Security characterisation of a hardened AES cryptosystem using a laser

Cyril Roscian, Florian Praden,
Jean-Max Dutertre, Jacques Fournier and Assia Tria.

April 26th, 2012

Contents

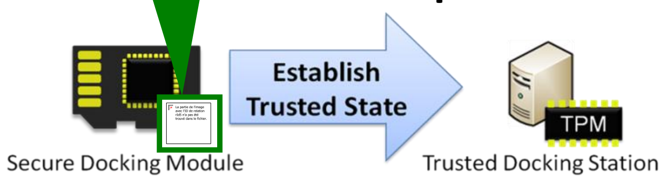
Introduction: SECRICOM context

HW AES to securely & rapidly encipher communication between SDM and TPM

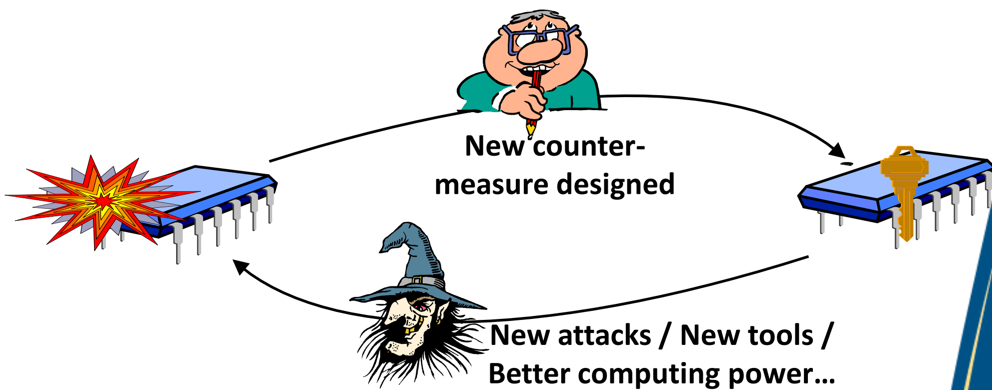
SECURITY PARADIGM

The security of a system is determined by the security of its weakest link

SDM Concept



Constant race between 'hackers' and 'security designers'



It was then vital to implement and validate attack-resistant AES implementations for the SDM

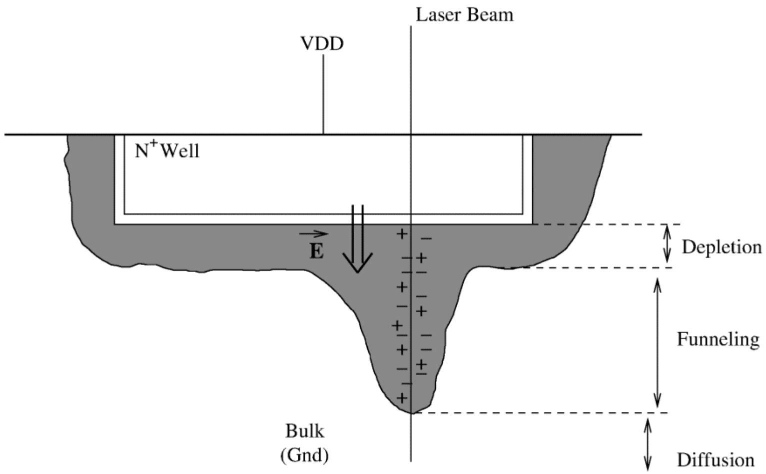
Introduction: Attack techniques

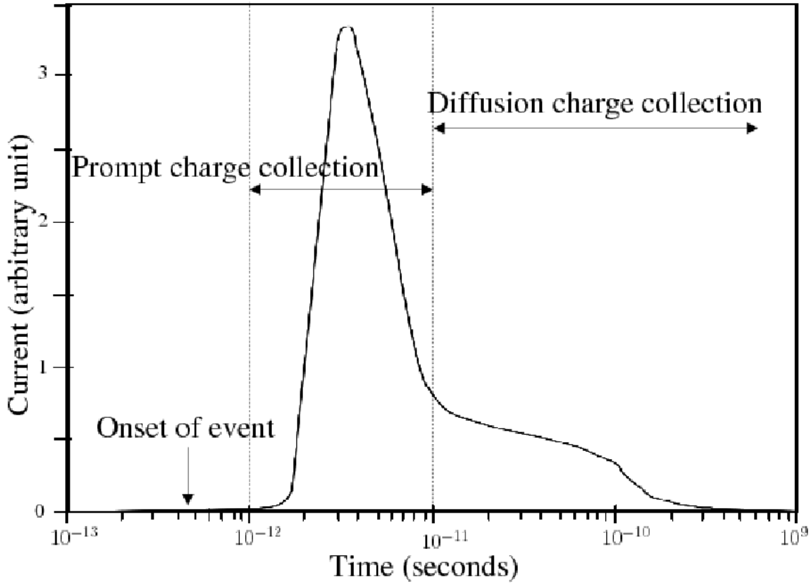
- Physical attacks can be used to retrieve sensitive information.
- Three type of attacks:
  - Invasive attacks
  - Observation or passive attacks
  - Perturbation or fault attacks
- In this presentation we shall present the characterisation work done based on laser-based fault attacks.

