESENT [Bogdanov et al 08] :

- Distinguisher on 20 / 21 rounds
- Key-recovery on 24 rounds

Statistical Saturation Distinguisher

$D = 0$
for S values of $x_s \in \mathbb{F}_2^s$ **do**
    Create a table T of size 2^q
    for M values of $x_t \in \mathbb{F}_2^t$ **do**
        $(y_q, y_r) = E((x_s, x_t))$
        $T[y_q] \mathrel{+}= 1$
    for all $y_q \in \mathbb{F}_2^q$ **do**
        $D \mathrel{+}= T[y_q](T[y_q] - 1)/2$

For S structures

For all elements in a structure

Count the number of occurrences of the partial ciphertexts

Compute the statistic

This distinguisher is the same as the improved truncated differential distinguisher

Link between SS, TD and ML distinguishers

Link [Leander 11] :

For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

Link between SS, TD and ML distinguishers

Link [Leander 11] :

For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

- SS attacks link mathematically with ML attacks

Link between SS, TD and ML distinguishers

Link [Leander 11] :
For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

- SS attacks link mathematically with ML attacks

SS is a chosen plaintext (CP) attack
ML is a known plaintext (KP) attack

Link between SS, TD and ML distinguishers

Link [Leander 11] :
For a fixed $x_s \in \mathbb{F}_2^s$, we denote by $C(x_s)$ the capacity of the distribution of y_q :

$$C = 2^{-s} \sum_{x_s \in \mathbb{F}_2^s} C(x_s)$$

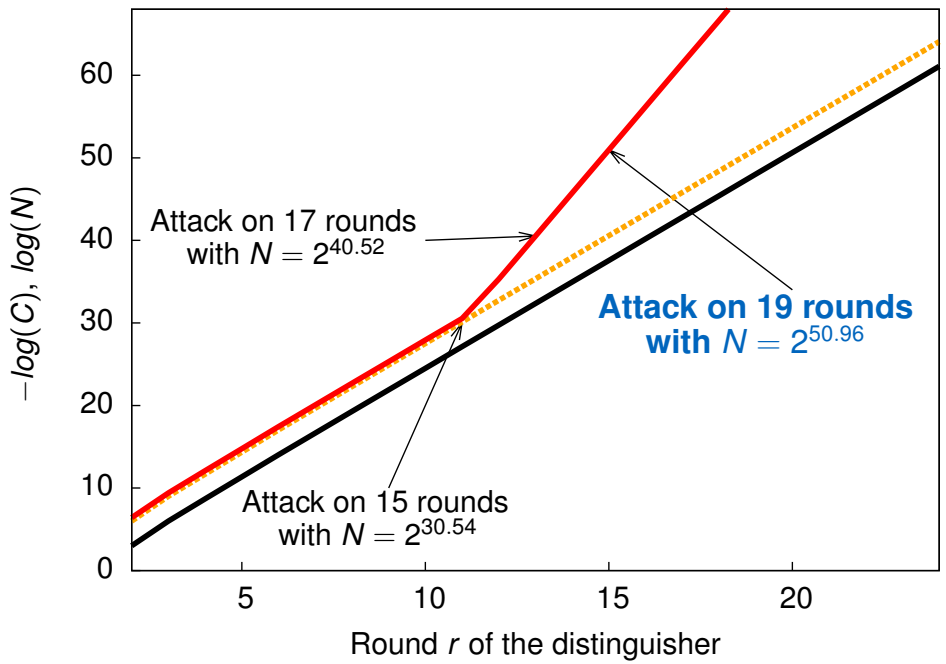
- SS attacks link mathematically with ML attacks

SS is a chosen plaintext (CP) attack
ML is a known plaintext (KP) attack

- SS attacks link algorithmically with TD attacks

On the SS Attack on PRESENT [Collard Standaert 09]

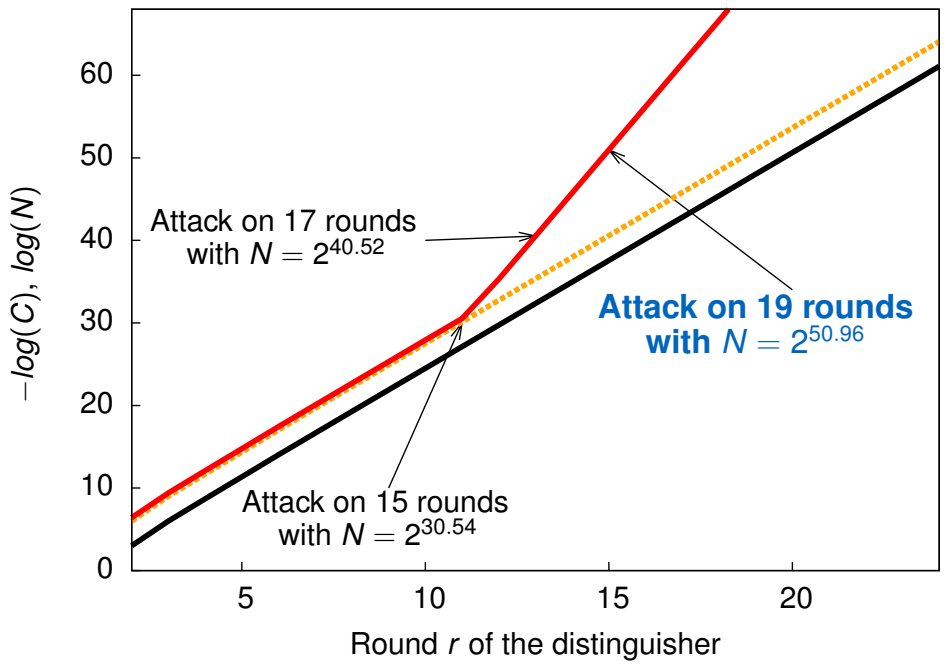
Attack on $r + 4$ rounds with $M = 2^{32}$



