Smart Trusted Technologies & Services for the Networked Society

September 25-27, 2013 – Nice, French Riviera

Fault Injection to Reverse Engineer DES-like Cryptosystems

Hélène Le Bouder, Sylvain Guilley, Bruno Robisson, Assia Tria

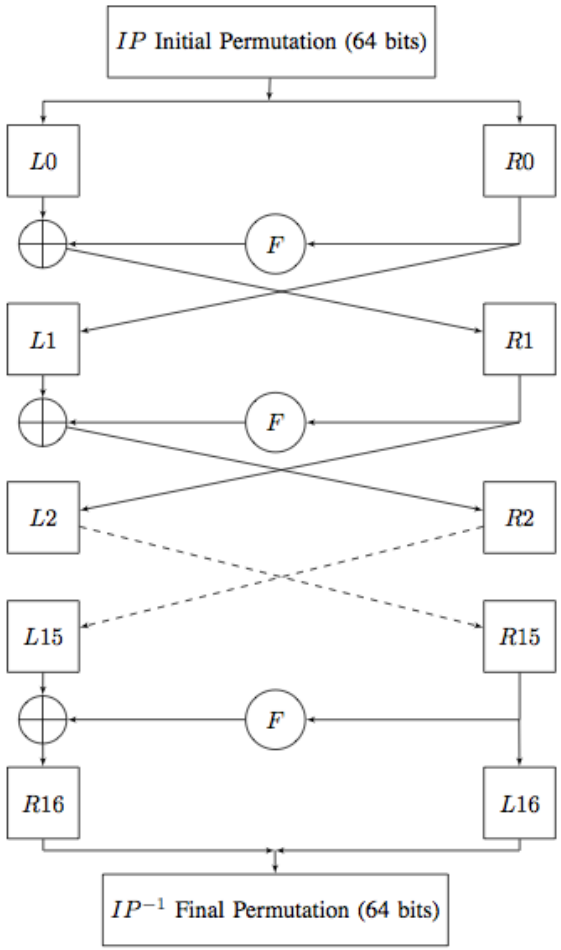
26 September 2013

- In contradiction with Kerckhoffs' principle [?], private algorithms are still used.
- Creating a strong new cryptosystem from scratch is not easy.
- These algorithms respect some properties identical to algorithm which has gained one's spurs.
- When the goal of an attacker is to retrieve information on a private algorithm, his attack is termed reverse engineering.
- Pseudo DES with customized s-boxes.
- Even if an algorithm is securely designed, it may be vulnerable to physical attacks as fault injection attacks.
- The fault injection attacks consist in disrupting the circuit behaviour.
- FIRE Fault Injection for Reverse Engineering.

Plan

DES Data Encrytption Standard

- Established by the NIST [?]
- A symmetric cryptosystem, specifically a 16-round Feistel cipher.
- Starts by IP, a permutation of 64 bits and finishes by its inverse IP^{-1}.
- The round function F on 32 bits consists in 4 steps.
  - Expansion E which maps 32 bits in 48 bits by duplicating half of the bits.
  - $\oplus$ with the 48 bits of round key K_j, $j \in [\![1, 16]\!]$.
  - 8 S-boxes S_i : boolean functions $6 \rightarrow 4$
  - Permutation P of 32 bits.