Laser-based phenomena on ICs

Single Event Effect

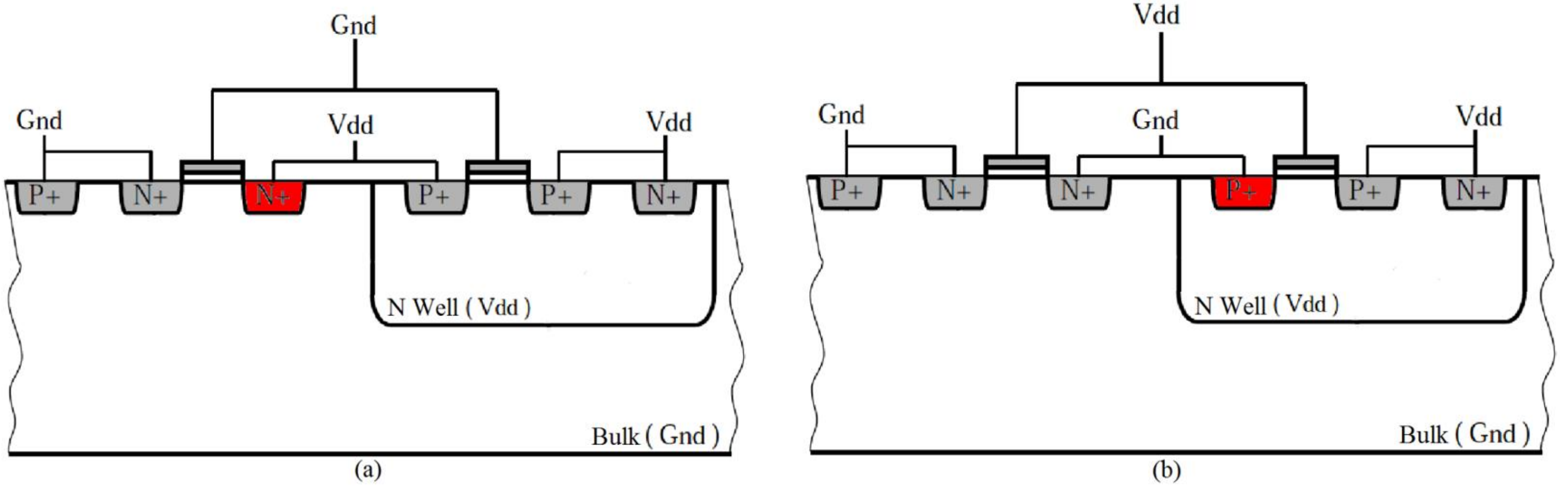
- ★Photo-electric effect (Bandgap energy)
- ★Electron-hole pairs creation
  - ★They drifted in opposite directions
- ★Creation of a transient current





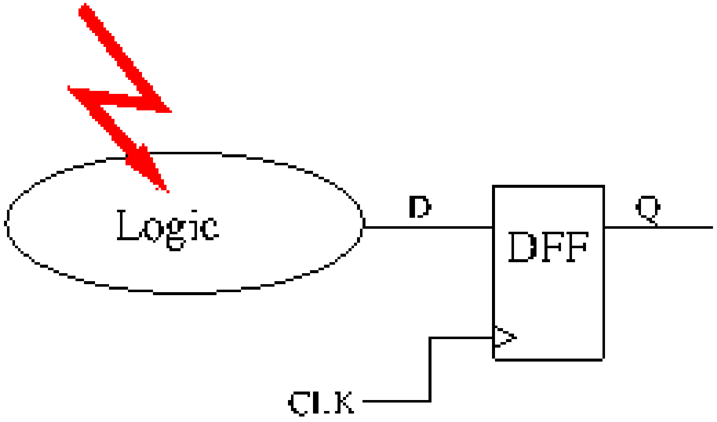
Sensitive Zones

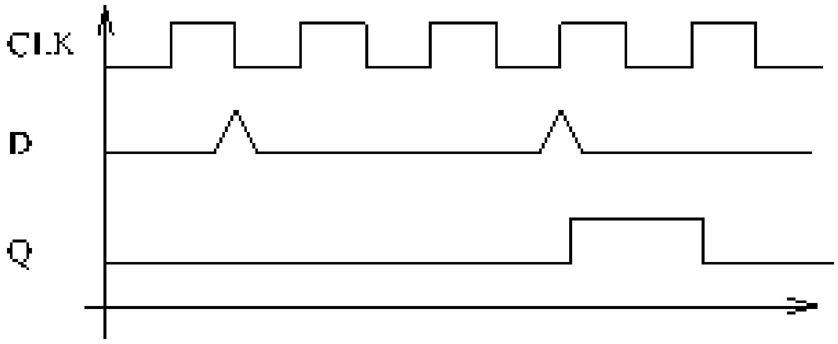
- Strong electric field needed
  - Reverse biased PN junction
- Data dependent
- Example with the inverter