- [Collard Standaert 09]
  Data increases linearly
- [Leander 11]
  Estimate of the capacity C
- [Our work]
  Data is $N = \frac{2^{q+1}}{M \cdot C^2} \cdot \varphi_a^2$

On the SS Attack on PRESENT [Collard Standaert 09]

Attack on $r + 4$ rounds with $M = 2^{32}$



- [Collard Standaert 09]
  Data increases linearly
- [Leander 11]
  Estimate of the capacity C
- [Our work]
  Data is $N = \frac{2^{q+1}}{M \cdot C^2} \cdot \varphi_a^2$

- The attack has been verified experimentally [Kerckhof et al 11]
- Our estimate match with the experiments
  (N around 2^{51} for 19 rounds)

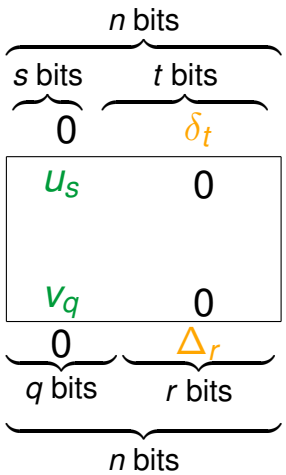
Outline

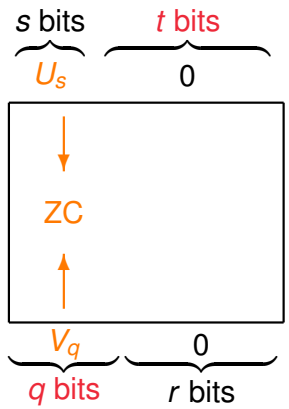
Mathematical Relation between ID and ZC

[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

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



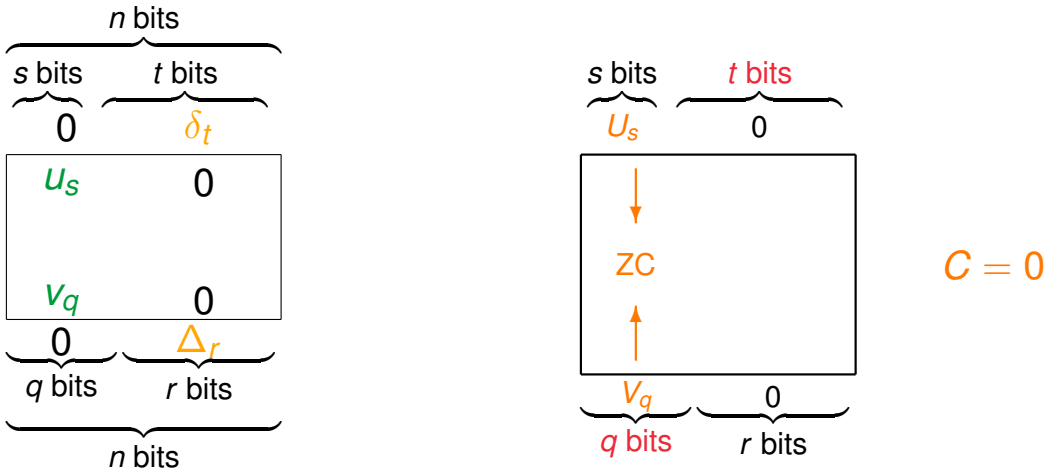


$C = 0$

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

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:

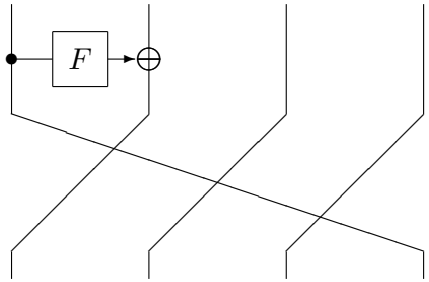
Ciphers	ID	ZC
LBlock / TWINE	14	14
MARS	11	11
SMS4	11	11
Skipjack	24	17
Skipjack (only rule A)	16	16
Four-Cell	18	12

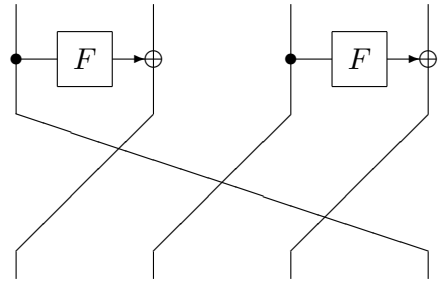
Example of Patterns (for LBlock) :

- Impossible differential :
  $(00000000, 00\Delta 00000) \nrightarrow (0\Gamma 000000, 00000000)$
- Zero correlation approximation :
  $(000U0000, 00000000) \nrightarrow (00000000, 0V000000)$

