Countermeasures against EM Analysis

Paolo Maistri[1], Sebastien Tiran[2], Amine Dehbaoui[3], Philippe Maurine[2], Jean-Max Dutertre[4]

(1) 

(2) 

(3) 

(4) 

Context

- Side channel analysis is a major threat against cryptographic implementations

Several leakage channels :
Time
Power
EM
…

Several analysis algorithms :
Simple
Differential
Higher-order Differential
Correlation
Behavioral
…

Several Countermeasures :
Random Masking
Dual-rail Implementations
Fake Computations (Noise)
Register Renaming
…

Outline

- Experimental Setup
- Encryption IPs
  - @ Montpellier : DES Jamming
  - @ Grenoble : AES Morph
  - @ Gardanne : AES Dual
  - Attacks and Results for each IP
- Perspectives

Experimental Setup

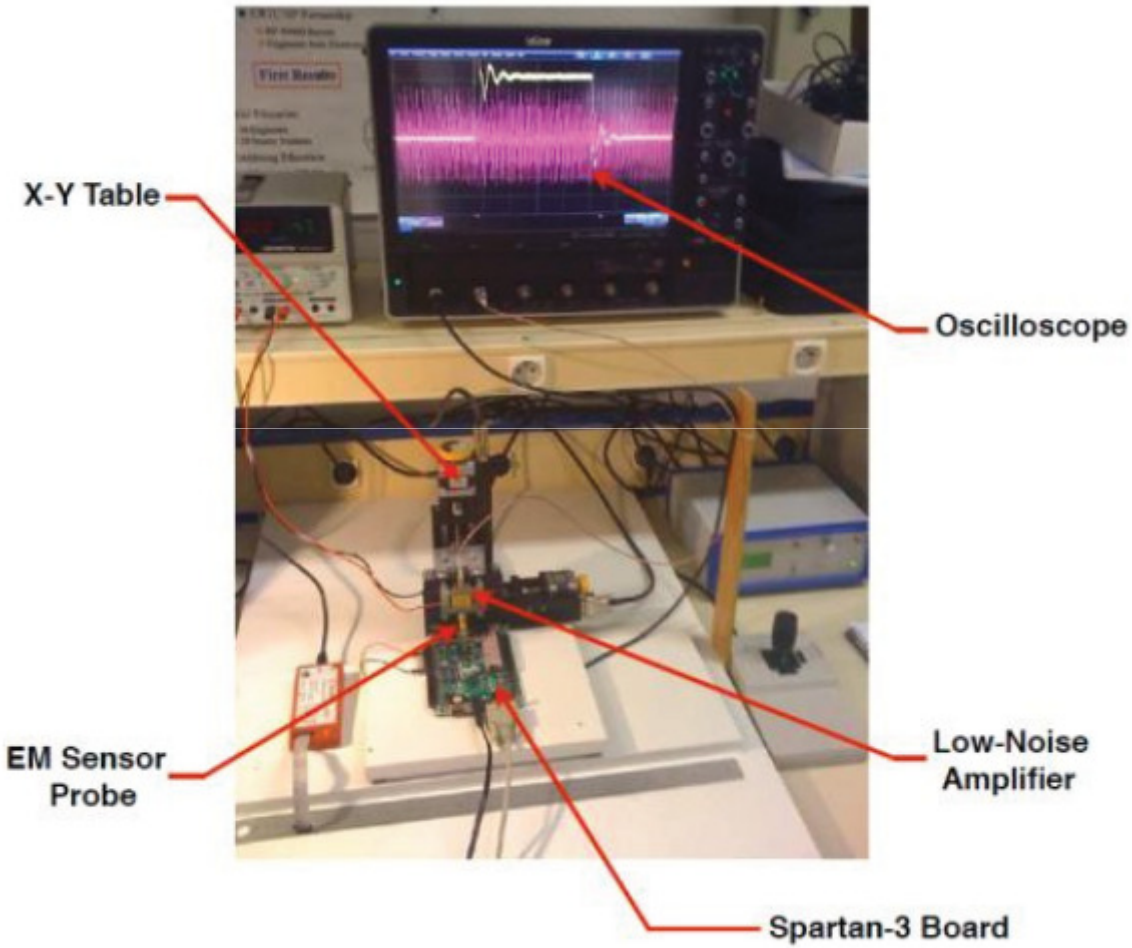
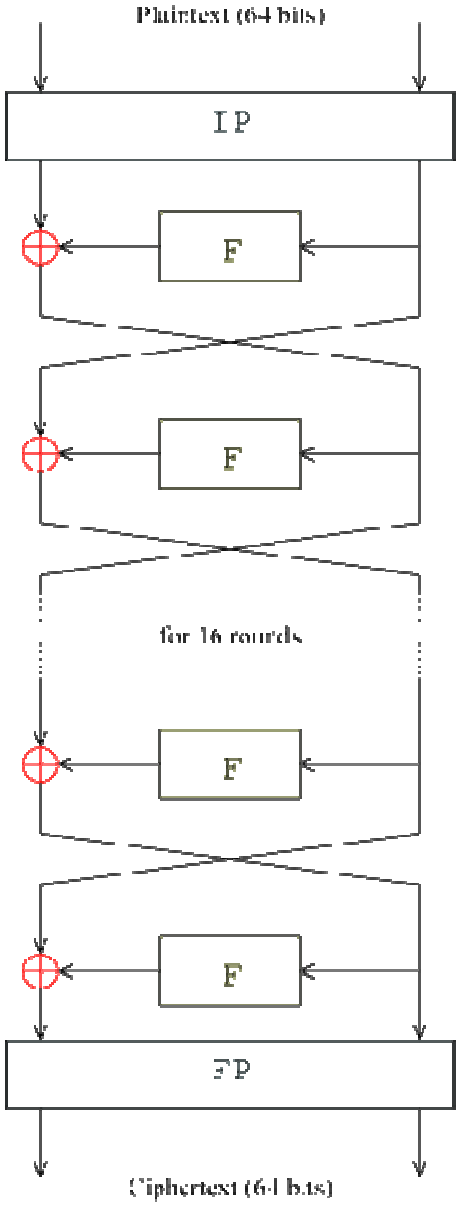