From SEE to faults

- A SEE can be induced without any effect on the target operation
- Two ways to make a fault
  - Change the state of a register of the chip
  - Create a SEE on the logic

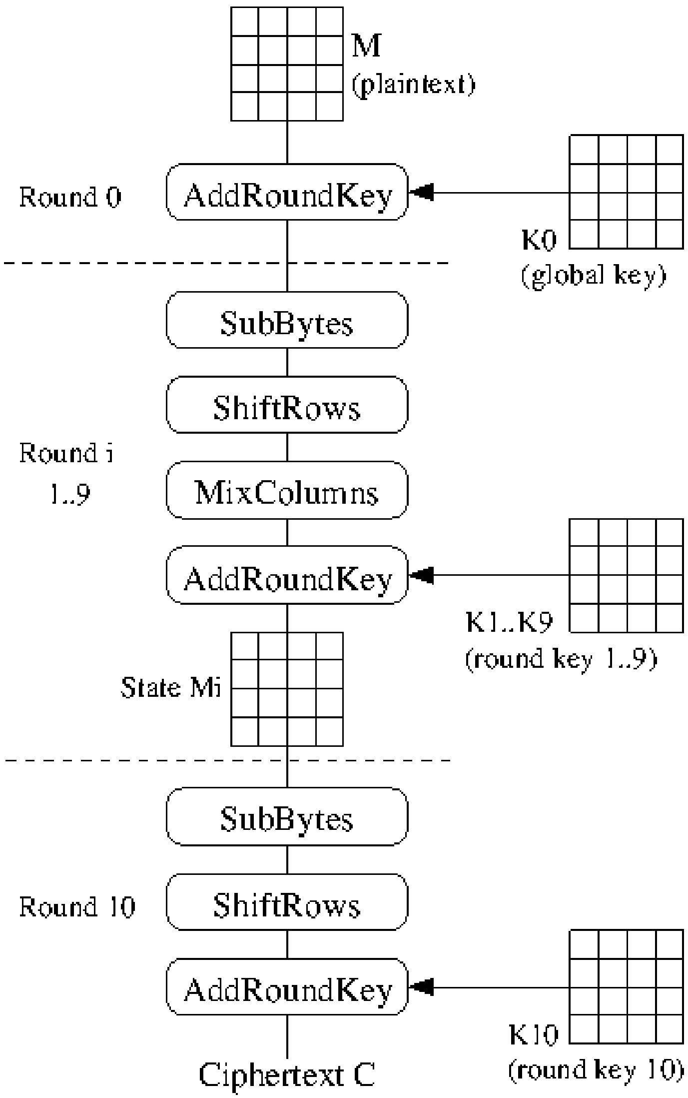




The hardened AES test chip

The AES algorithm

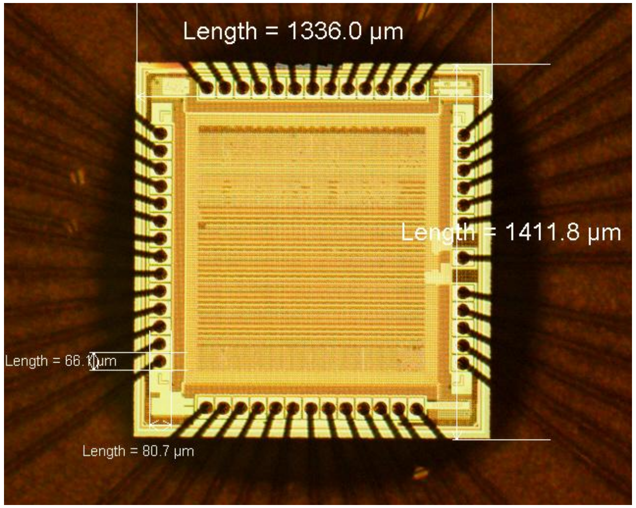
- Standard symmetric key algorithm (NIST).
- 4 Transformations used iteratively.
- 10 Rounds and 1 initial Round