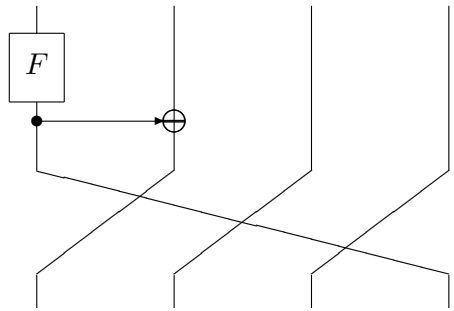
Example of Constructions

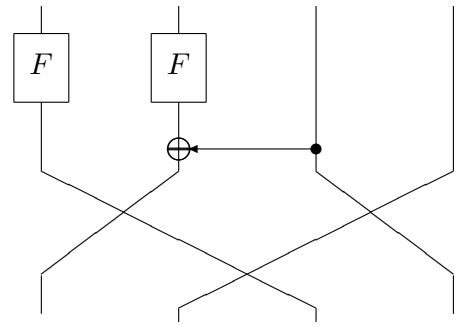
Feistel-Type



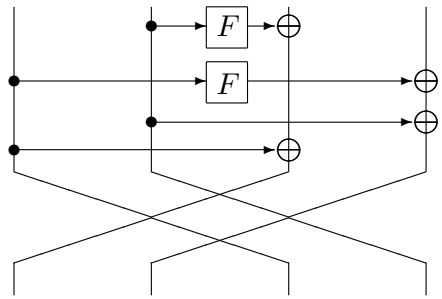


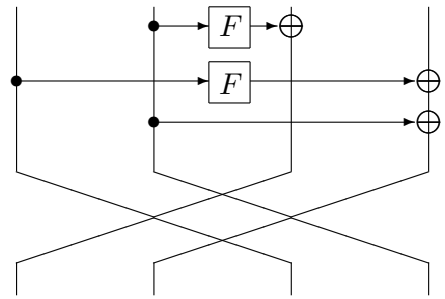
Skipjack-Type





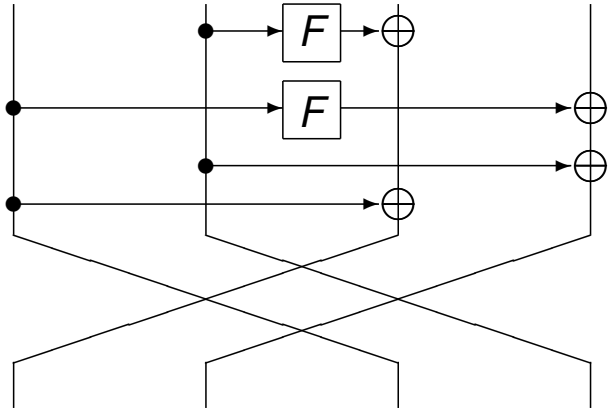
EGNF-Type





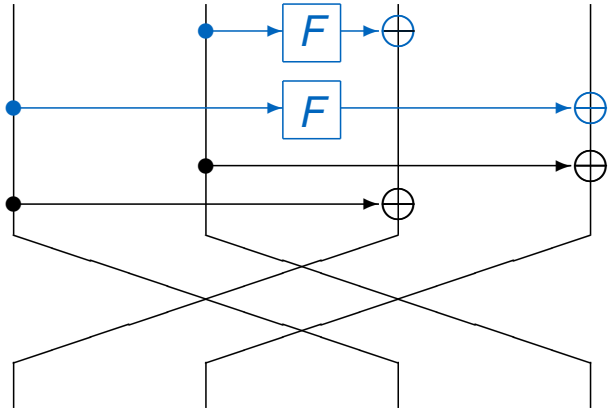
Representation of the Round Function

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



Representation of the Round Function

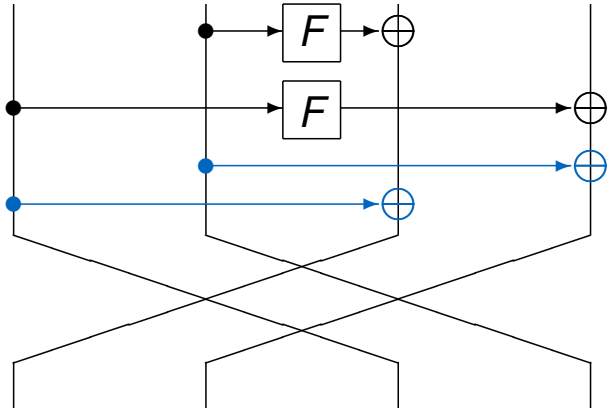
- F-layer
- X-layer
- P-layer



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

Representation of the Round Function

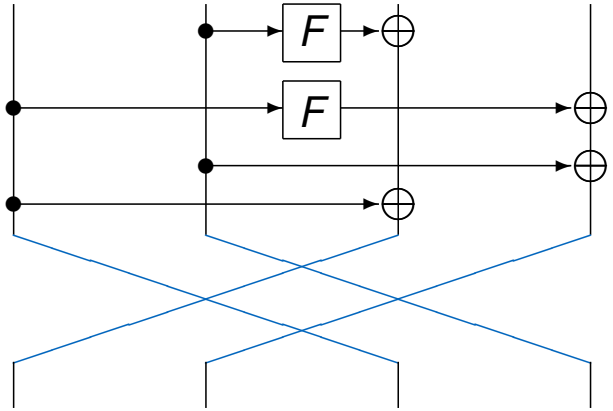
- F-layer
- X-layer
- P-layer



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

Representation of the Round Function

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

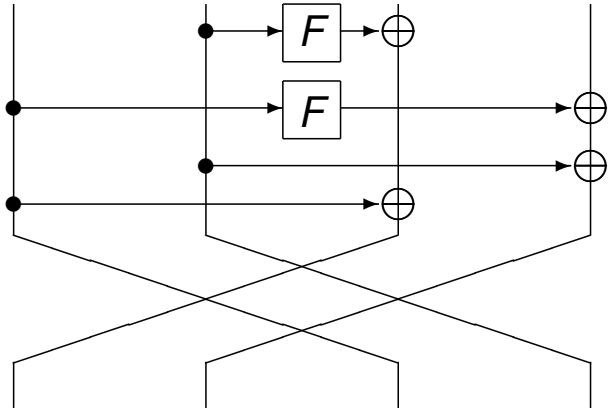


$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

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

Representation of the Round Function

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

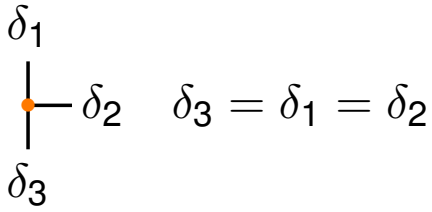


$$\mathcal{F} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & F & 1 & 0 \\ F & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{X} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

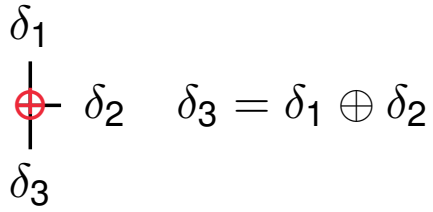
$$\mathcal{P} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \text{and } \mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

Rules to find ZC and ID distinguishers

Differential Context :