Figure 3. EM measurement platform

DES algorithm

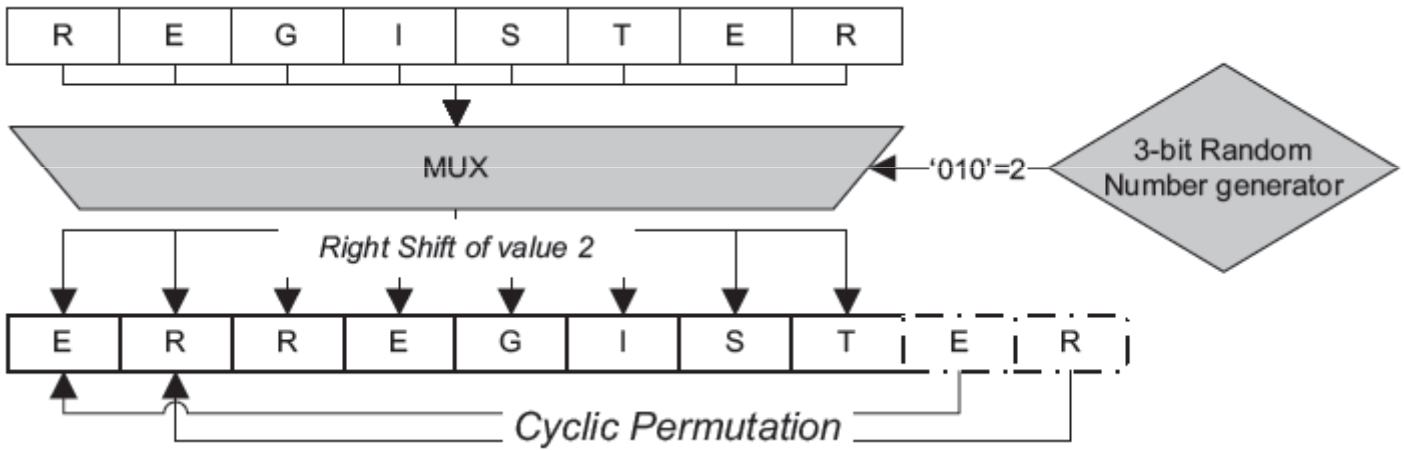
- Symmetric block cipher
  - Ptx 64b, Key 56b
- Feistel network
  - 16 rounds
- Round operations
  - Key Addition
  - Sbox
  - Permutation



