Differential cryptanalysis in block ciphers

Seminar of Departement 1

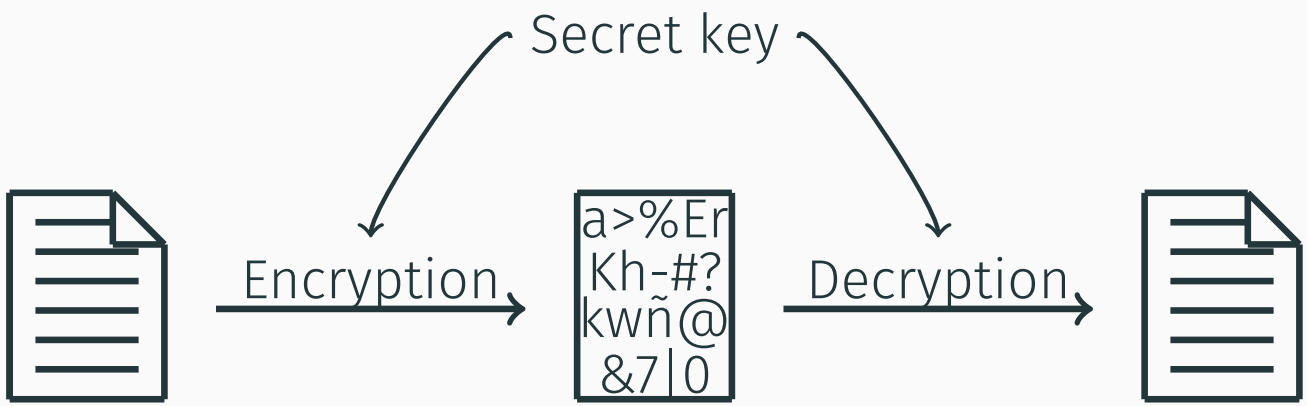
RODRÍGUEZ CORDERO Ana Margarita

11 July 2022

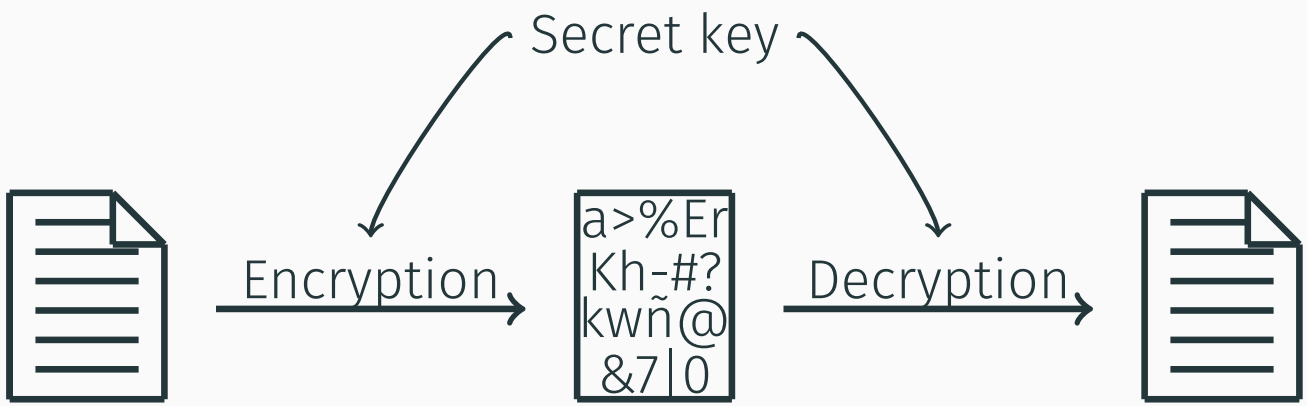
Université de Lorraine
LORIA

Introduction

Symmetric Cryptography

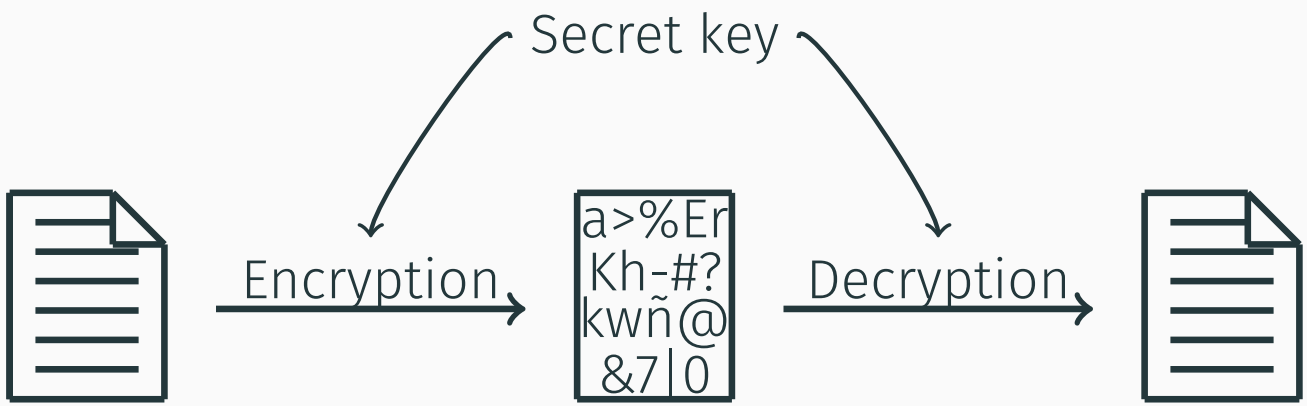


Symmetric Cryptography



- Stream ciphers
- Block ciphers

Symmetric Cryptography

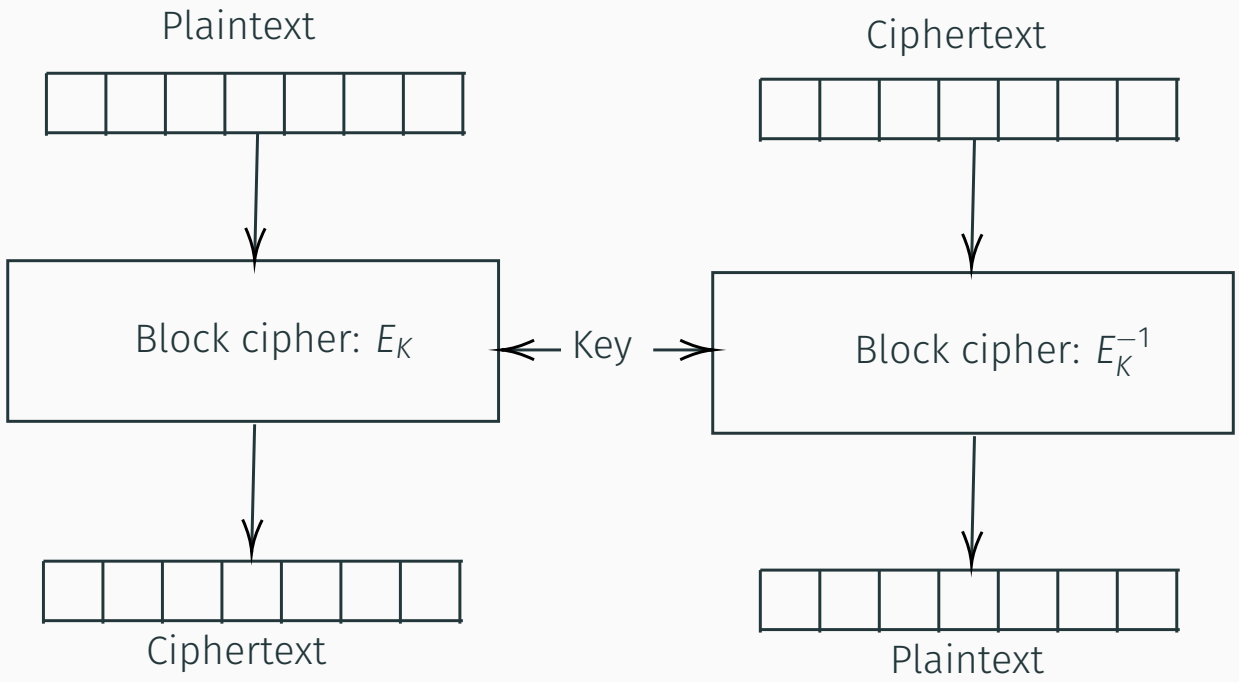


- Block ciphers

Block ciphers

Definition

Given a key $K \in \mathbb{F}_2^m$, a message $M \in \mathbb{F}_2^N$, a *block cipher* of block size n is an invertible function E_K that encrypts the message M in blocks of size n.



Round function

Round function

Linear layer

Round function