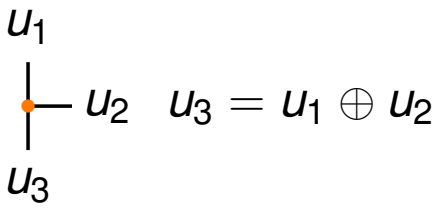
$\delta_3 = \delta_1 = \delta_2$



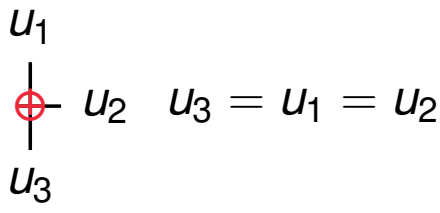
$\delta_3 = \delta_1 \oplus \delta_2$

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

Linear Context :



$u_3 = u_1 \oplus u_2$

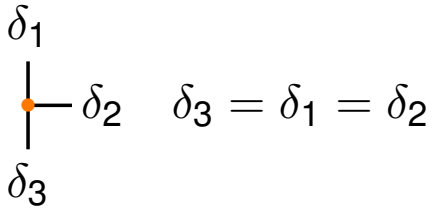


$u_3 = u_1 = u_2$

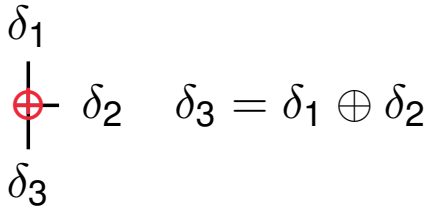
$u_1 = u_2 = 0$
$u_1 \neq 0$ and $u_2 \neq 0$

Rules to find ZC and ID distinguishers

Differential Context :



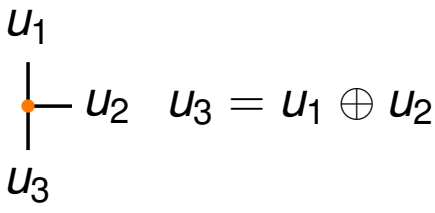
$\delta_3 = \delta_1 = \delta_2$



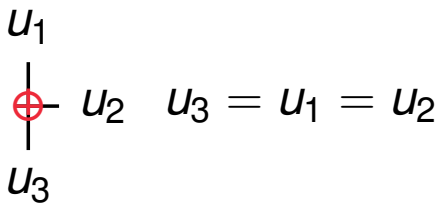
$\delta_3 = \delta_1 \oplus \delta_2$

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

Linear Context :



$u_3 = u_1 \oplus u_2$

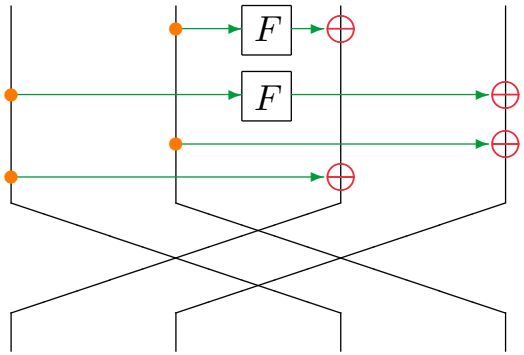


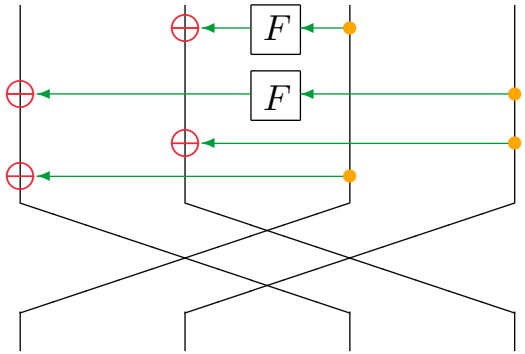
$u_3 = u_1 = u_2$

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

$\oplus$ and $\bullet$ ”play orthogonal roles”