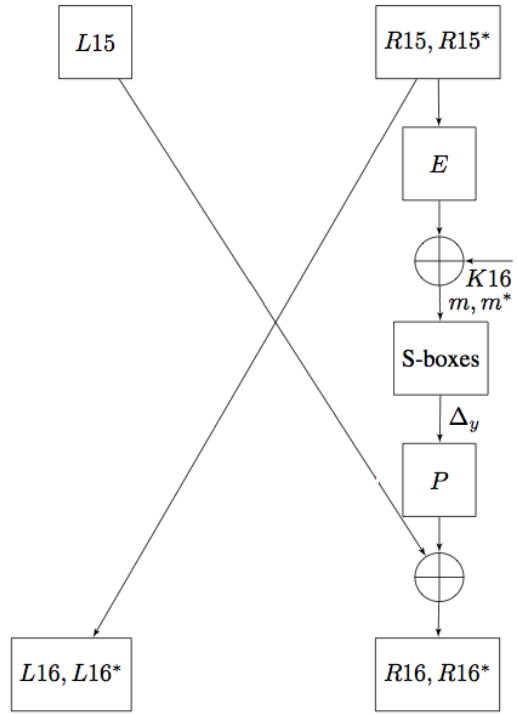


S-boxes

- S-boxes S_i, $i \in [\![1, 8]\!]$ substitute a 6-bits input m_i for a 4-bits output y_i.
- $S_i(m_i) = y_i$
- S-boxes are represented with a table of 4 lines and 16 columns.
- Let m_i be one input, the first and the last bit establish the line number. The bits in the middle establish the column number. To sum up m_i defines the position in the s-box of a cell and y_i defines the value in the same cell.

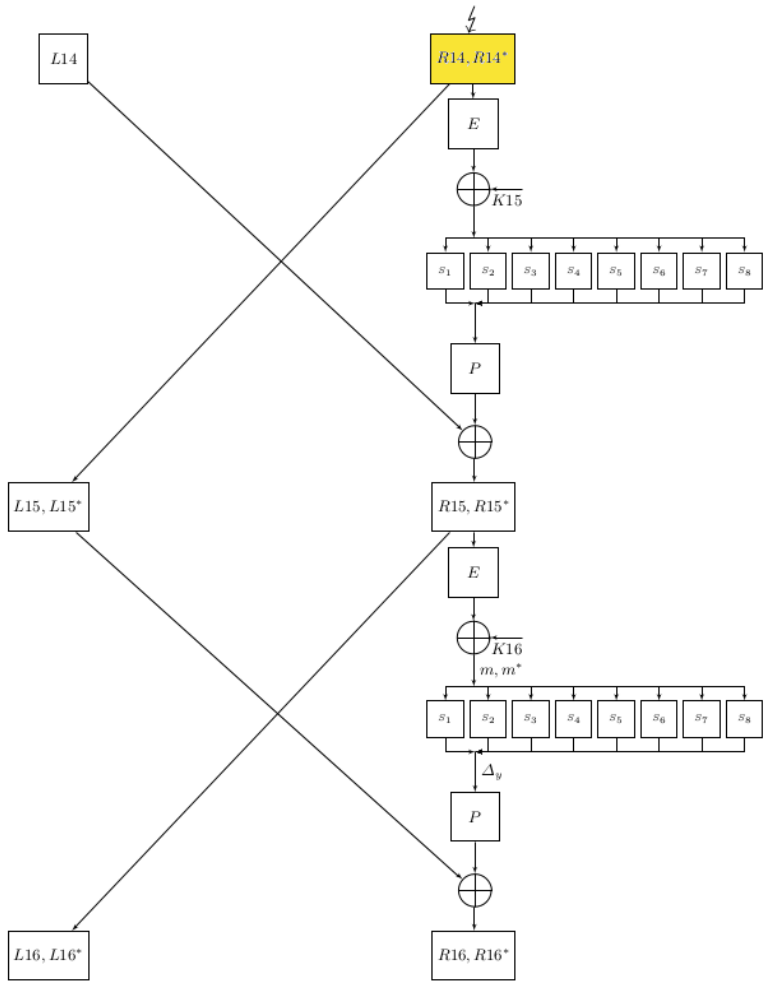
First FIRE attack [?]

- A single bit fault occurs in $R15$.
- C and C^* are known thus $L16$, $R16$, $L16^*$ and $R16^*$ can be obtained with IP.
- $m = E(R15) \oplus K16 = E(L16) \oplus K16$
  $m^* = E(R15^*) \oplus K16 = E(L16^*) \oplus K16$
- $L15$ is unknown, the s-boxes outputs y and y^* cannot be retrieved.
  $y = P^{-1}(R16 \oplus L15)$
  $y^* = P^{-1}(R16^* \oplus L15)$
- $\Delta_y = y \oplus y^* = P^{-1}(R16 \oplus R16^* \oplus L15 \oplus L15) =$
  $P^{-1}(R16 \oplus R16^*)$
- $S_i(m_i) \oplus S_i(m_i^*) = \Delta_{y_i}$
- S-boxes are defined up to a translation.
- They finish with an exhaustive search.