Linear layer

- Matrix multiplication

Round function

Linear layer

- Matrix multiplication
- Bit, byte, nibble permutations

Round function

Linear layer

- Matrix multiplication
- Bit, byte, nibble permutations
- Constant additions

Round function

Linear layer

- Matrix multiplication
- Bit, byte, nibble permutations
- Constant additions

Non-linear layer

Round function

Linear layer

- Matrix multiplication
- Bit, byte, nibble permutations
- Constant additions

Non-linear layer

- Substitution boxes (S-boxes)

Round function

Linear layer

- Matrix multiplication
- Bit, byte, nibble permutations
- Constant additions

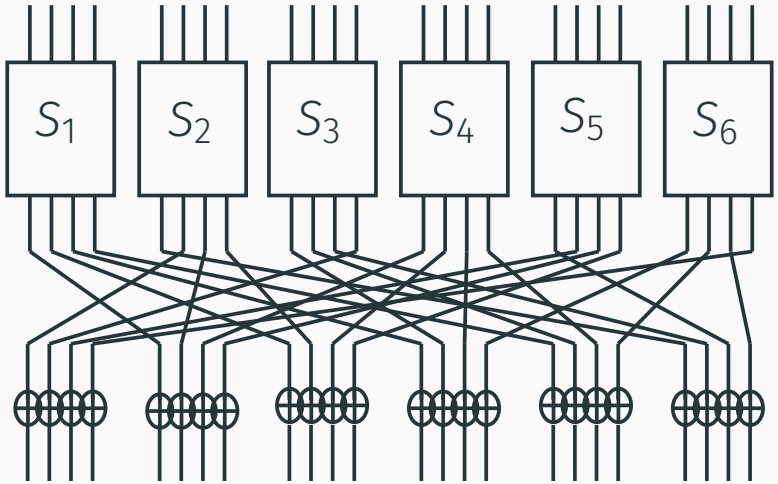
Non-linear layer

- Substitution boxes (S-boxes)