Mirror Round Function



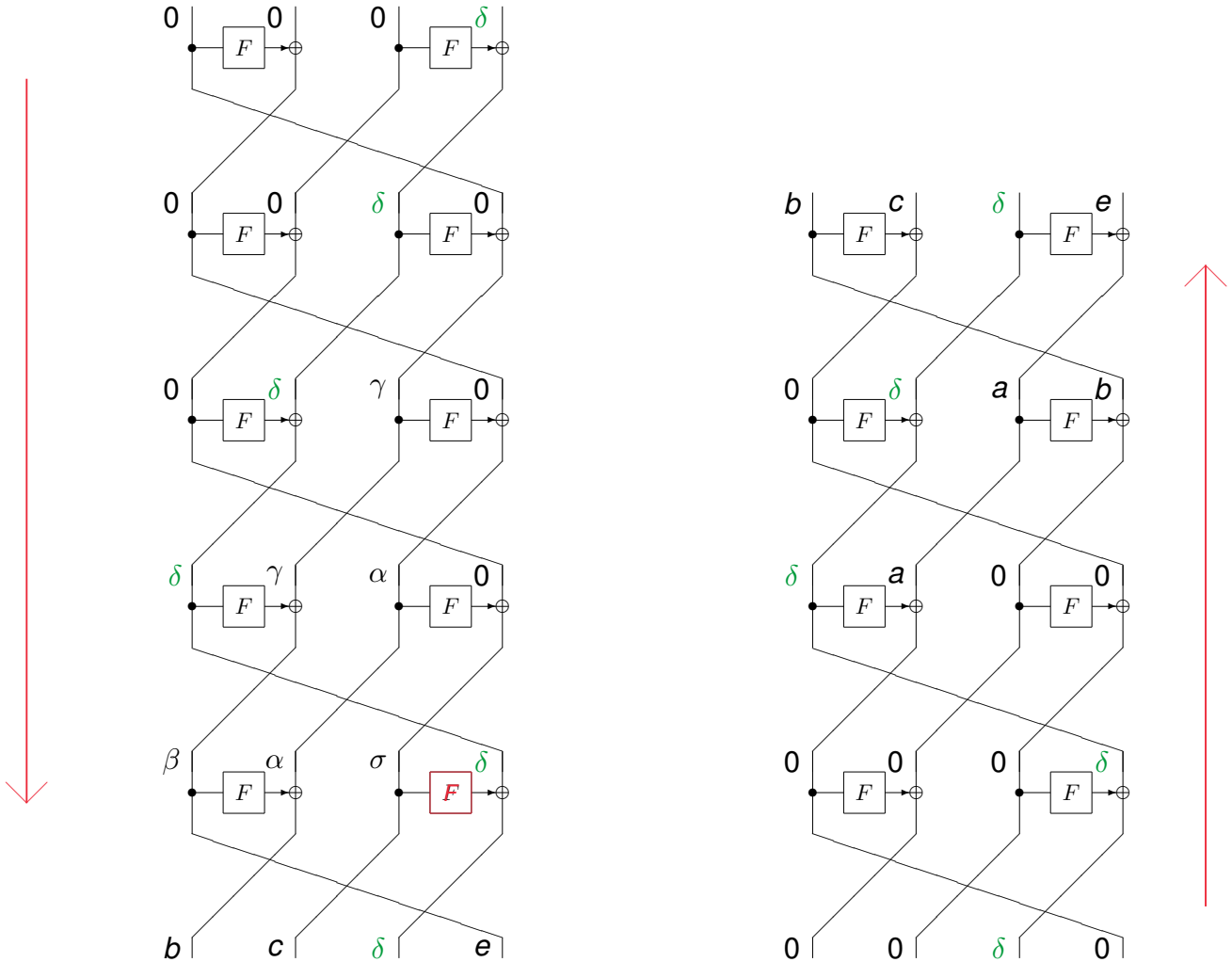


$$\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$$

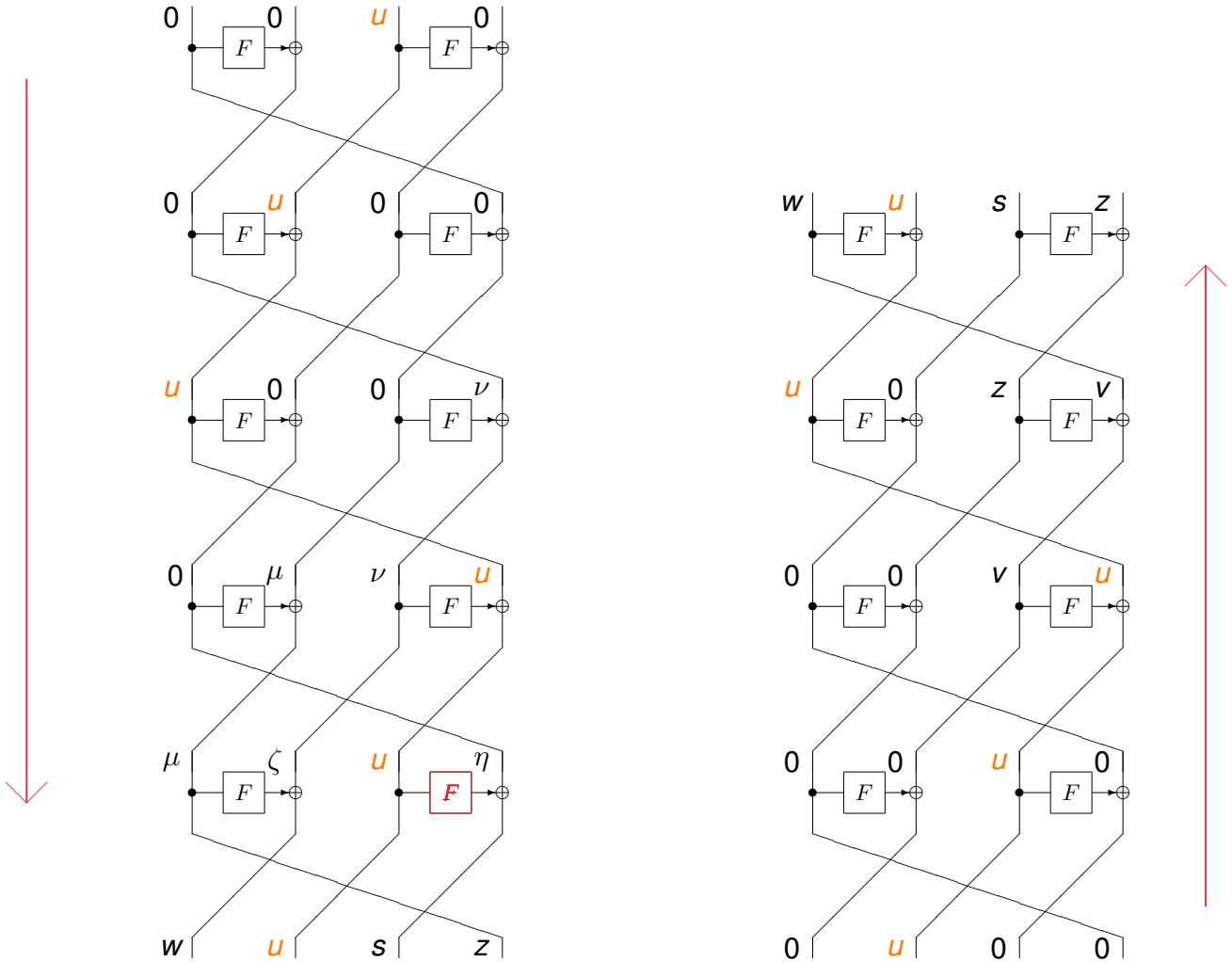
$$\mathcal{M} = \mathcal{P} \cdot \mathcal{X}^T \cdot \mathcal{F}^T$$

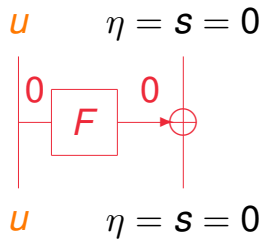
- $\mathcal{M}$ is the matrix representation of the mirror round function
- In general $\mathcal{M}^T \neq \mathcal{R}$
- Used to find ZC distinguishers [Soleimany Nyberg 2013]