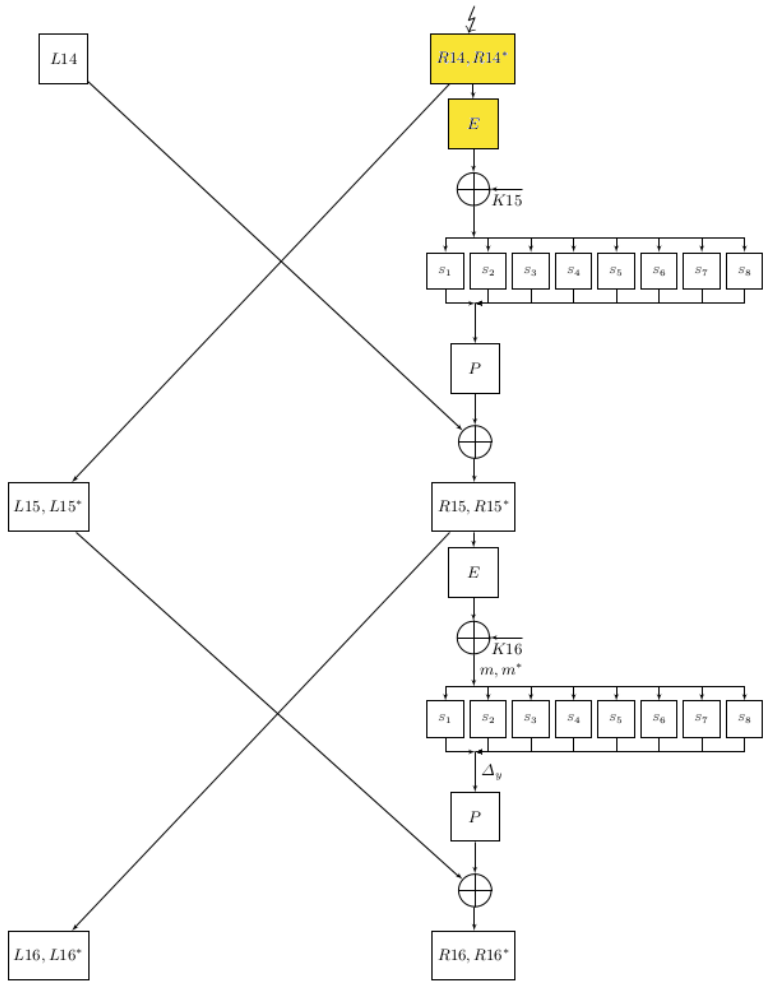
The Attack Path

- A single-bit fault is injected in $R14$.
- The fault is more propagated than in $R15$, i.e. more bits in the s-boxes inputs of the last round are faulted.
- In $R15$ two s-boxes can have faulty inputs i.e 1 or 2 different impacted s-boxes.
- In $R14$ all s-boxes can have faulty inputs i.e 1,2,3,4,5,6,7 or 8 different impacted s-boxes.