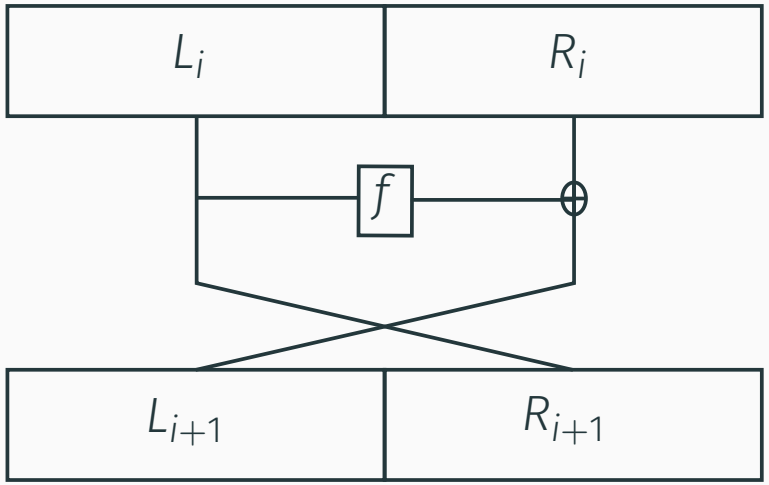
x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7
$S(x)$	0x5	0x3	0x4	0x6	0x2	0x7	0x0	0x1

SPN and Feistel cipher

SP Network



Feistel Structure



Cryptanalysis

Cryptanalysis

- Can we distinguish the cipher from a random permutation?

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?
- Is there any weakness in the design?

Cryptanalysis

- Can we distinguish the cipher from a random permutation?
- Is the ciphertext giving us any information?
- Is there any weakness in the design?

Provable security

Establish and meet security parameters

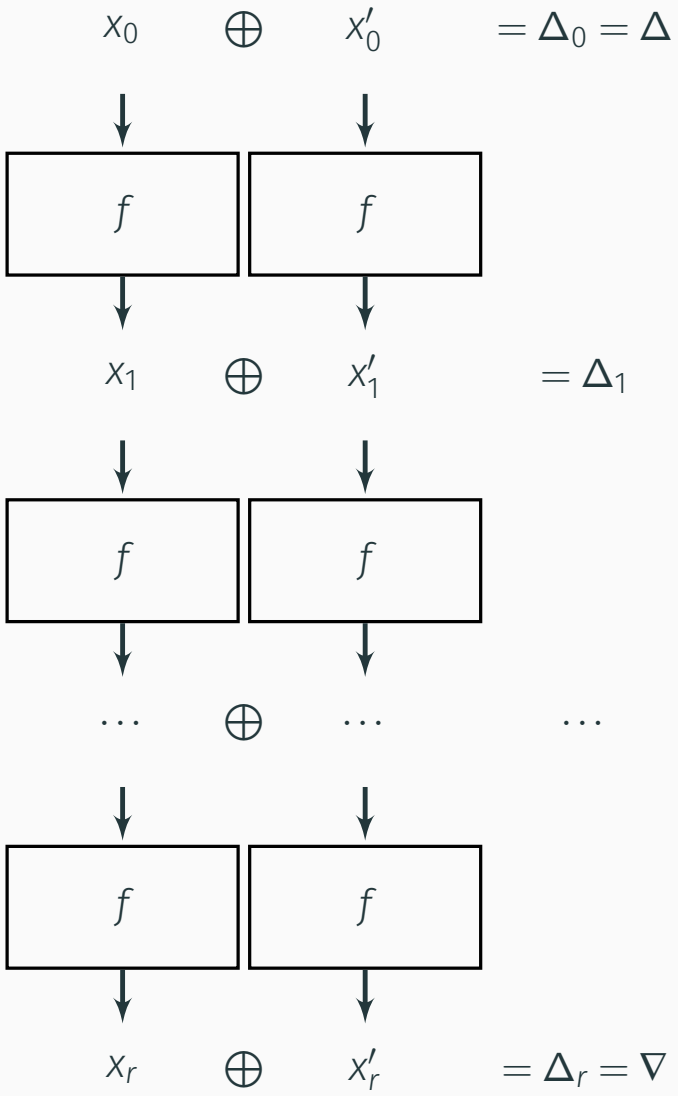
Differential attacks

Differential Attacks

Given a block cipher E, a plaintext P and an unknown key K, differential attacks study the propagation of input differences throughout the cipher:

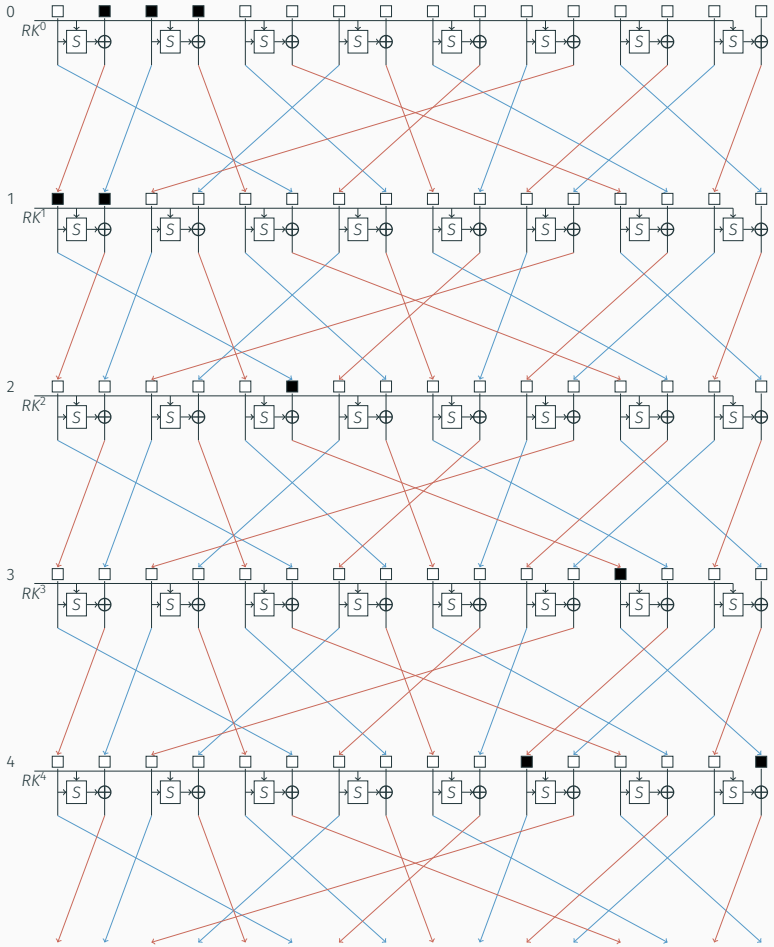
$$\nabla = E_K(P) \oplus E_K(P \oplus \Delta).$$