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 distinguisher 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 distinguisher 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 ($\mathcal{R} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{F}$) :

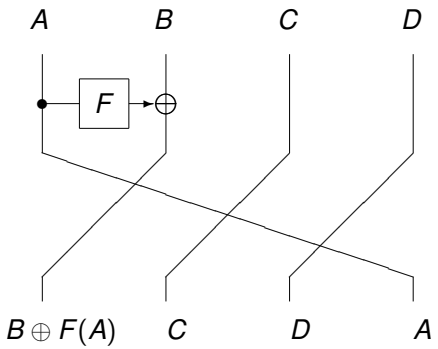
$$\mathcal{R} = \mathcal{Q} \cdot \mathcal{M} \cdot \mathcal{Q}^{-1} \text{ or } \mathcal{F} \cdot \mathcal{P} \cdot \mathcal{X} = \mathcal{Q} \cdot \mathcal{M}^{-1} \cdot \mathcal{Q}^{-1}$$

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

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

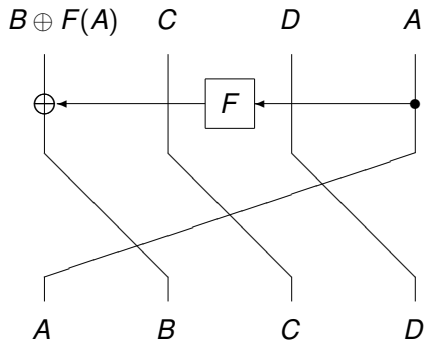
Illustration of the Proof for a Type-I Feistel

Round function



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

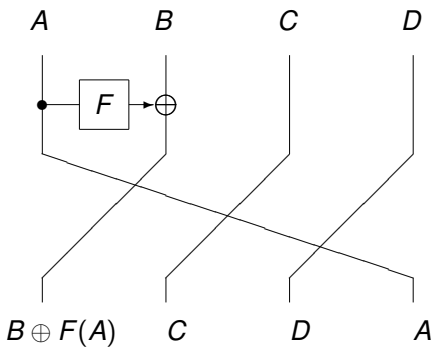
Inverse function



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

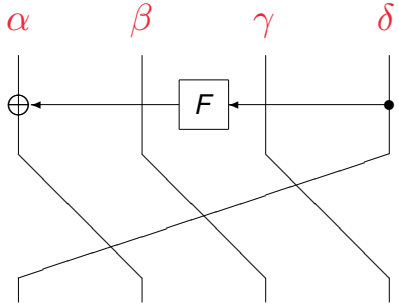
Illustration of the Proof for a Type-I Feistel

Round function



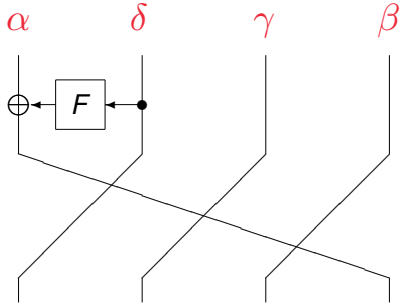
$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$$

Inverse function



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

Permutation of the branches

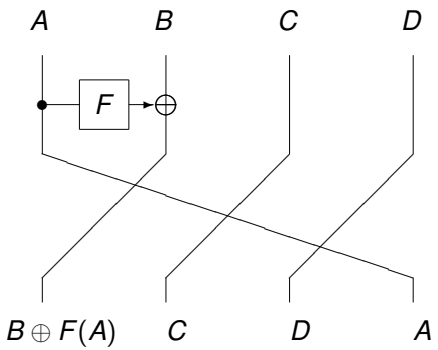


$$\mathcal{Q} \cdot \mathcal{R}^{-1} \cdot \mathcal{Q}^{-1}$$

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

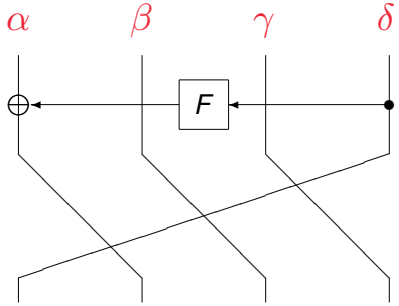
Illustration of the Proof for a Type-I Feistel

Round function



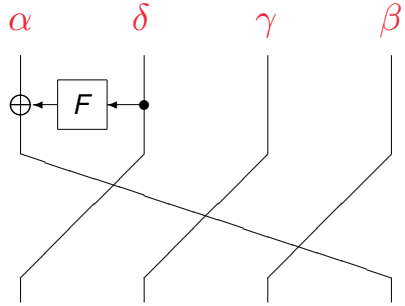
$$\mathcal{R} = \mathcal{P} \cdot \mathcal{F}$$

Inverse function



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

Permutation of the branches



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

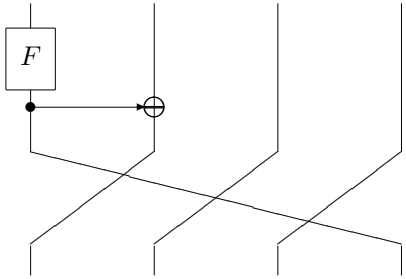
$$(\alpha, \beta, \delta, \gamma) \to (\alpha, \delta, \gamma, \beta)$$

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

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

Illustration for Proof for Skipjack Rule-A

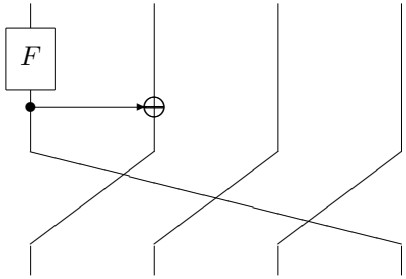
Round function



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

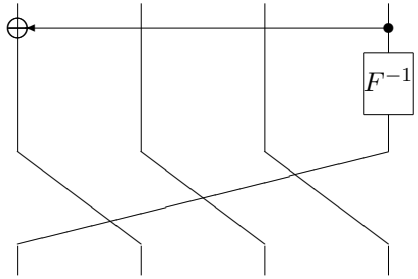
Illustration for Proof for Skipjack Rule-A