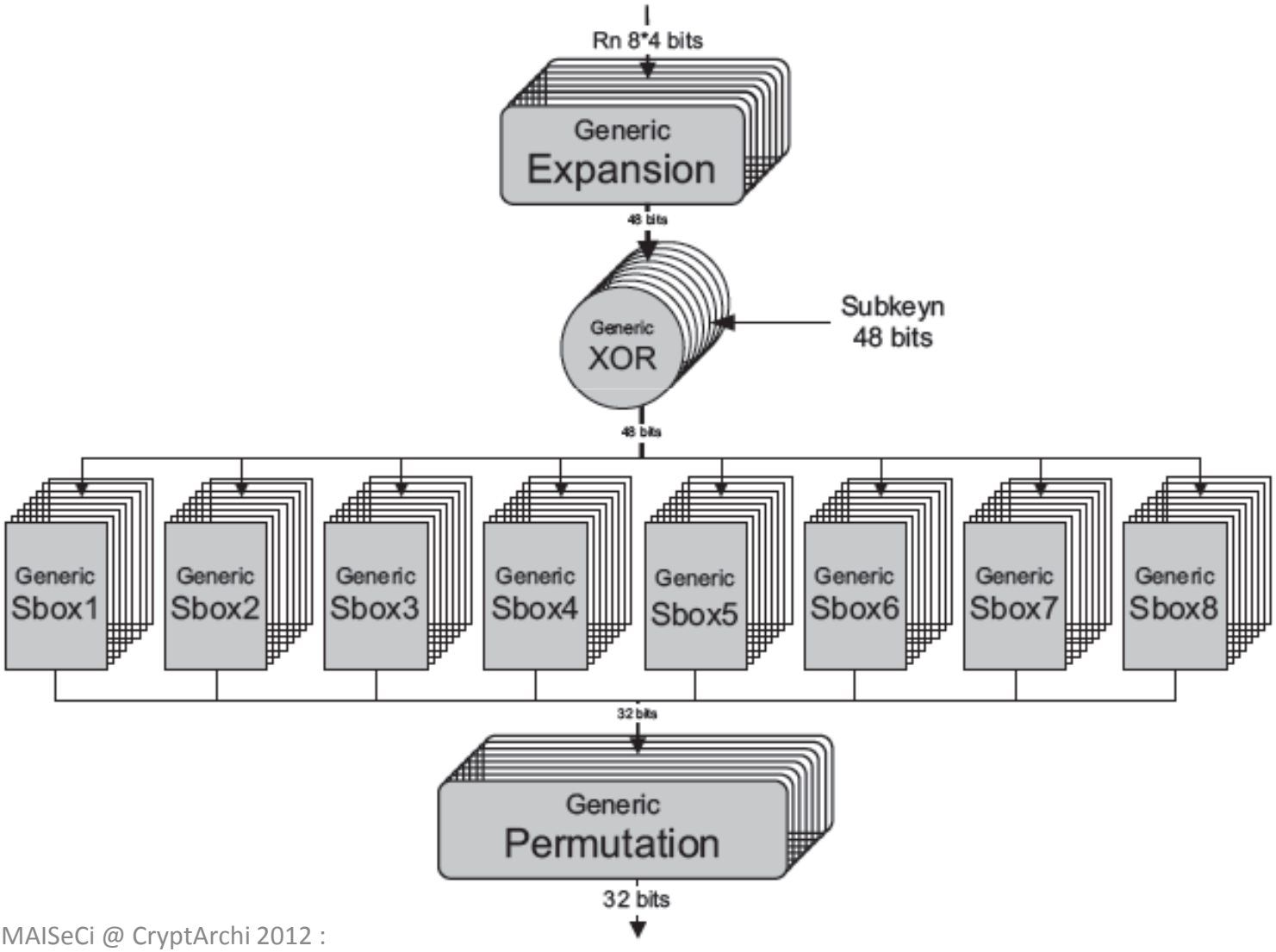
DES Jamming (1/3)

- What the countermeasure does
  - Resources randomly compute and store different values,
  - All parts are always activated
- What the countermeasure does not
  - Instantiate functional units for the sole purpose of computing random operations

DES Jamming (2/3)



DES Jamming (3/3)