Differential Attacks

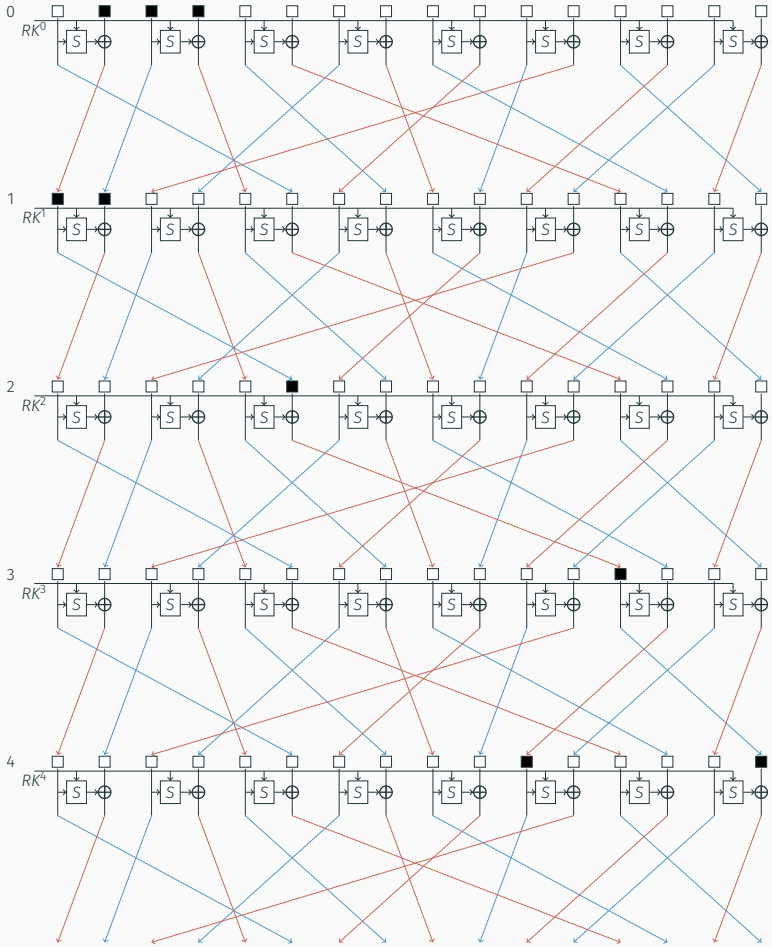


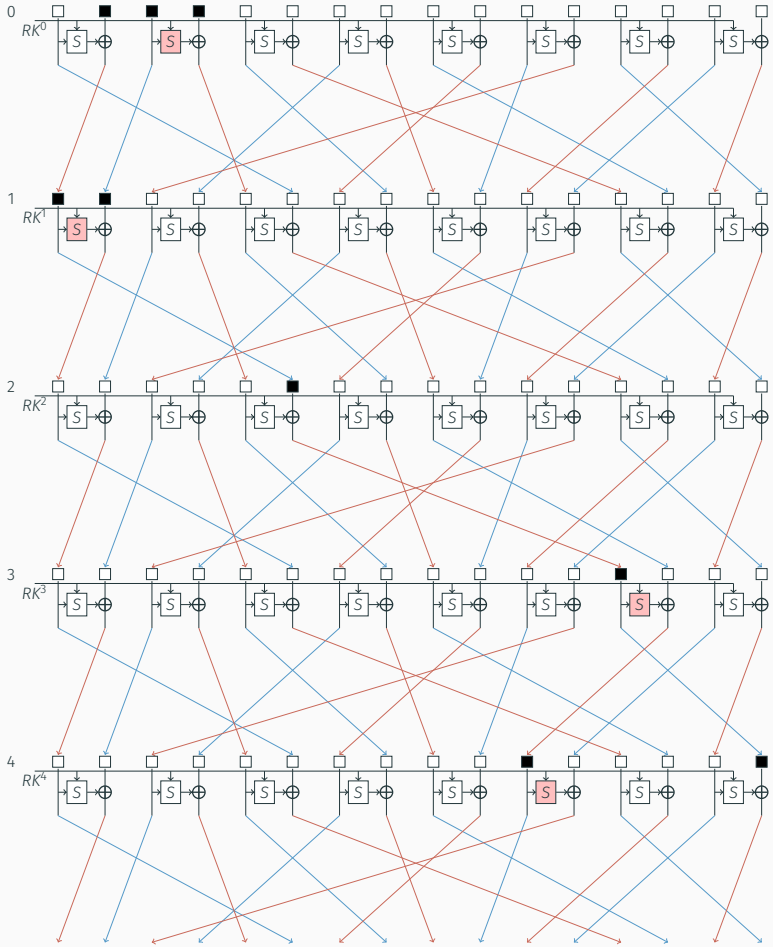
- Δ - input difference
- ∇ - output difference
- $\nabla = E_K(X) \oplus E_K(\Delta \oplus X)$, for $X \in \mathbb{F}_2^n$
- Is $P(\Delta \to \nabla)$ high?

Differential Attack



Differential Attack





Differential property

Differential property

Difference propagates with probability 1 in the linear layer

Differential property

Difference propagates with probability 1 in the linear layer

Difference Distribution Table:

$$DDT(\Delta_i, \nabla_o) = \#\left\{\mathbf{x} \in \mathbb{F}_2^n : S(\mathbf{x}) \oplus S(\mathbf{x} \oplus \Delta_i) = \nabla_o\right\}$$

Δ: Input difference	∇: output difference							
	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7
0x0	8	0	0	0	0	0	0	0
0x1	0	2	2	0	0	2	2	0
0x2	0	2	2	0	0	2	2	0
0x3	0	0	0	4	0	0	0	4
0x4	0	0	0	0	4	0	0	4
0x5	0	2	2	0	0	2	2	0
0x6	0	2	2	0	0	2	2	0
0x7	0	0	0	4	4	0	0	0

Differential Attack

- Step 1: *Abstraction*:
  - Truncated differential patterns.
  - Number of S-boxes minimized.