Round function



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

Inverse function



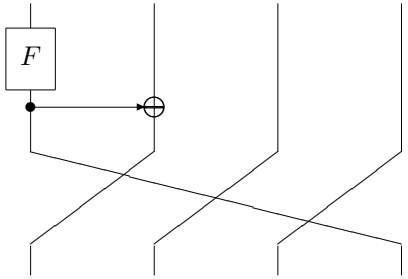
$$\begin{aligned}\mathcal{R}^{-1} &= \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \\ &= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}\end{aligned}$$

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

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

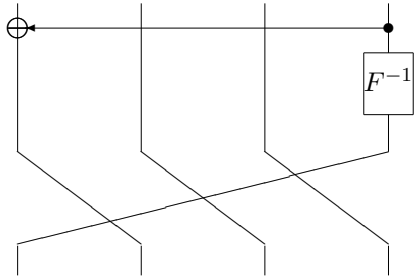
Illustration for Proof for Skipjack Rule-A

Round function



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

Inverse function

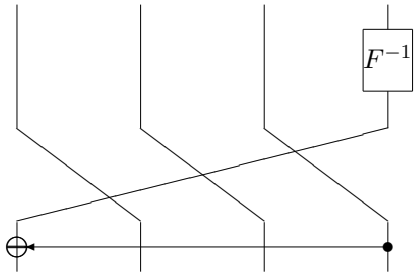


$$\begin{aligned}\mathcal{R}^{-1} &= \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \\ &= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}\end{aligned}$$

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

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

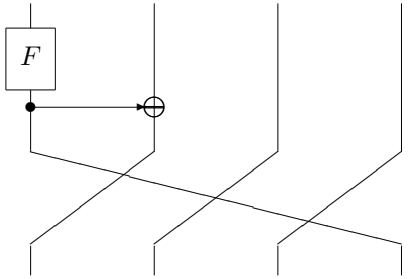
Exchange the order of the operations



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

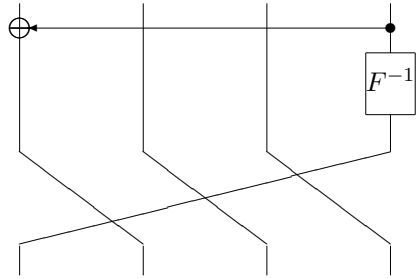
Illustration for Proof for Skipjack Rule-A

Round function



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

Inverse function

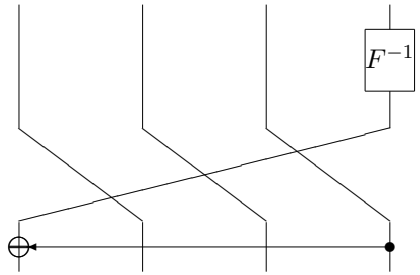


$$\begin{aligned}\mathcal{R}^{-1} &= \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1} \\ &= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}\end{aligned}$$

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

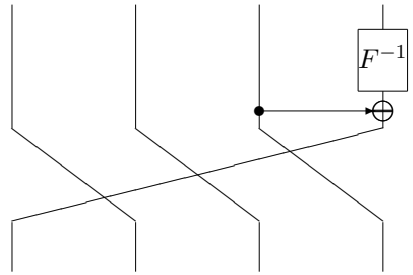
$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

Exchange the order of the operations



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

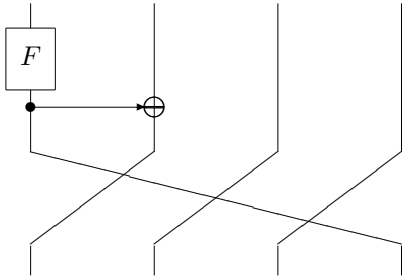
Equivalent formulation



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

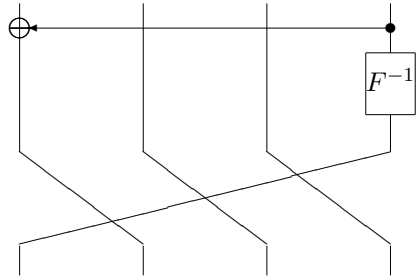
Illustration for Proof for Skipjack Rule-A

Round function



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

Inverse function

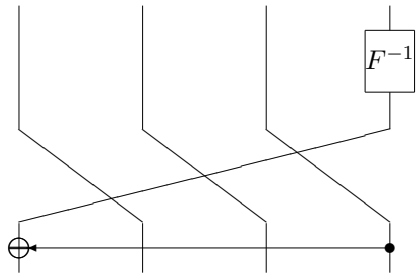


$$\mathcal{R}^{-1} = \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1}$$
$$= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}$$

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

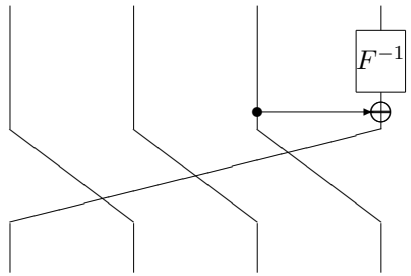
$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

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

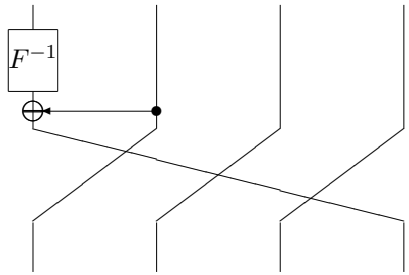
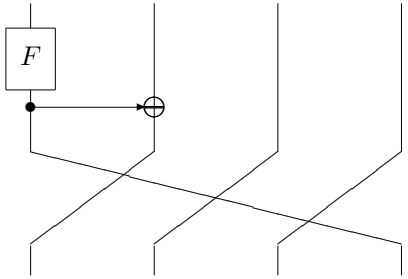