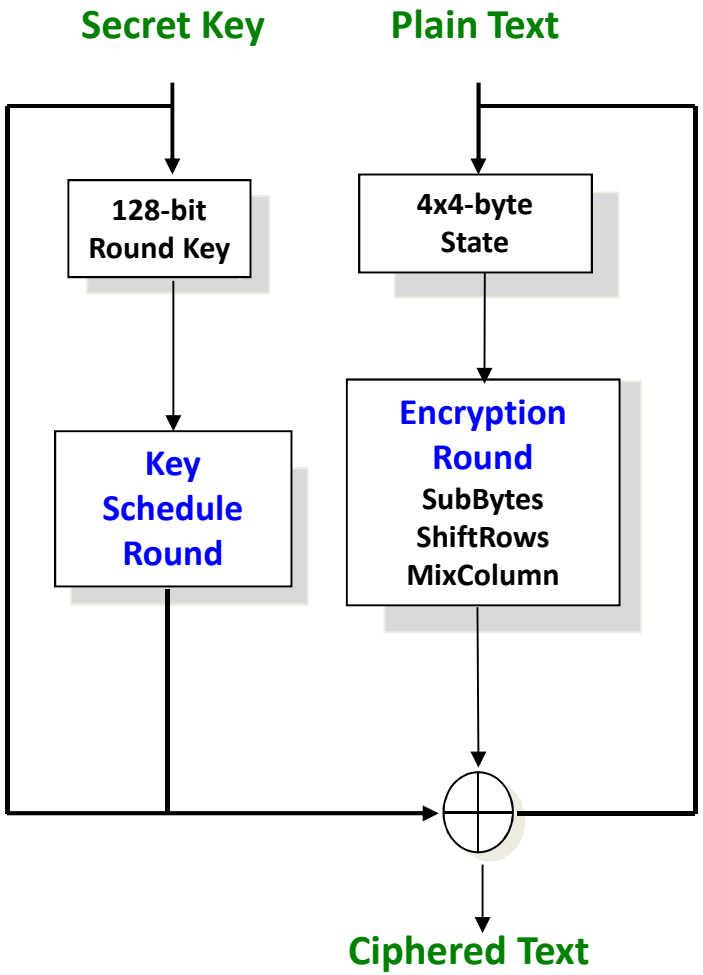


Attacking DES Jamming

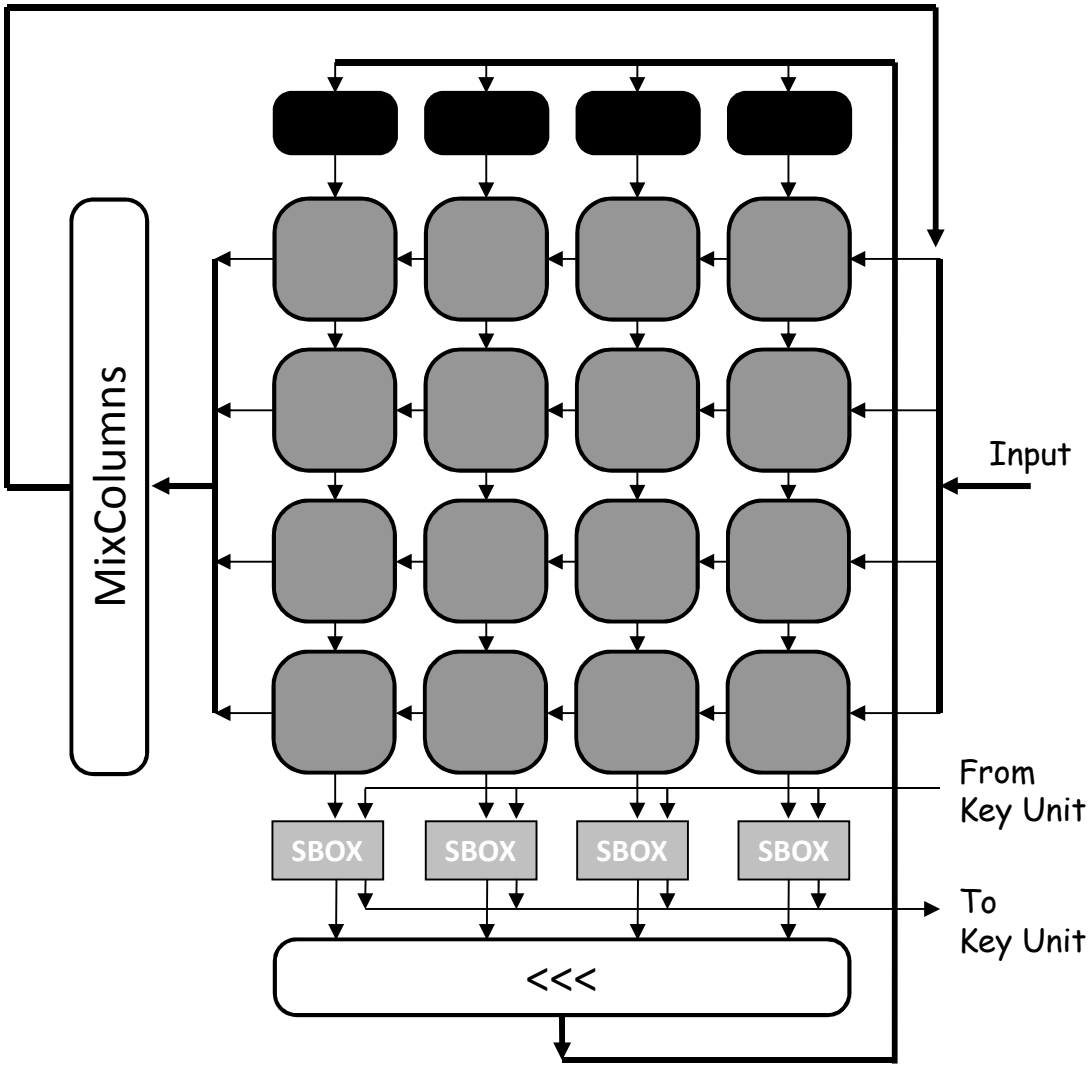
- Implementation :
  - Spartan 3 1000
  - Freq: 50 MHz (vs 108)
  - Slices: 1105 (vs 294, +276%)
- Attack: CPA-HW, SCAN
- Data set: 500k traces
- Results: only 7 sub-keys obtained
  - All sub-keys obtained after 200-600 traces w/o countermeasure

