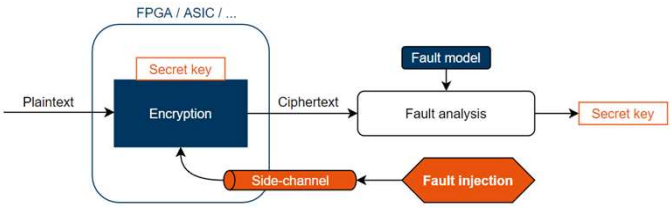
Fault Resistant Symmetric Encryption Implementation

Pierre-Antoine TISSOT, Lilian BOSSUET, Vincent GROSSO
Univ Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien UMR5516, F-42023 St-Etienne, France

Introduction

Fault injection [1]



Error detection [2]

Error detection code $\mathcal{C}$
- $\forall yx_1, x_2 \in \mathcal{C}, x_1 + x_2 \in \mathcal{C}$
- $\forall x \in \mathcal{C}, \forall \in \bar{\mathcal{C}}, x + y \in \bar{\mathcal{C}}$

Code abiding function f
- $\forall x \in \mathcal{C}, f(x) \in \mathcal{C}$
- $\forall y \in \bar{\mathcal{C}}, f(y) \in \bar{\mathcal{C}}$

Example of error detection *parity bit method*
- f an encryption process
- $\mathcal{C} = [5,4,2]_2$
- $x = 010111 \in \mathcal{C}$
- $y = 010001 \quad y' = 010101$
- y is faultless and y' has a fault
- Detection on y'

S-boxes

PRESENT S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

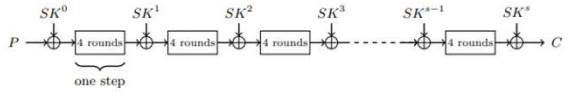
PRESENT S-box extended on 5-bit

x	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
$S[x]$	18	…	…	0A	…	0C	17	…	…	12	00	…	14	…	…	1B
x	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
$S[x]$	…	06	1D	…	1E	…	…	11	09	…	…	0F	…	03	05	…

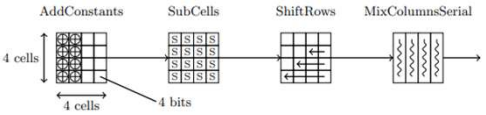
Contribution

Code abiding LED cipher implementation

AES-like design [3]
- Ultra-lightweight 64-bit block symmetric encryption
- 64 and 128-bit length of the kek



LED design
- s steps of 4 rounds

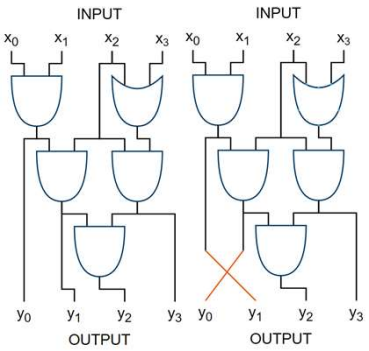


Goal
- Add fault detection to the LED cipher

Equivalence classes

Criteria
- number of logical gates
- information diffusion

Wire crossing equivalence
- same number of gates
- same diffusion



Experimental Results

Error detection

Fault injection on LED
- Fault simulation
- Random bit of the state
- Random moment of the encryption

Results
- Error detected at the end of the encryption

Equivalence classes

Affine equivalence relation : $S \sim A \Leftrightarrow S = B_1 \circ A \circ B_2$ [4]
- 302 affine equivalence classes

Wire equivalence on affine functions : $B \sim C \Leftrightarrow B = \mathcal{L} \circ C$
- 15 362 wire equivalence classes

Global wire equivalence :

$$S \sim W \Leftrightarrow S = B_1 \circ A \circ B_2 = \mathcal{L}_1 \circ C_1 \circ A \circ C_2 \circ \mathcal{L}_2 = \mathcal{L}_1 \circ W \circ \mathcal{L}_2$$

- S an ordinary S-box
- A the affine equivalence representative of S
- B_1 and B_2 some affine functions
- C_1 (resp. C_2) the wire equivalence representative of B_1 (resp. B_2)
- $\mathcal{L}_1$ and $\mathcal{L}_2$ some wire crossings
- W the global wire equivalence representative of S

$15\,362 \times 302 \times 15\,362$ global equivalence classes

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
A	0	1	2	3	4	6	8	A	5	B	C	F	E	D	9	7
B_1	6	7	9	8	4	5	B	A	F	E	0	1	D	C	2	3
B_2	D	8	0	5	2	7	F	A	B	E	6	3	4	1	9	C
C_1	3	7	C	8	2	6	D	9	F	B	0	4	E	A	1	5
C_2	7	1	0	6	8	E	F	9	B	D	C	A	4	2	3	5
W	0	7	3	F	6	B	9	4	5	A	1	E	2	C	8	D

Conclusion

Error detection added on 4-bit operations

Further work
- Add error detection on heavier cipher as AES
- Change error detection to error correction
  - $\mathcal{C} = [6,3,2]_2$

From $16!$ permutations to $15362 \times 302 \times 15\,362$
- Reduction by a 300 factor

References

M. Tunstall, D. Mukhopadhyay, and S. Ali. *Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault*, 2009 **[1]**

T. Simon, L. Batine, J. Daemen, V. Grosso, P. Massolino, K. Papagiannopoulos, F. Regazzoni, and N. Samwel, *Friet: an Authenticated Encryption Scheme with Built-in Fault Detection*, 2020 **[2]**

J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, *The LED Block Cipher*, 2011 **[3]**

C. De Cannière. *Analysis and design of symmetric encryption algorithms*, 2009 **[4]**