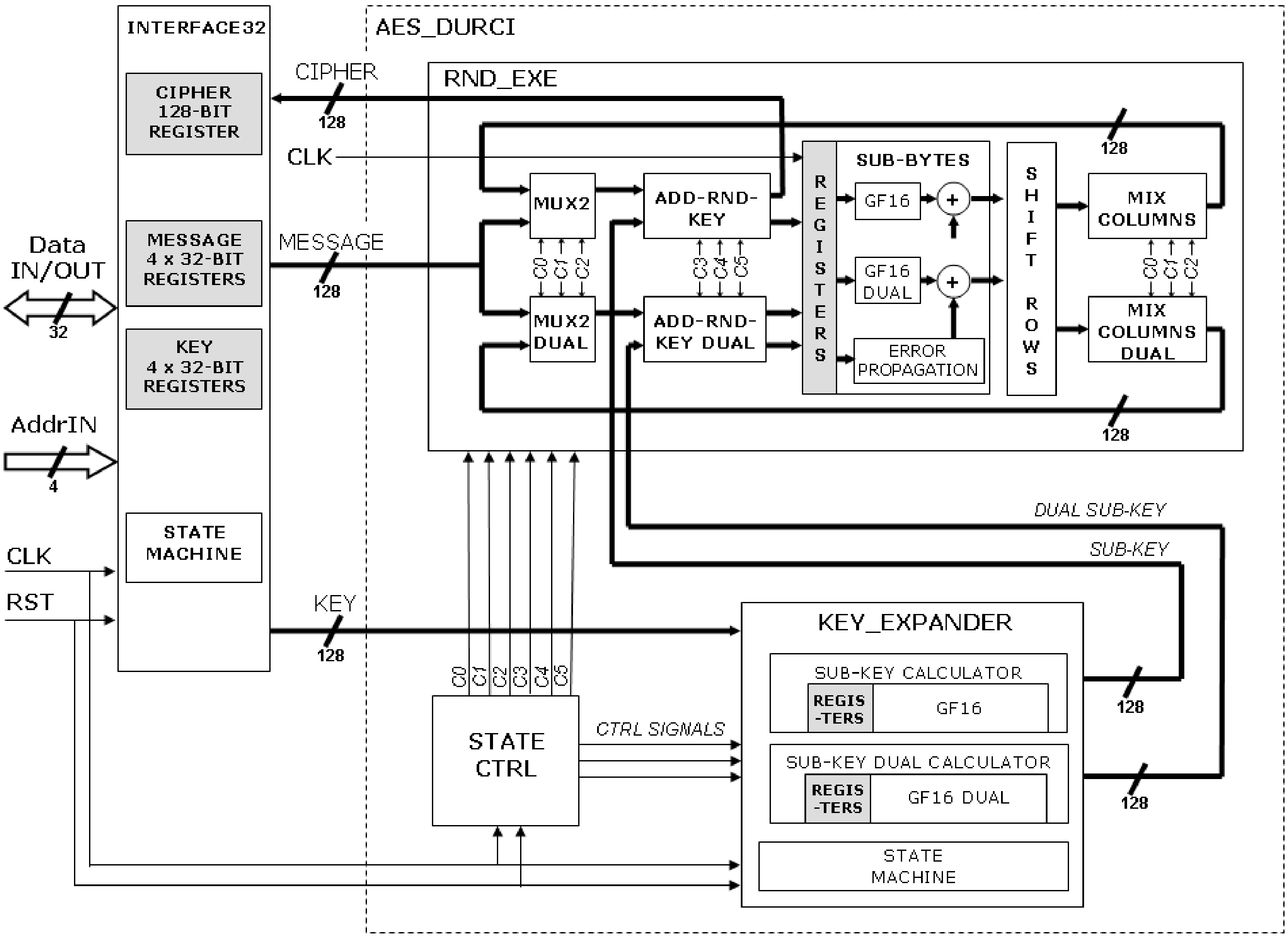
The hardened AES…

- ★ Chip designed with the HCMOS9gp 130nm STM technology

- ★ Die size: 1336µm x 1411.8µm



The ASIC AES

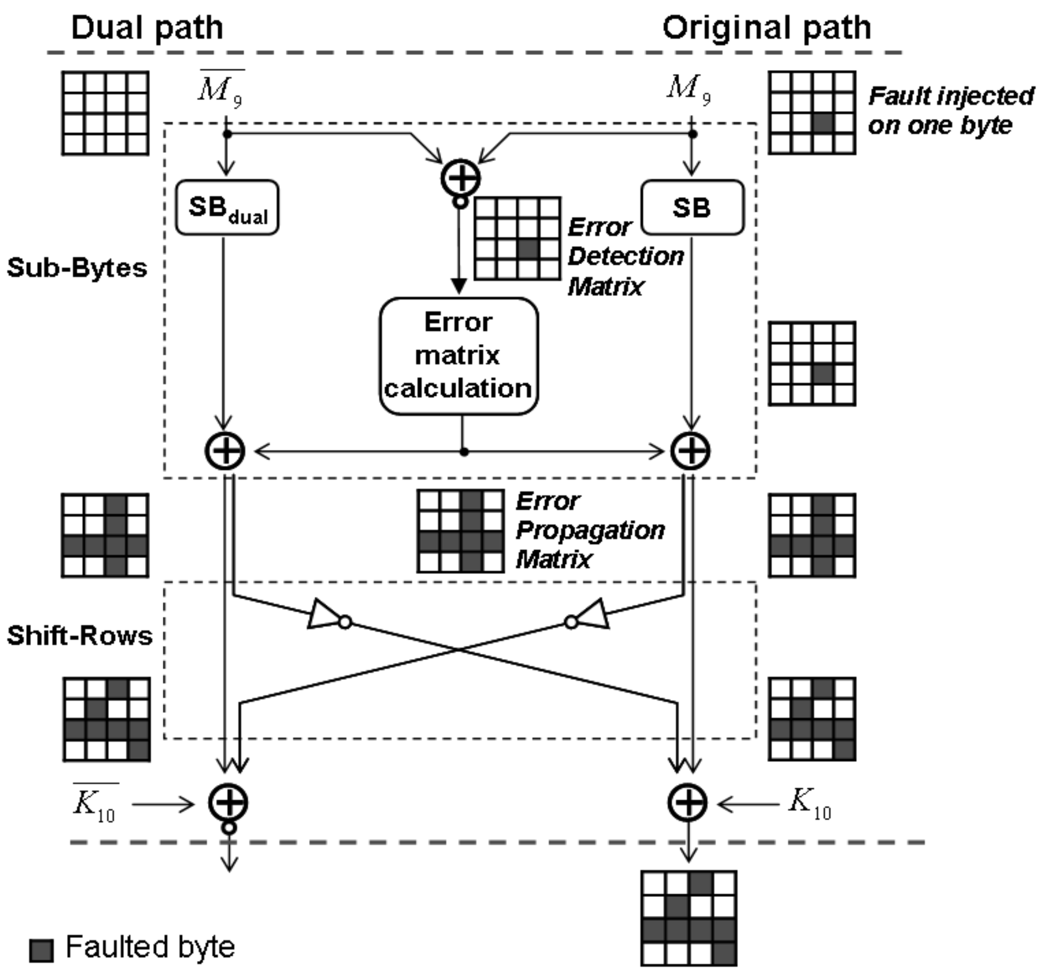

INTERFACE32
CIPHER 128-BIT REGISTER
MESSAGE 4 x 32-BIT REGISTERS
KEY 4 x 32-BIT REGISTERS
STATE MACHINE
Data IN/OUT
32
AddrIN
4
CLK
RST
AES_DURCI
CIPHER
128
CLK
MESSAGE
128
KEY
128
RND_EXE
MUX2
MUX2 DUAL
ADD-RND-KEY
ADD-RND-KEY DUAL
C0 C1 C2
C3 C4 C5
REGISTERS
SUB-BYTES
GF16
GF16 DUAL
ERROR PROPAGATION
SHIFT ROWS
MIX COLUMNS
MIX COLUMNS DUAL
C0 C1 C2
128
128
DUAL SUB-KEY
SUB-KEY
C0 C1 C2 C3 C4 C5
STATE CTRL
CTRL SIGNALS
KEY_EXPANDER
SUB-KEY CALCULATOR
REGIS -TERS
GF16
SUB-KEY DUAL CALCULATOR
REGIS -TERS
GF16 DUAL
STATE MACHINE
128
128

… its countermeasures

- Fault detection mechanism
  - Duplication of the data path
  - Error calculation and spreading
- The Cross-ShiftRows
  - ShiftRows operation crossed between the two paths.
  - For each byte: half of its bits are crossed with the other path.
  - Additional protection due to the loss of information