AES algorithm

- Symmetric block cipher
  - Ptx 128b,
  - Key 128/192/256b
- SPN cipher
  - 10/12/14 rounds
- Round operations
  - SubBytes
  - ShiftRows
  - MixColumns
  - Key Addition



AES Morph (1/3)



- Quite small
- 32-bit data-path
- 4 Substitution Boxes
- 4 GF Multipliers for *MixColumns*
- 10 clock cycles per round
- On-the-fly key unrolling (using shared *S-Boxes*)

AddRoundKey and State

2-stage S-Box

Register layer

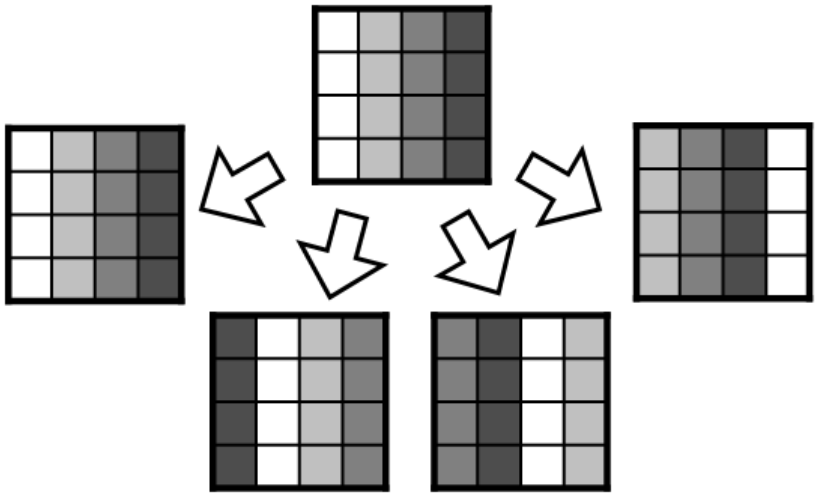
Combinatorial logic

8-bit signal

32-bit signal

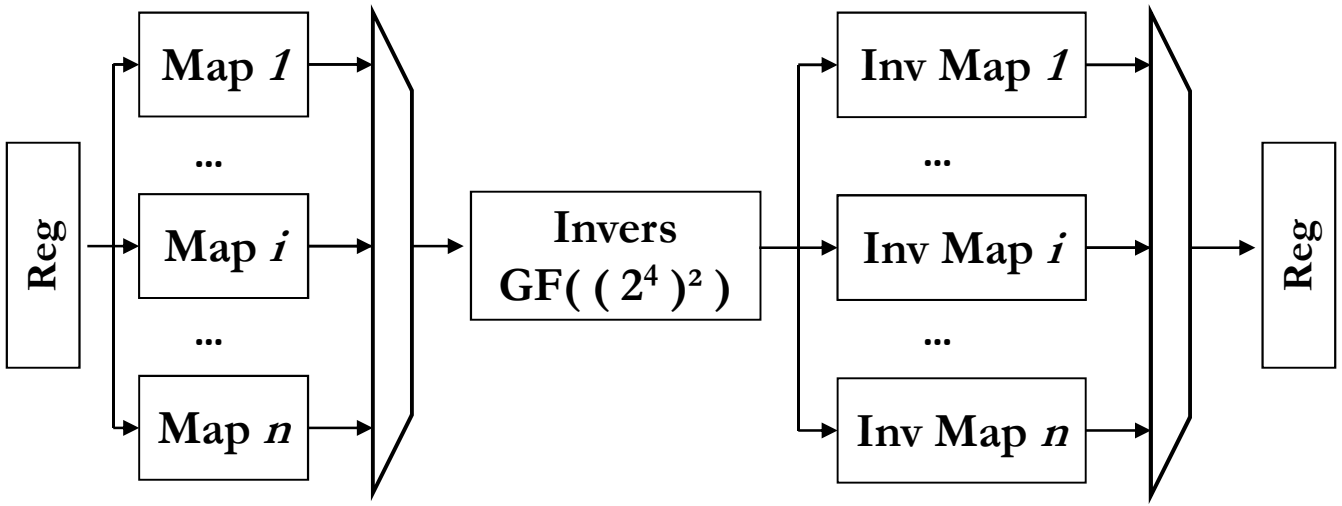
AES Morph (2/3)

- Dynamic resource allocation done intra-round
- Column relocation
  - Several external constraints (*MixColumns*, *ShiftRows*, …)
  - Only 4 different configurations



AES Morph (3/3)

- For each S-Box, implement several parallel mappings
  - From 1 to 8 possible dynamic mappings
  - Choose randomly at runtime
  - At the output, choose the correct inverse mapping to get back the result
- Limited to S-Box data path
- Independence ?

