INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Ecole Nationale Supérieure des Mines SAINT-ETIENNE

www.emse.fr

HOST 2013

Frontside Laser Fault Injection on Cryptosystems -Application to the AES's last round-

Cyril Roscian, Jean-Max Dutertre and Assia Tria

Secured Architecture and System Laboratory – Centre Microélectronique de Provence - Gardanne

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

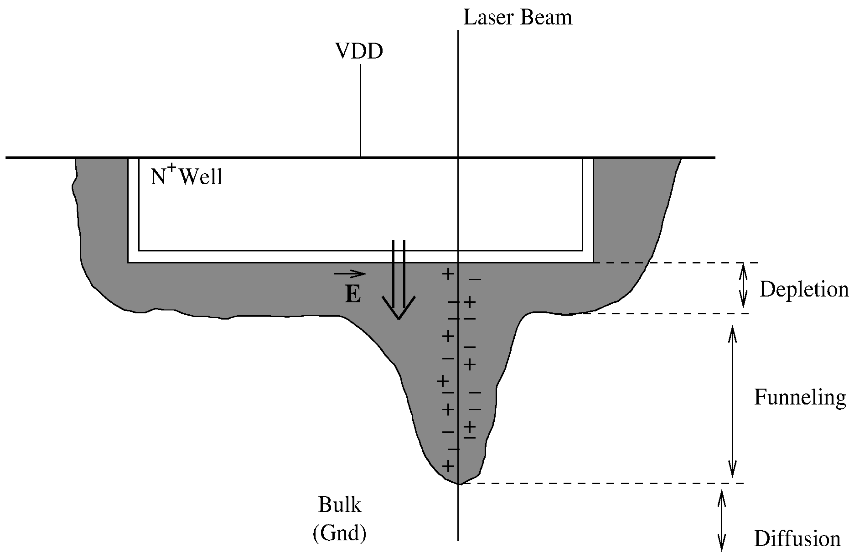
MINES TELECOM
INSTITUT Mines-Télécom

Planning

- **Introduction**
  - Laser effect on ICs
  - Sensitivity zones
  - Fault injection mechanism
- **Experimental Setup**
- **Analysis of fault injection**
- **Performing DFA on experimental data**
  - Giraud’s DFA
  - Roche et al. DFA
  - Simplification of existing DFA
- **Conclusion**

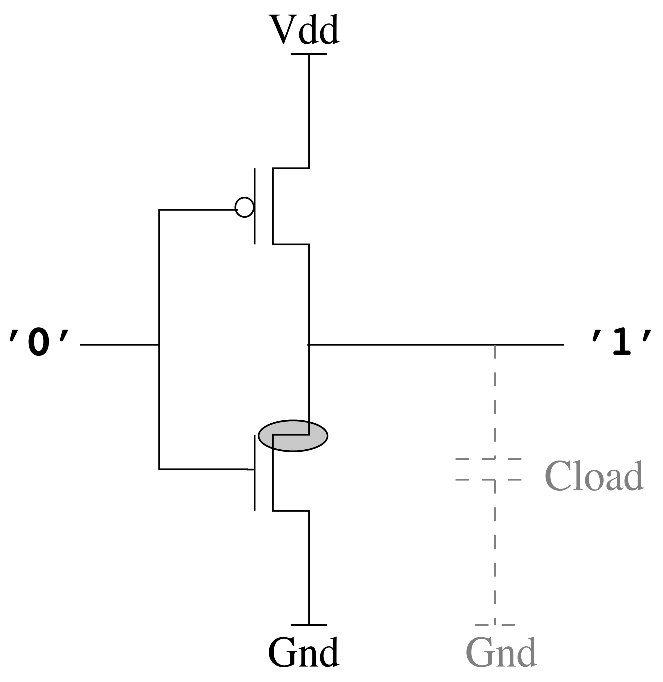
Laser effect on ICs

- Creation of electron-hole pair along the laser beam due to the photoelectric effect
- Stretch the electric field
- Creation of a transient current
- Possible SEE on PN junction
  - Source and drain of transistors