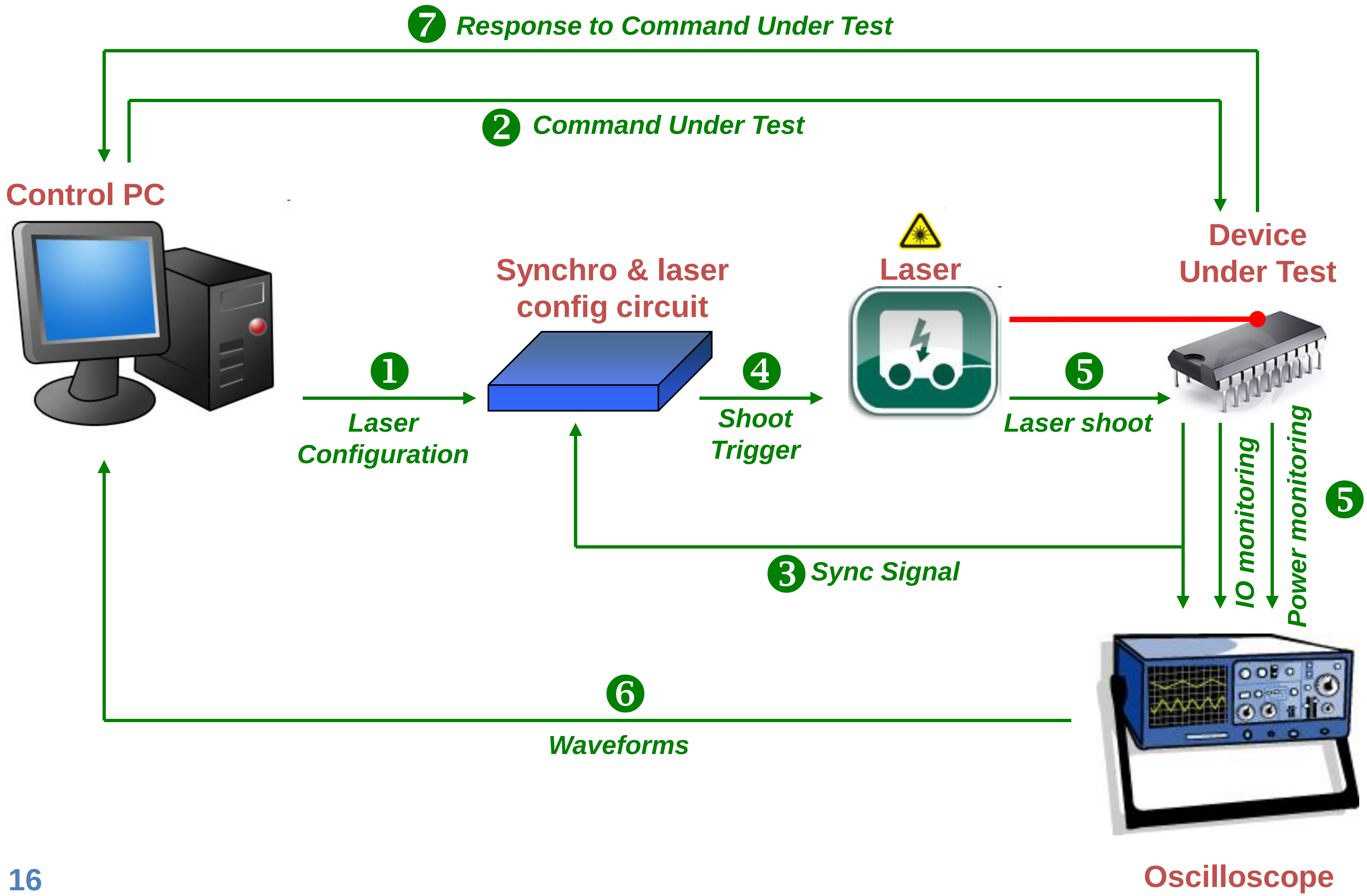
The countermeasures

- ★ Propagation of a fault on the last AES round

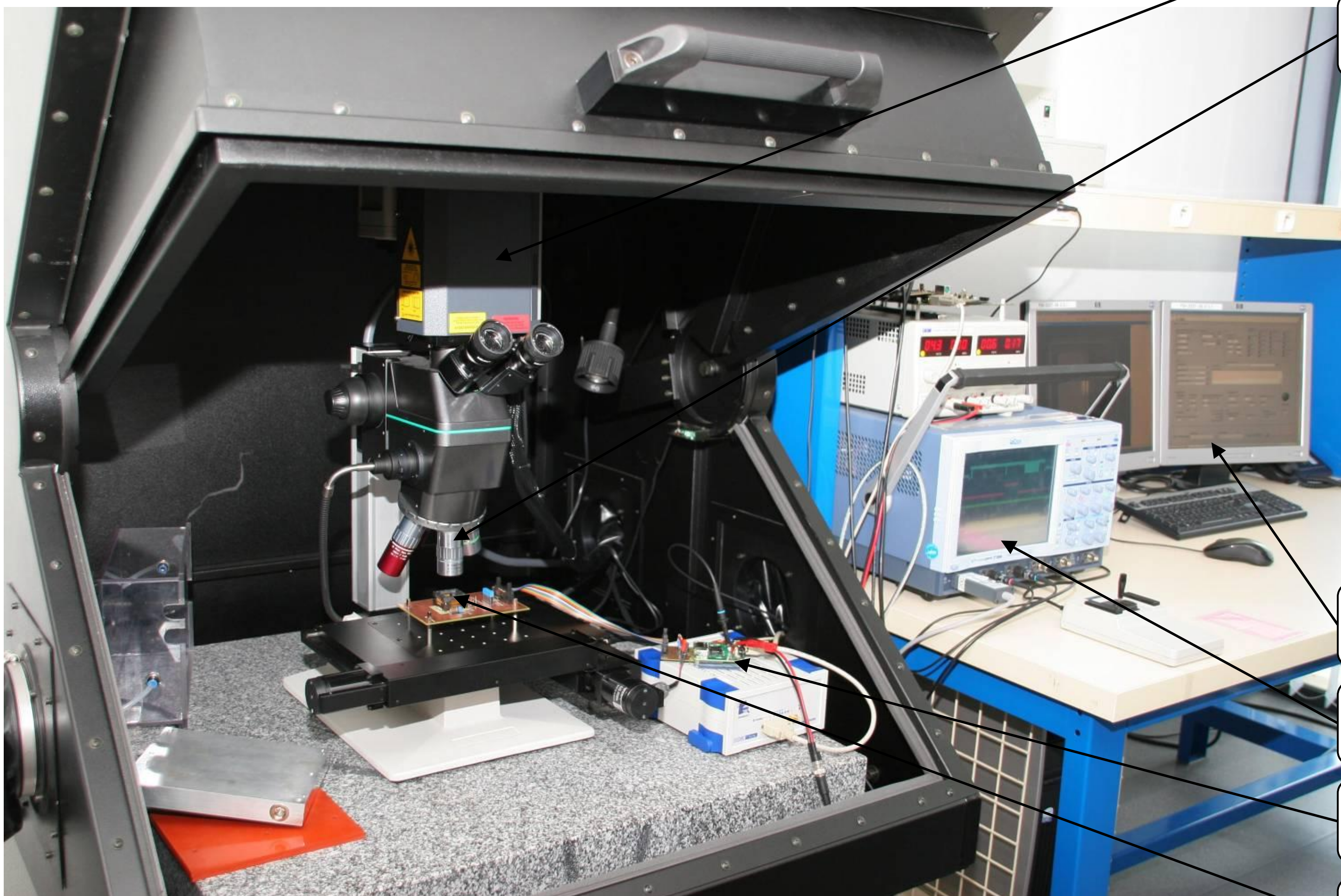


Fault Injection on the AES

Experimental set-up



The laser test bench



Fault injection on the datapath

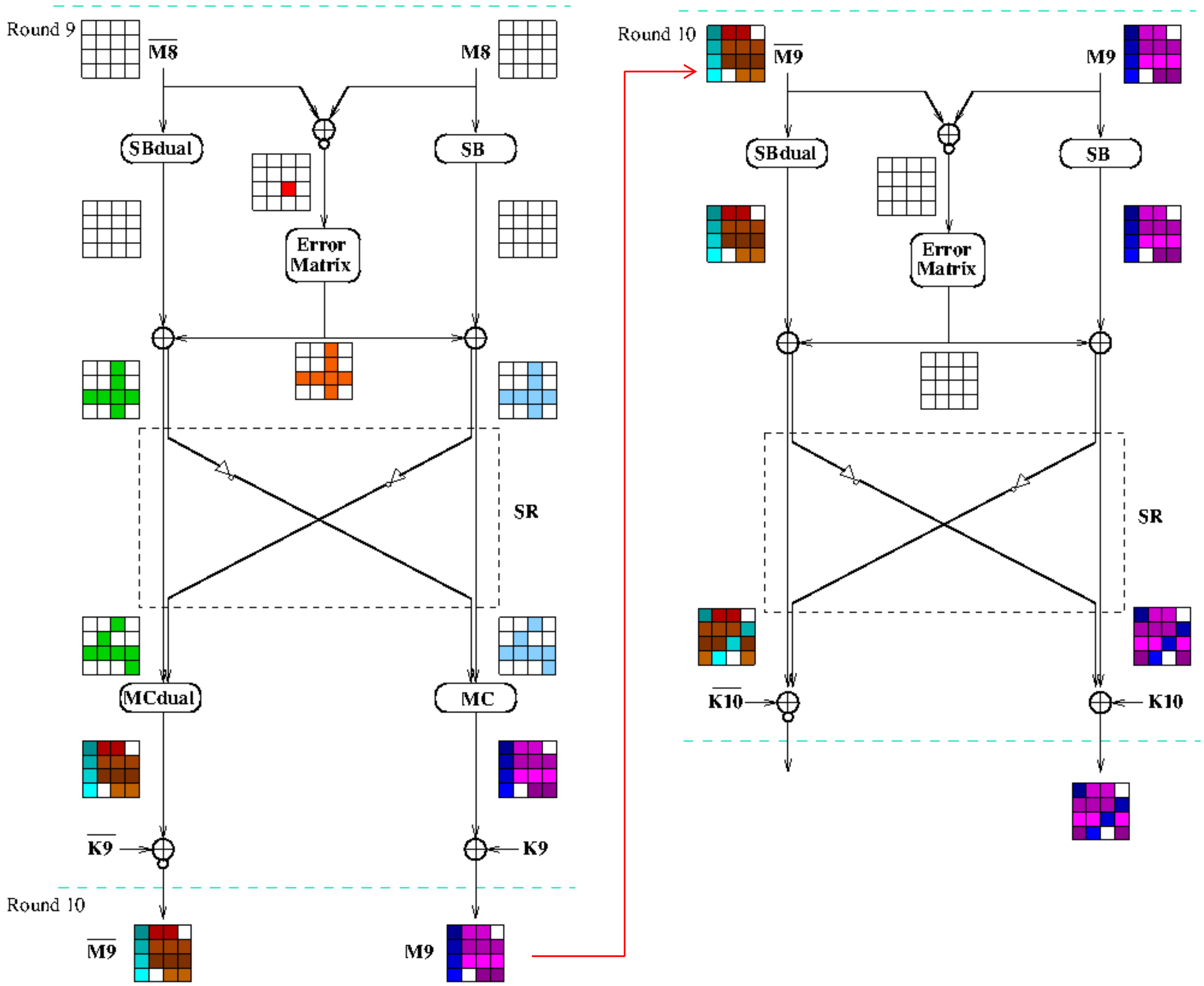
- Injection into the SubByte’s registers.
- Detection mechanism triggered.
- Application of the Giraud’s DFA.
  - Need to have a mono-bit error.
- The value of the error is known.
  - The faulty cipher text is blurring with the error value.
- Loss of information due to the Cross-ShiftRows