Differential Attack

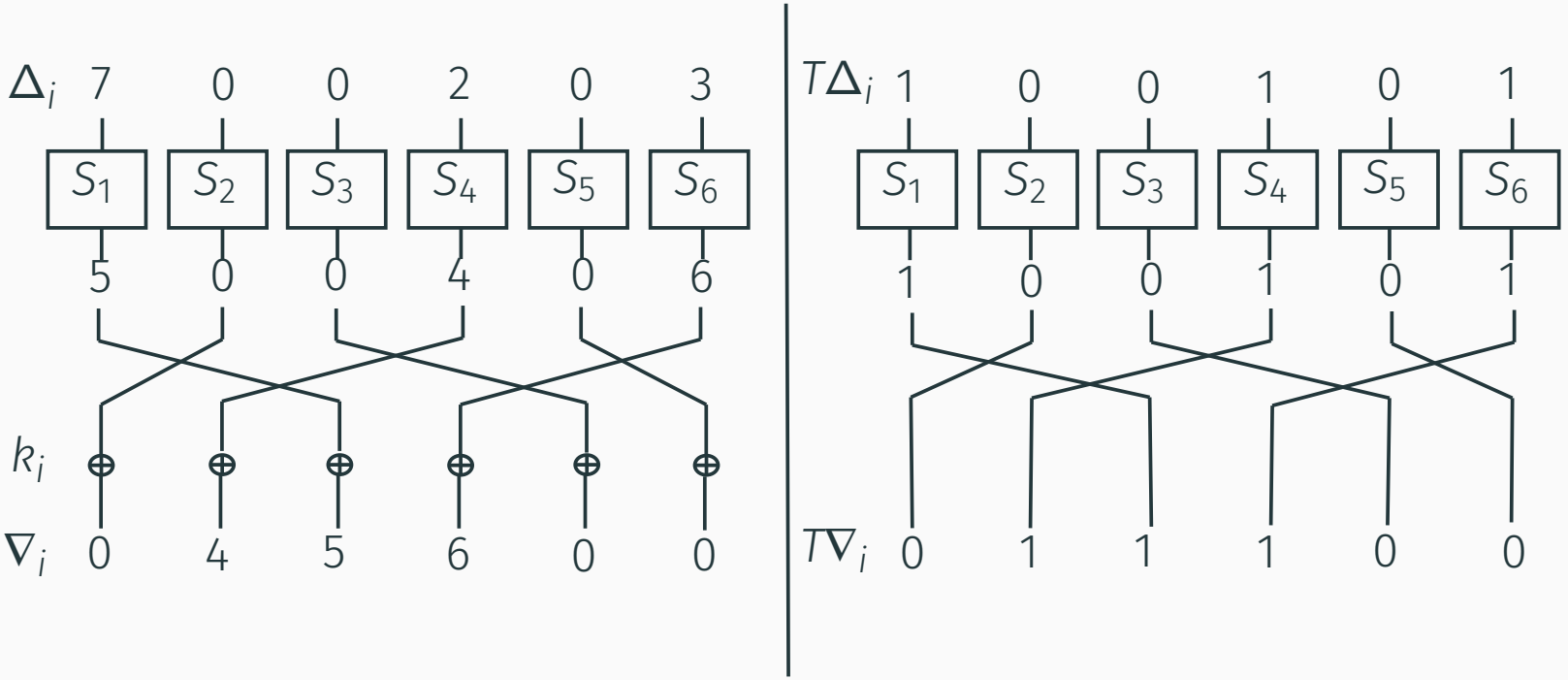
- Step 1: *Abstraction*:
  - Truncated differential patterns.
  - Number of S-boxes minimized.
- Step 2: *Enumeration*:
  - Find non-abstracted differential characteristics: Distinguishers.

Differential Attack

- Step 1: *Abstraction*:
  - Truncated differential patterns.
  - Number of S-boxes minimized.
- Step 2: *Enumeration*:
  - Find non-abstracted differential characteristics: Distinguishers.

$\rightarrow$ Modelling with MILP

Step 1



- Find minimum number of active S-boxes
- Find all difference patterns minimizing the active number of S-boxes

Step 2

- Find a differential characteristic that fits the truncated pattern.
- Modelling the S-box Difference Distribution Table

Linear S-box modelling

S-box modelling

- Conditional modelling technique
  $(x_0, \ldots, x_{m-1}) = (\delta_0, \ldots, \delta_{m-1}) \in \{0,1\}^m$ implies $x_m = \delta_m \in \{0,1\}$

$$\sum_{i=0}^{m-1} (-1)^{\delta_i} x_i + (-1)^{\delta_m + 1} x_m - \delta_m + \sum_{i=0}^{m-1} \delta_i \geq 0$$

- H representation of the convex hull
  - Greedy algorithm
  - Minimizing the set of inequalities as a MILP problem

S-box modelling

- Product-of-Sum Representation of Boolean Functions
  - Representation of the DDT as a boolean function
  - Minimization with Quine-McCluskey (QM) algorithm