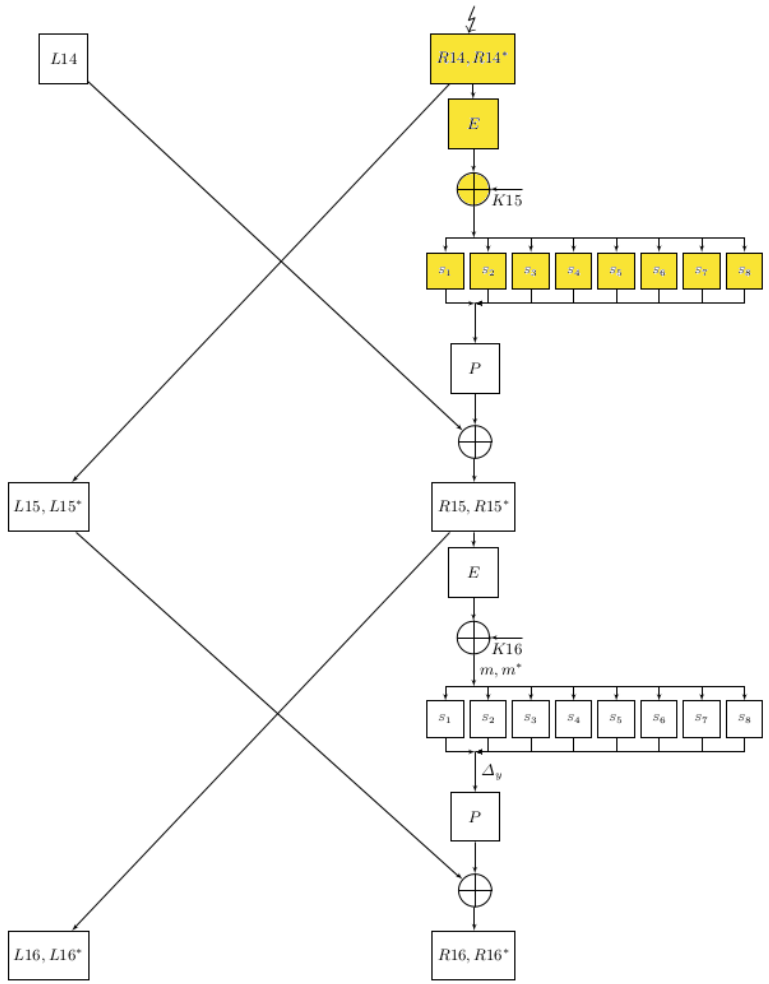
Propagation of the faulty bits

1. E can multiply the numbers of bits by 2.



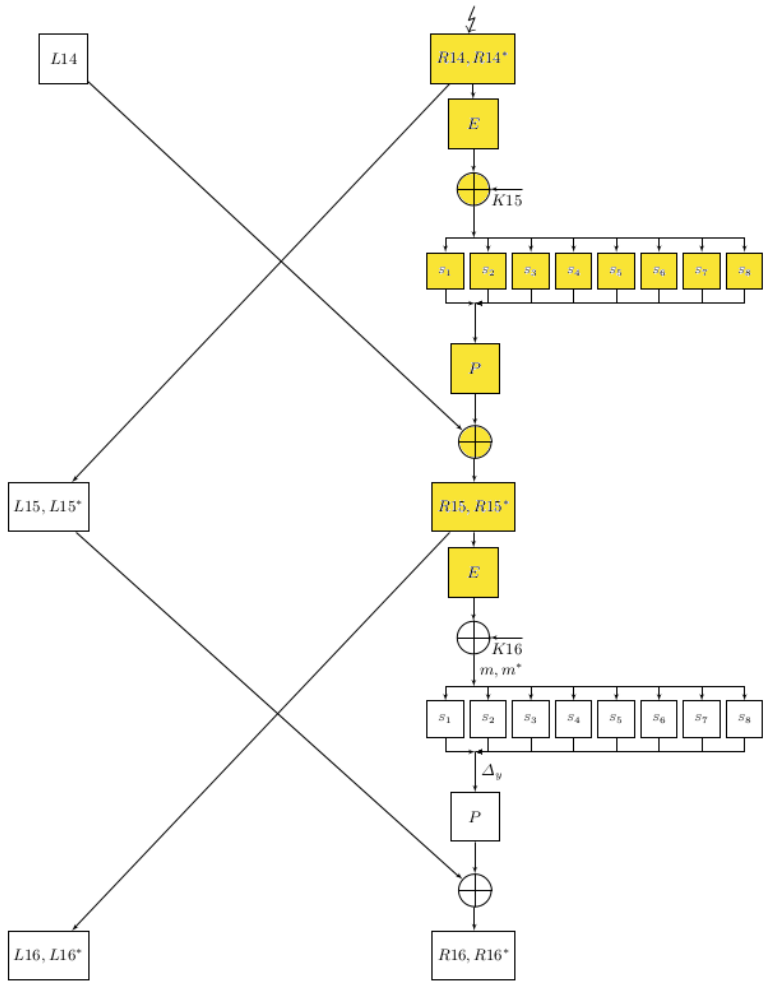
Propagation of the faulty bits

1. E can multiply the numbers of bits by 2.
2. After S-boxes of round 15, the numbers of faulty bits can be equal at 8.



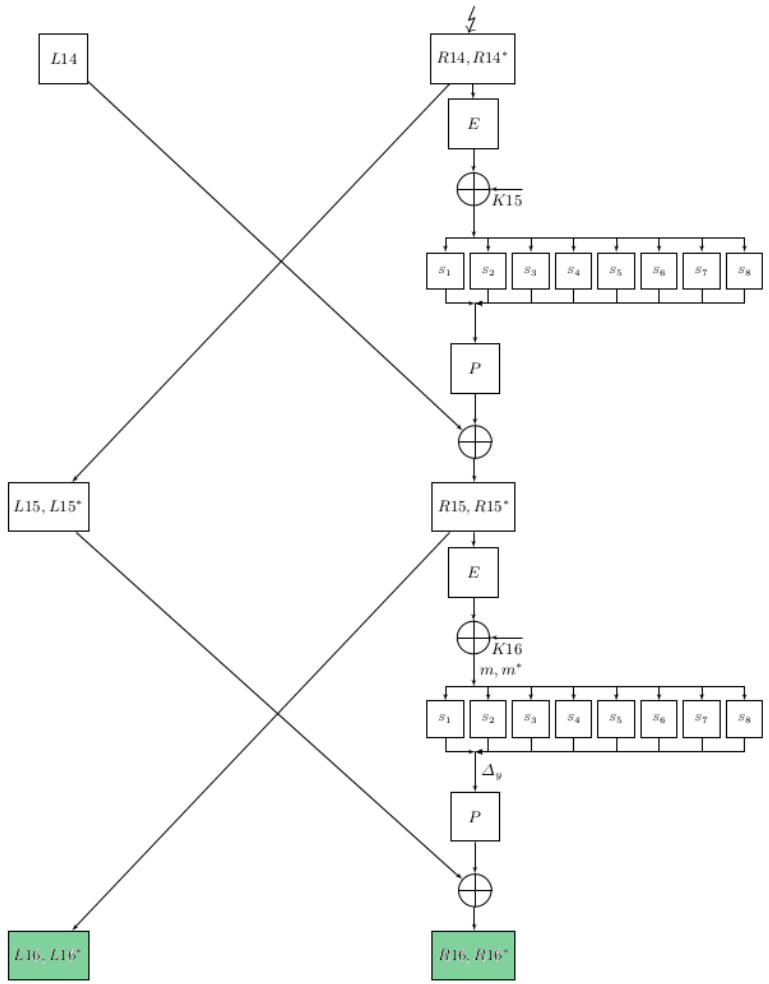
Propagation of the faulty bits

1. E can multiply the numbers of bits by 2.
2. After S-boxes of round 15, the numbers of faulty bits can be equal at 8.
3. Finally thank to the E in round 16, the numbers of faulty bits can be equal at 16.
4. The permutation P dispatches the faulty bits and the 8 s-boxes can have faulty inputs.