Fault injection on the detection mechanism

- How to neutralize the Cross-ShiftRows?
  - Inject the same fault on the two data path
  - Very hard due to the local effect of the laser

- Inject the fault on the detection mechanism
  - The mechanism spreads the fault on the two paths
  - The Cross-ShiftRows is neutralized
  - Injection on the Round 9
  - Application of another type of DFA on the Mixcolumns (Piret, 2003)

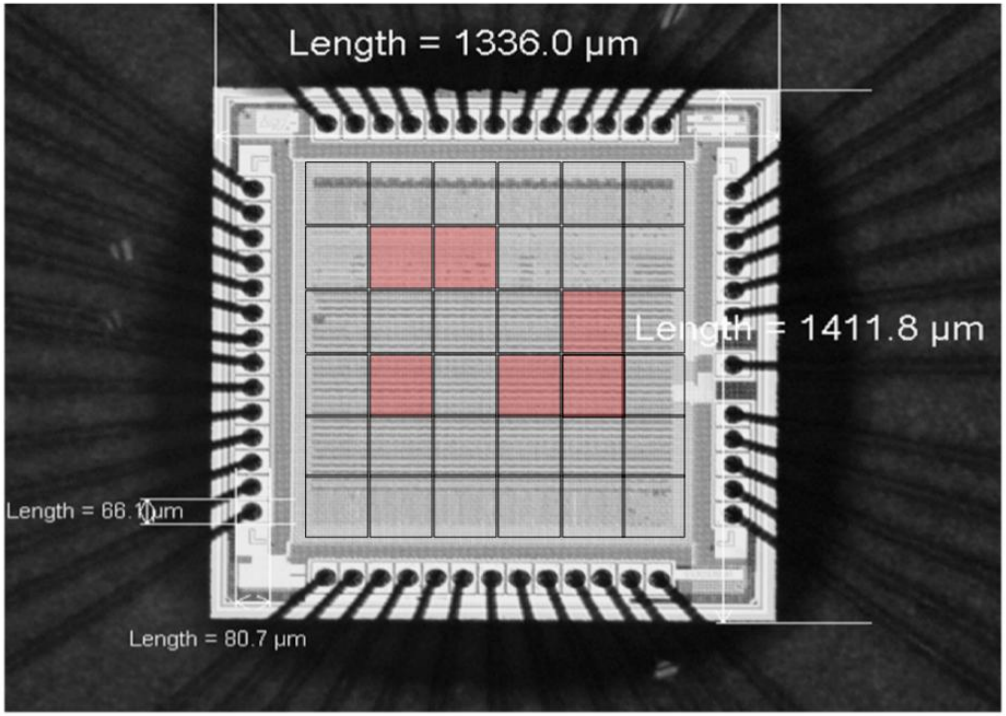
Injection on the detection mechanism



Results

Localization of the registers

- The registers are dispersed across the ASIC
- ASIC's surface split into 36 zones to made a cartography



Results (data path)

- For the first scheme of injection:
  - In “Black Box” approach
    - The error is spread by the countermeasures
    - Classical DFA inefficient
  - In “White Box” approach
    - 6 out of 16 bytes of the secret key were found.
    - Need the complete knowledge of the Cross-Shiftrows architecture.

Results (detection mechanism)

- Injection on the error matrix:
  - No significant results.
  - The error matrix isn’t implemented with registers.
  - Very hard to synchronize the laser bench and the encryption.
  - The injected fault are not latched by the next register.

Conclusions

- In “Black Box” => DFA inefficient
- In “White Box”
  - Few bytes of the key recovered
  - The error value spread should be a random
- Identification of a theoric weakness
  - Using the error matrix to inject faults
- Design rules for implementing secure encryption AES for the SDM

Thank You

Any questions?

And visit our demo stand to learn about other physical tests done (power, EM, clock glitch…) !!