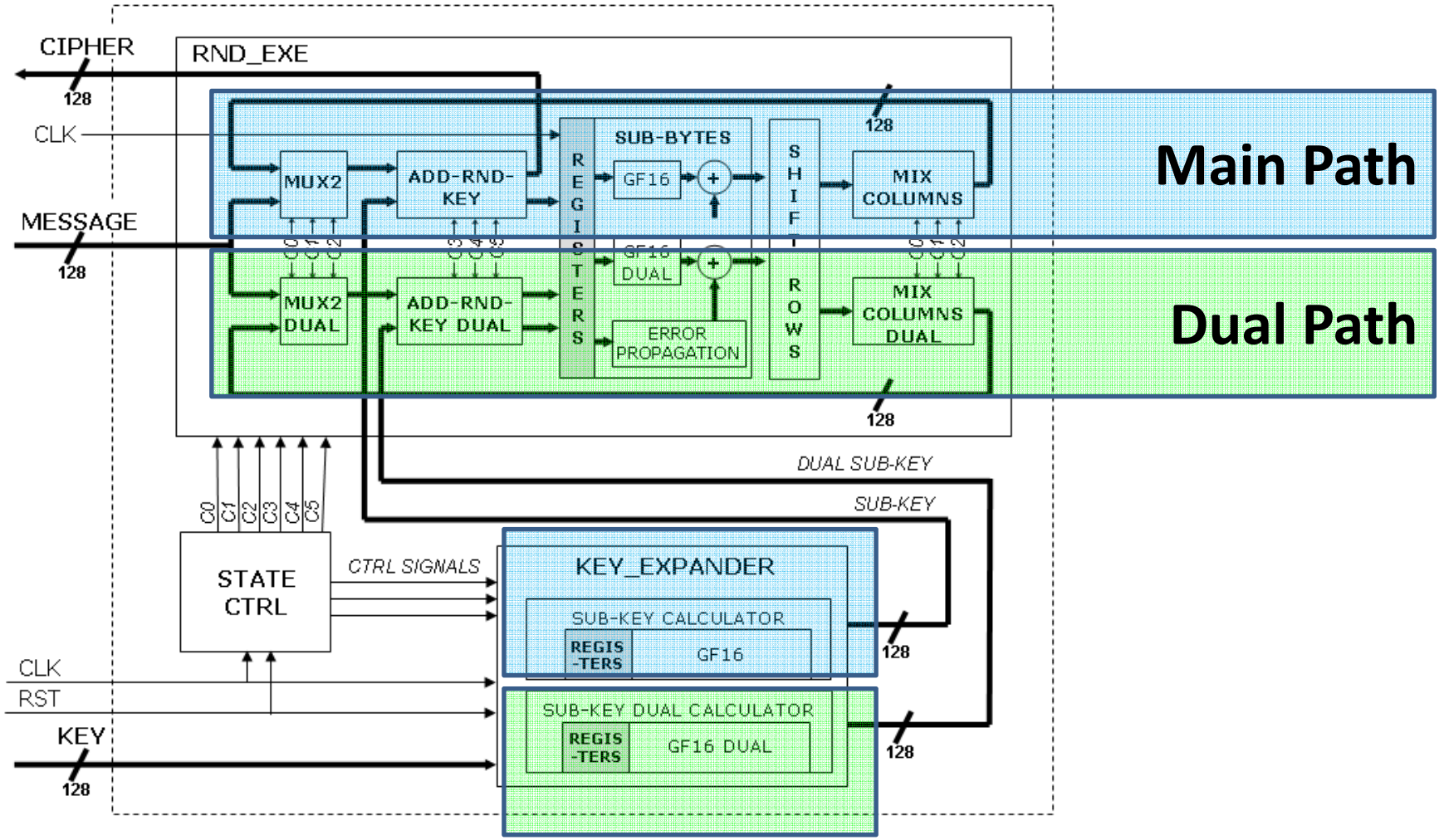


Attacking AES Morph

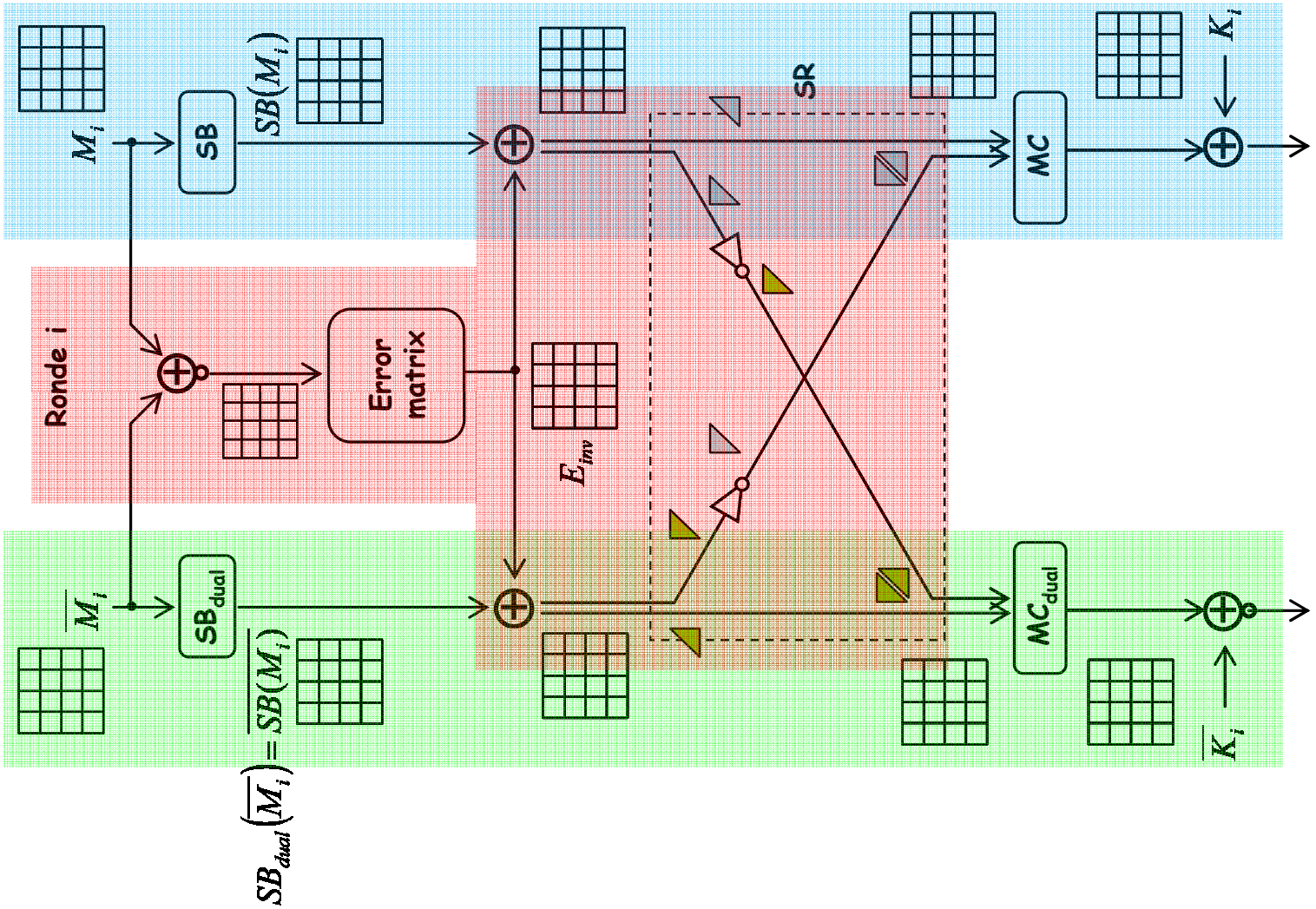
- Implementation :
  - Spartan 3 1000
  - Freq: 50 MHz
  - Slices: 1445 (vs 1199, +20%)
- Attack: CPA-HW
- Data set: 200k traces
- Results:

No countermeasures vs CPA	Countermeasures vs CPA	Countermeasures vs SCAN
~21k traces	~80k traces	~60k traces

AES Dual (1/2)