Cluster search

Cluster search

Definition

A cluster is a set of differentials with the same input-output differences

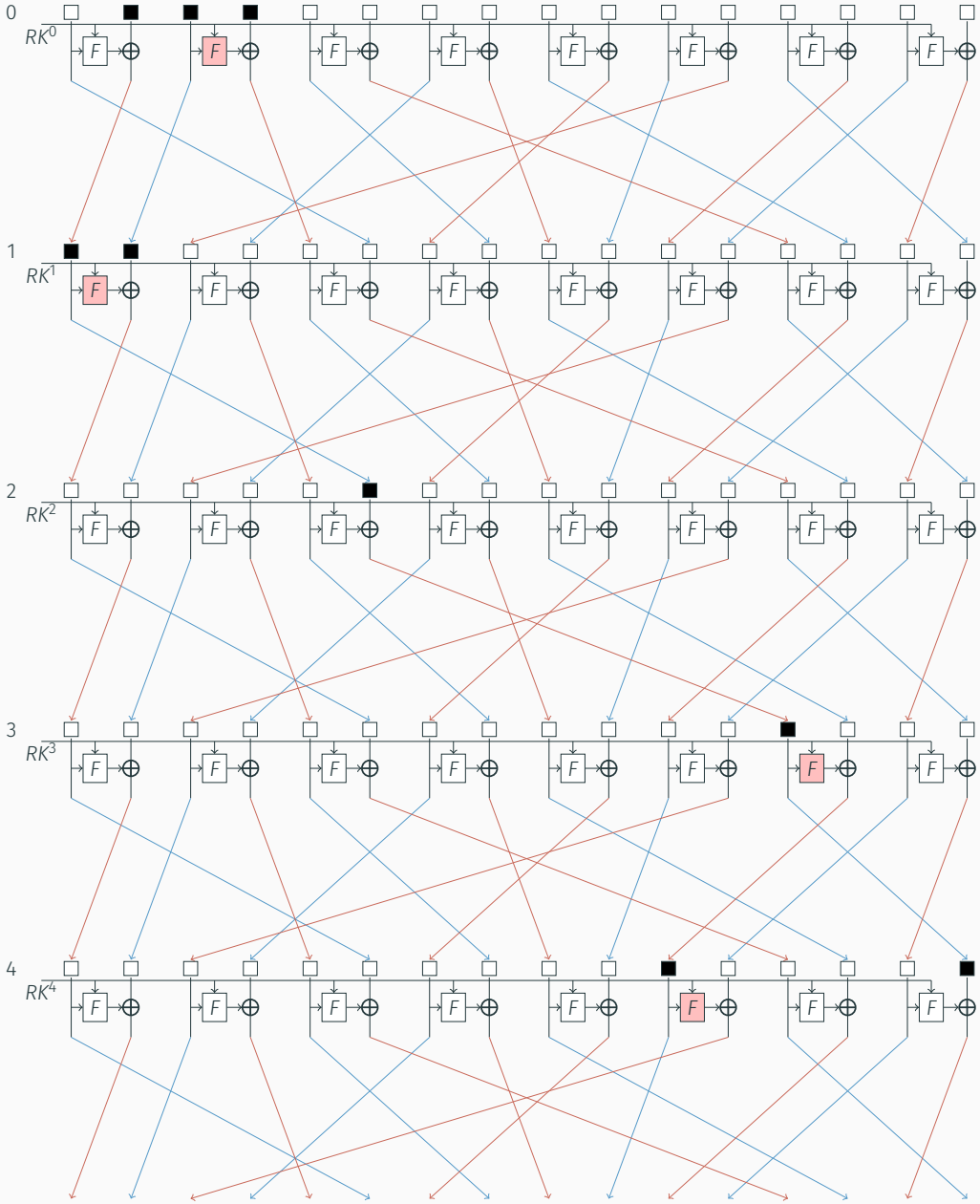
Cluster search

Definition

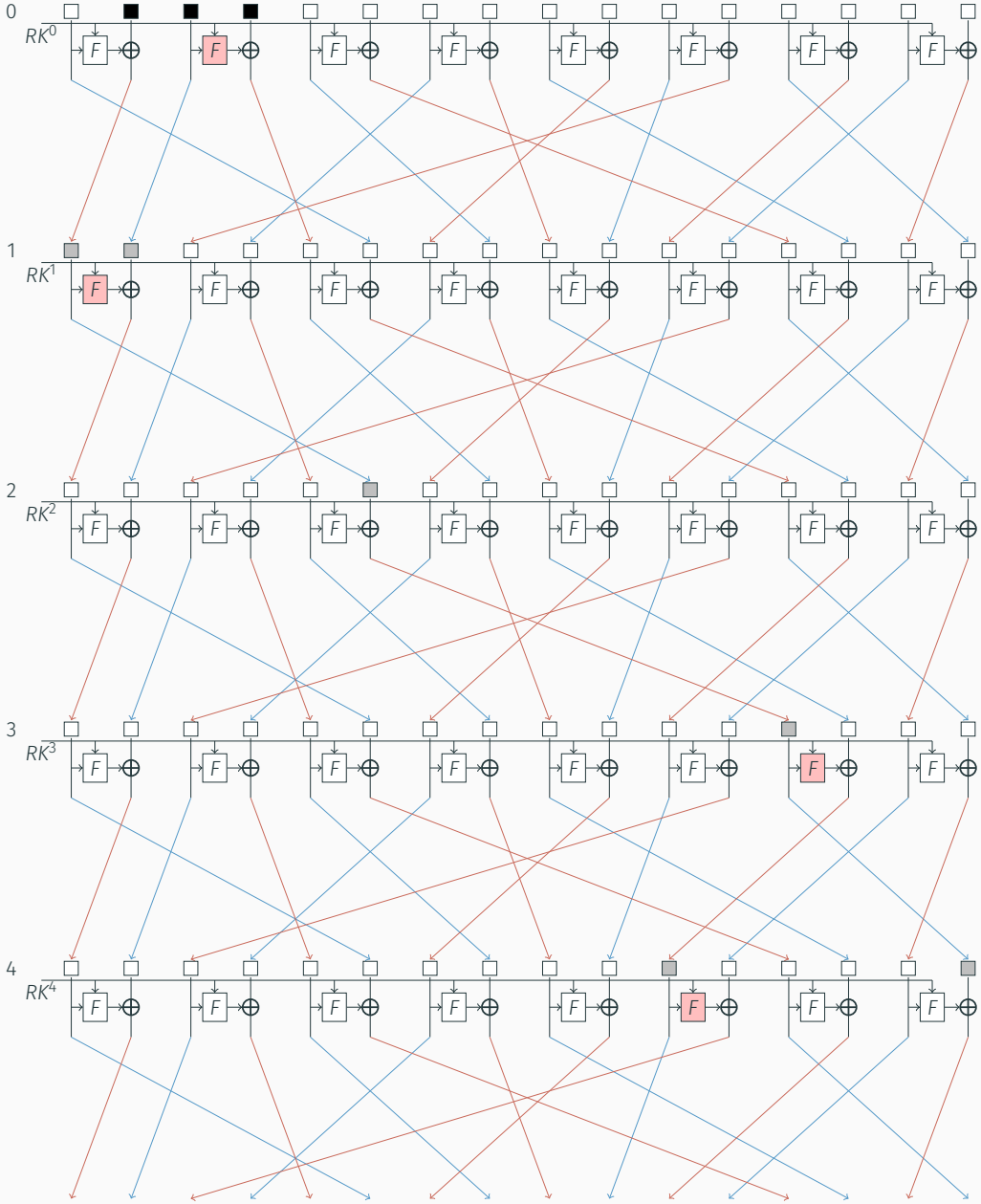
A cluster is a set of differentials with the same input-output differences