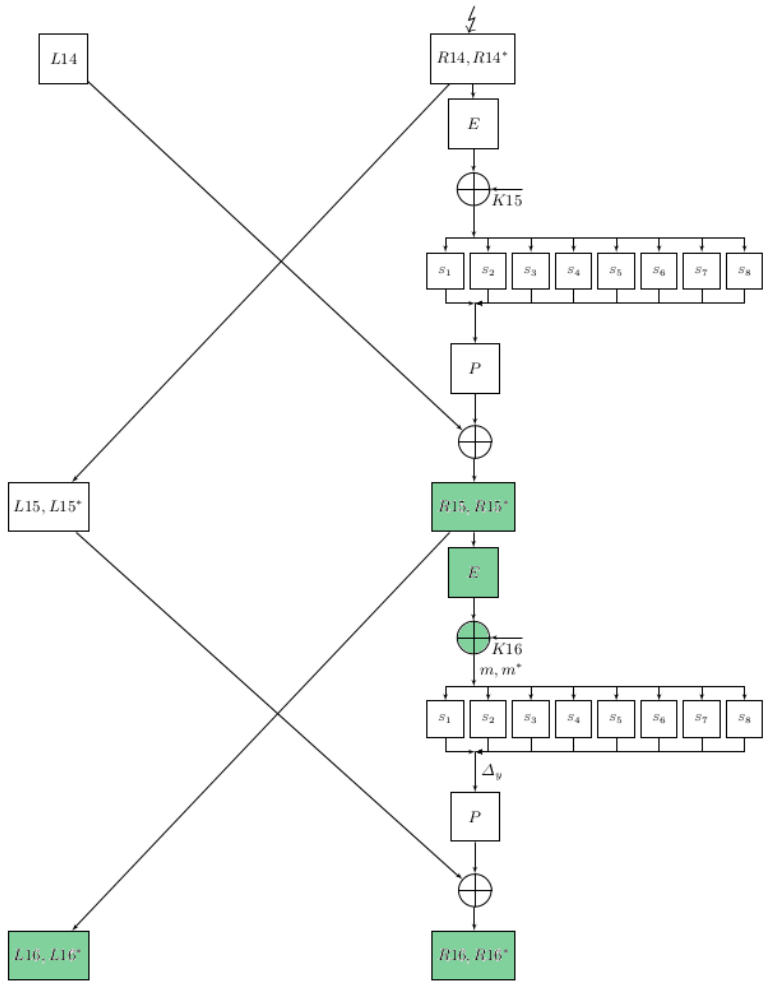
Inputs are known

- As in [?] $R16$, $L16$, $R16^*$ and $L16^*$ are known.



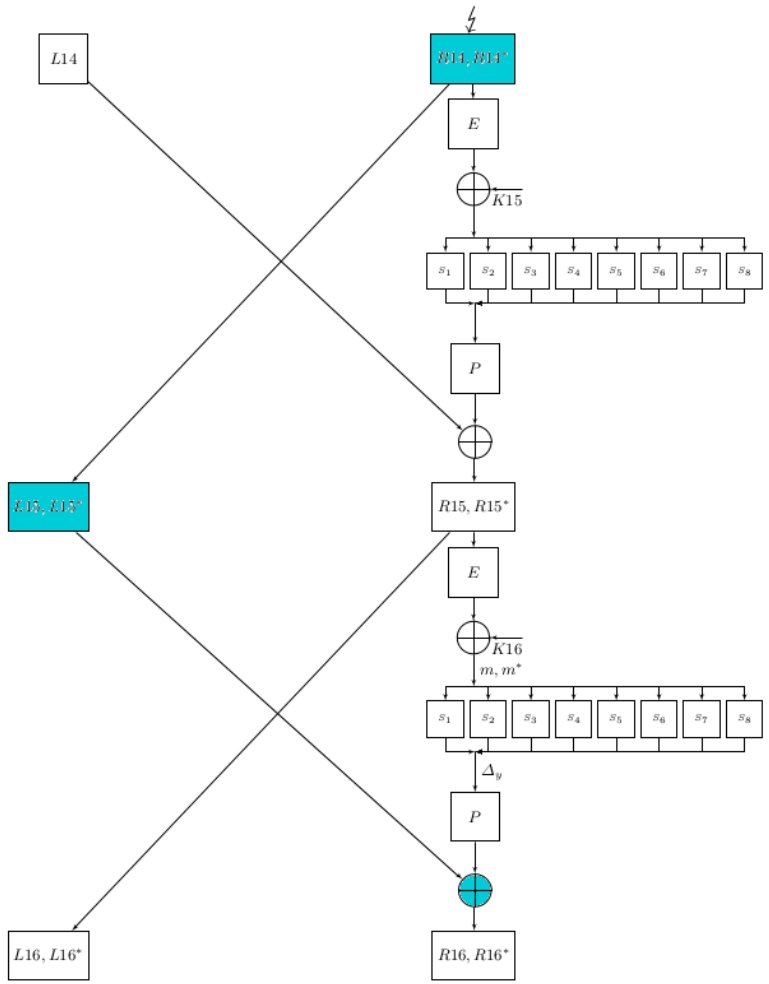
Inputs are known

- As in [?] $R16$, $L16$, $R16^*$ and $L16^*$ are known.
  $\Rightarrow$ Thus the inputs of s-boxes m and m^* are known.