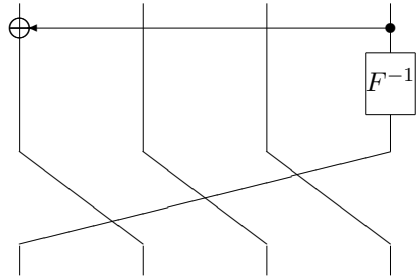
Illustration for Proof for Skipjack Rule-A

Round function



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

Inverse function

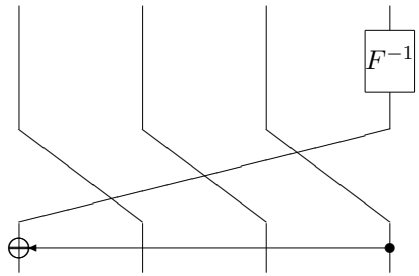


$$\mathcal{R}^{-1} = \mathcal{F}^{-1} \cdot \mathcal{X}^{-1} \cdot \mathcal{P}^{-1}$$
$$= \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1} \cdot \mathcal{X}_*^{-1}$$

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

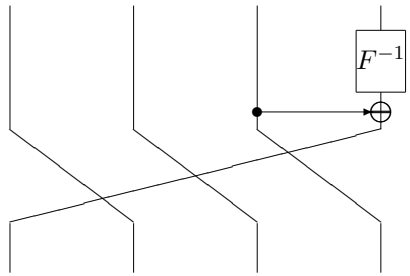
$$\mathcal{X}_*^{-1} = \mathcal{P} \cdot \mathcal{X} \cdot \mathcal{P}^{-1}$$

Exchange the order of the operations



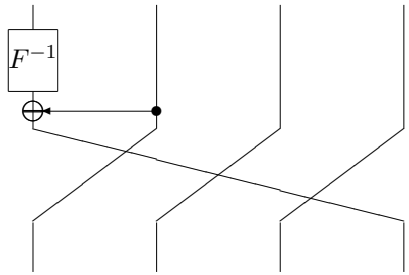
$$\mathcal{X}_*^{-1} \cdot \mathcal{P}^{-1} \cdot \mathcal{F}_*^{-1}$$

Equivalent formulation



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

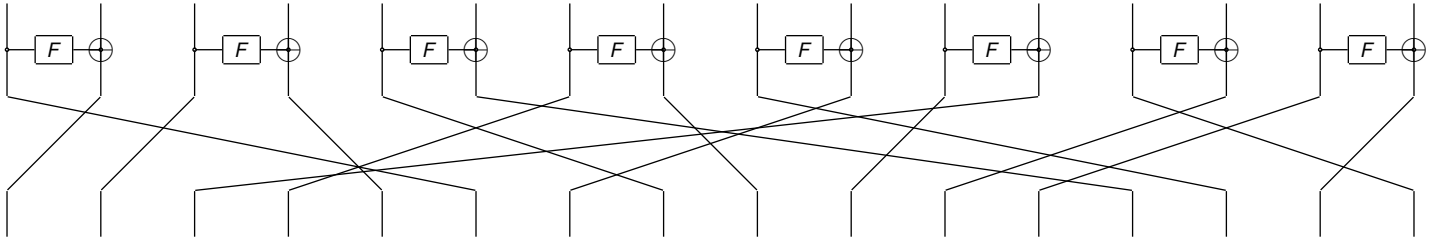
Permutation of the branches



The inverse function is “equivalent” to the mirror function

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

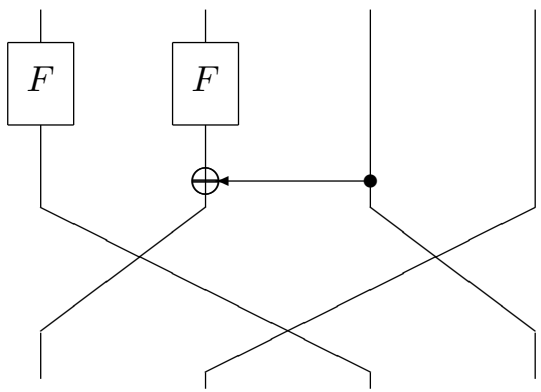
$$\gamma = \{16, 15, 12, 11, 14, 13, 10, 9, 8, 7, 4, 3, 6, 5, 2, 1\}$$

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
    $\pi = \{1, 2, 9, 4, 11, 6, 7, 8, 5, 12, 13, 10, 3, 0\}$

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



Outline

Differential-Linear Cryptanalysis

[Langford and Hellman 94] [Biham et al 02]

- $E = E_0 \circ E_1$
- A truncated differential on E_0
- A linear approximation on E_1

In [Blondeau Leander Nyberg 14]:

- We analyze the model.
- We generalize it to the case of multiple linear approximations and multiple input differences.
- We show that a differential-linear attack is a truncated differential attack.

Integral distinguishers and ZC distinguishers

The link of [Bogdanov et al 12]:

Let $F : \mathbb{F}_2^\alpha \times \mathbb{F}_2^\beta \to \mathbb{F}_2^\gamma \times \mathbb{F}_2^\delta$ a cipher with $H(x, y) = (H_1(x, y), H_2(x, y))$.
If the input and output linear masks u and v are independent, the approximation $< v, H(x) > \oplus < u, x >$ has correlation zero for any $u = (u_1, 0)$, and any $v = (v_1, 0) \neq 0$ (ZC distinguisher) if and only if the function $H_1(\lambda, y)$ is balanced for any λ (ZC integral distinguisher).

A ZC distinguisher with independent masks on r rounds $\Rightarrow$ an integral distinguisher on $r' \geq r$ rounds

An integral distinguisher on r rounds with balanced output set $\Rightarrow$ a ZC distinguisher on r rounds with independent masks

Conclusion

- Some strong relations between statistical attacks have been identified in the last 3 years
- Nevertheless some questions remain regarding the links with some other statistical attacks
- Based on these relations we wonder if we can simplify the security analysis of a symmetric cryptographic primitive