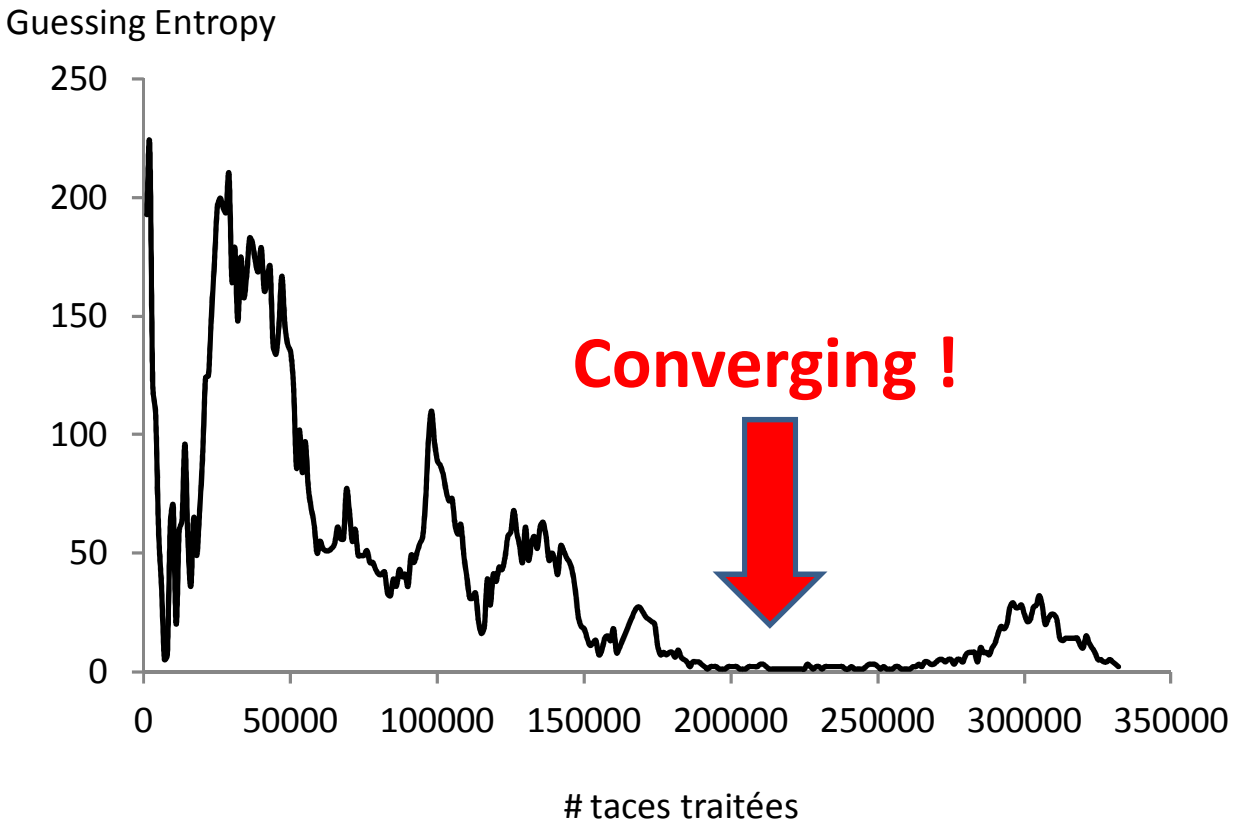

CIPHER
128
RND_EXE
CLK
MESSAGE
128
MUX2
ADD-RND-KEY
REGISTERS
SUB-BYTES
GF16
SHIFT ROWS
MIX COLUMNS
128
Main Path
MUX2 DUAL
ADD-RND-KEY DUAL
GF16 DUAL
ERROR PROPAGATION
MIX COLUMNS DUAL
128
Dual Path
DUAL SUB-KEY
SUB-KEY
C0
C1
C2
C3
C4
C5
STATE CTRL
CTRL SIGNALS
KEY_EXPANDER
SUB-KEY CALCULATOR
REGIS-TERS
GF16
128
CLK
RST
KEY
128
SUB-KEY DUAL CALCULATOR
REGIS-TERS
GF16 DUAL
128

AES Dual (2/2)


M_i
SB
$SB(M_i)$
SR
MC
K_i
Ronde i
Error matrix
E_{inv}
$\overline{M_i}$
SB_{dual}
$\overline{SB(M_i)}$
MC_{dual}
$\overline{K_i}$
$SB_{dual}(\overline{M_i}) = \overline{SB(M_i)}$

Attacking AES Dual

- Implementation:
  - ST 130 nm
  - 50 MHz
  - 1.2 V
- Attack:
  - CPA
- Data set:
  - 332k traces



Conclusions

- DES Jamming
  - Too few configurations, too little entropy
- AES Morph
  - Too few configurations, too little entropy
  - Dynamic mapping useless (due to other leakage)
- AES Dual
  - Quite strong !

Perspectives

- AES Morph
  - Increase number of configurations (intra-round + inter-round)
  - Mapping under new analysis

- **Next**:
  - EM fault attacks and countermeasures!