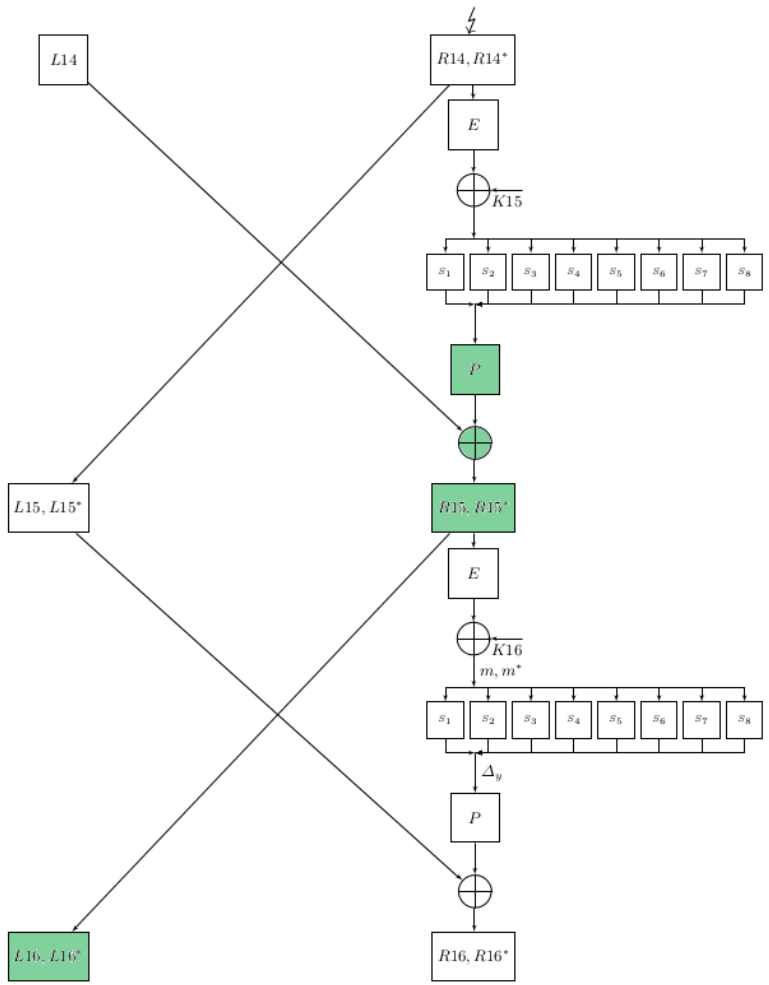


Differential outputs are unknown

- As in [?] $R16$, $L16$, $R16^*$ and $L16^*$ are known.
  $\Rightarrow$ the inputs of s-boxes m and m^* are known.
- $R14^* = L15^* \neq L15$.
  $\Rightarrow \Delta_y = P^{-1}(R16 \oplus R16^* \oplus L15 \oplus L15^*)$ is unknown.



- We can known the differential at the outputs s-boxes in round 15.
- Finally we have only two possible fault values in $R14^*$.
- This uncertainty in taken in account in Δ_y.



S-box properties

We can consider two properties of s-boxes justified by Brickell in [?].

1. Changing 1 input bit of an s-box results in changing at least 2 output bits.
2. Each line of an s-box is a permutation of the integers 0 to 15.

-
-
-
-
-

Statistics about the number of faults necessary to succeed an attack (estimated from 1000 attacks)

statistic tool	without P1 and P2	with P1 and P2
mean	423.07	234.76
standard derivation	63.30	34.08
median	413	231
minimum	313	168
maximum	654	394

Exhaustive search

The results are for 100 attacks with different numbers of faults

Number of faults	Average of number of s-boxes which are retrieved up to a translation	Median of maximal number of guesses to define s-boxes up to a translation	Maximum number of guesses to totaly define s-boxes
120	0.04	$4.549 \cdot 10^{42}$	2^{174}
140	0.89	$9.5105 \cdot 10^{14}$	2^{82}
160	2.76	62208	2^{47}
180	4.53	16	2^{36}
200	6.06	8	2^{35}
220	6.93	4	2^{33}
240	7,5	0	2^{32}

-
-
-
-
-

Bibliographie I

Thank you for your attention

Do you have any questions ?