- Hard to know the exact probability of a difference $\rightarrow$ Clusters

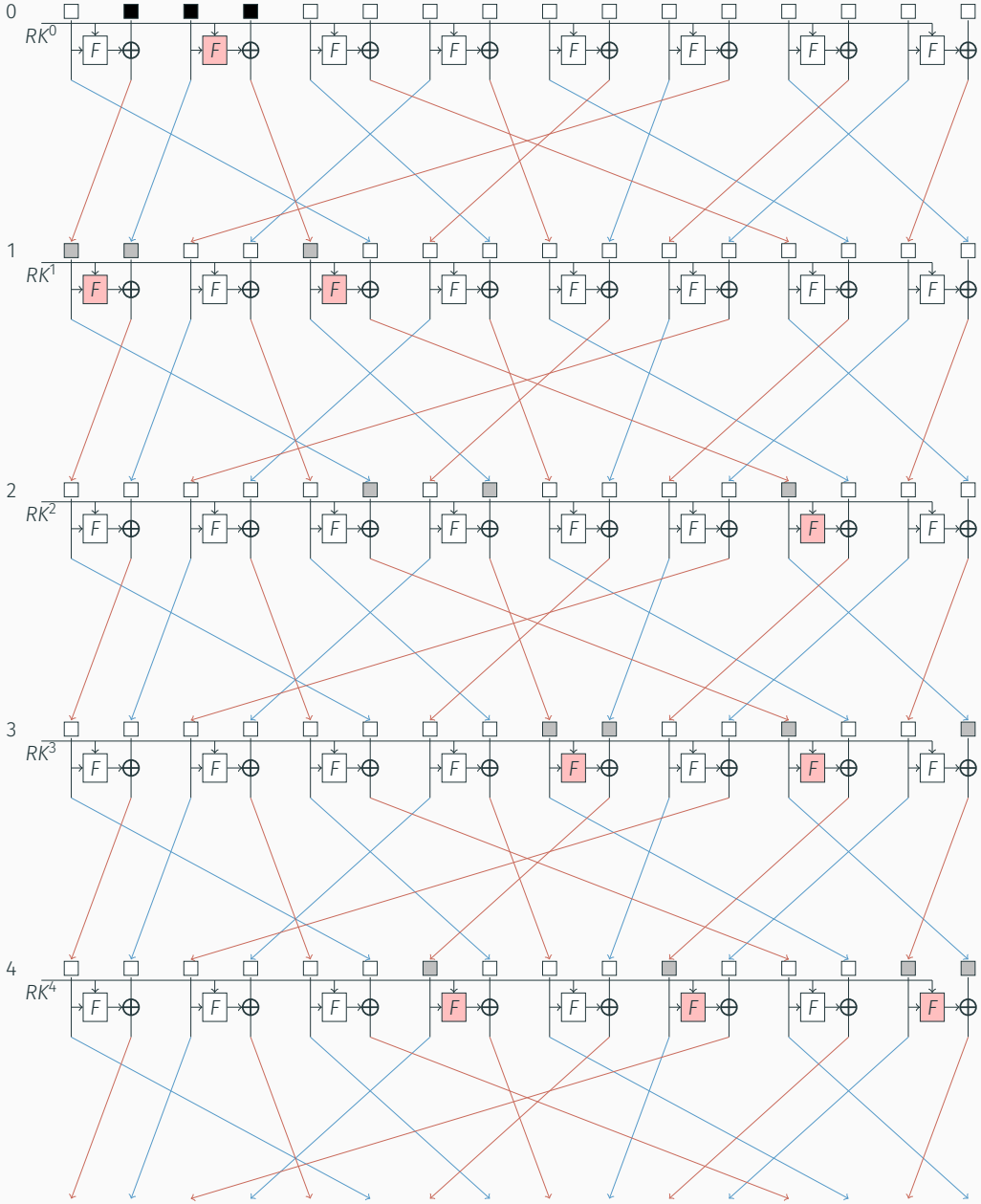
Cluster search



Cluster search



Cluster search



Differential cryptanalysis in block ciphers

Seminar of Departement 1

RODRÍGUEZ CORDERO Ana Margarita

11 July 2022

Université de Lorraine
LORIA