Sensitivity zones

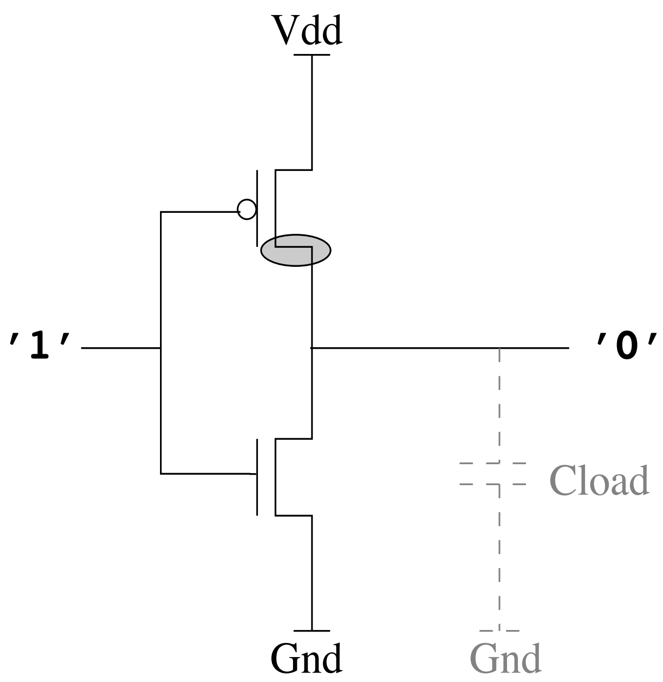
- Inverter's case:
  - 1st Case (output = '1')
    - PMOS ON
    - NMOS OFF
    - Only a strike on drain of NMOS will discharge the load and change the output state



The sensitivity zone is the drain of the OFF NMOS transistors

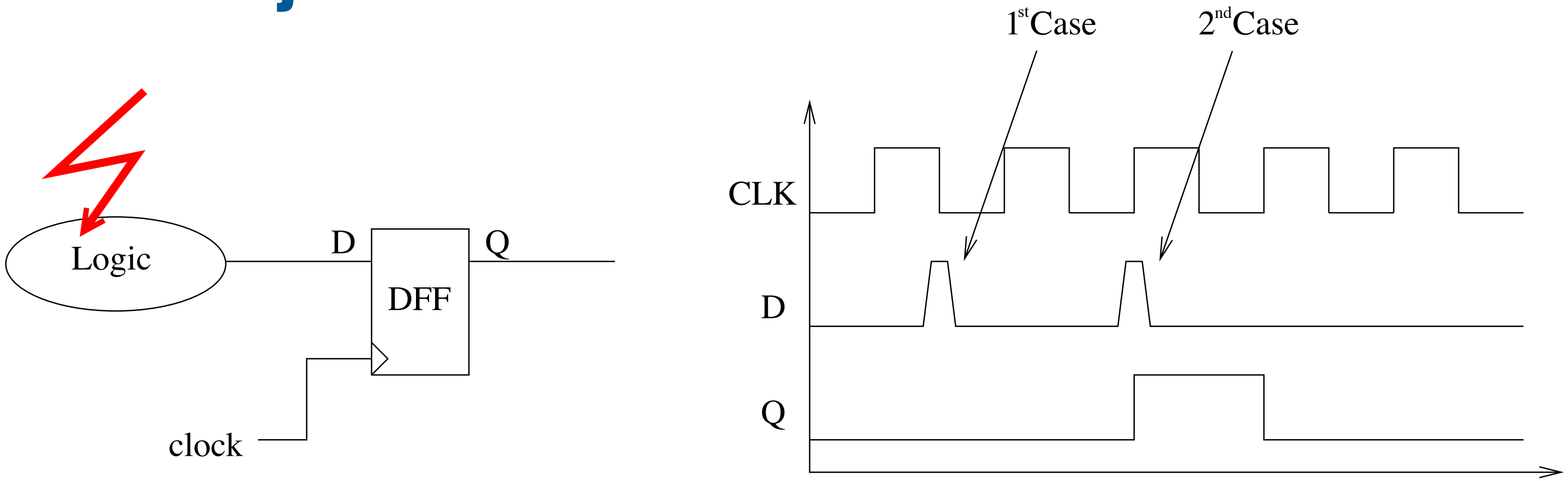
Sensitivity zones

- Inverter's case:
  - 2st Case (output = '0')
    - PMOS OFF
    - NMOS ON
    - Only a strike on drain of PMOS will charge the load and change the output state



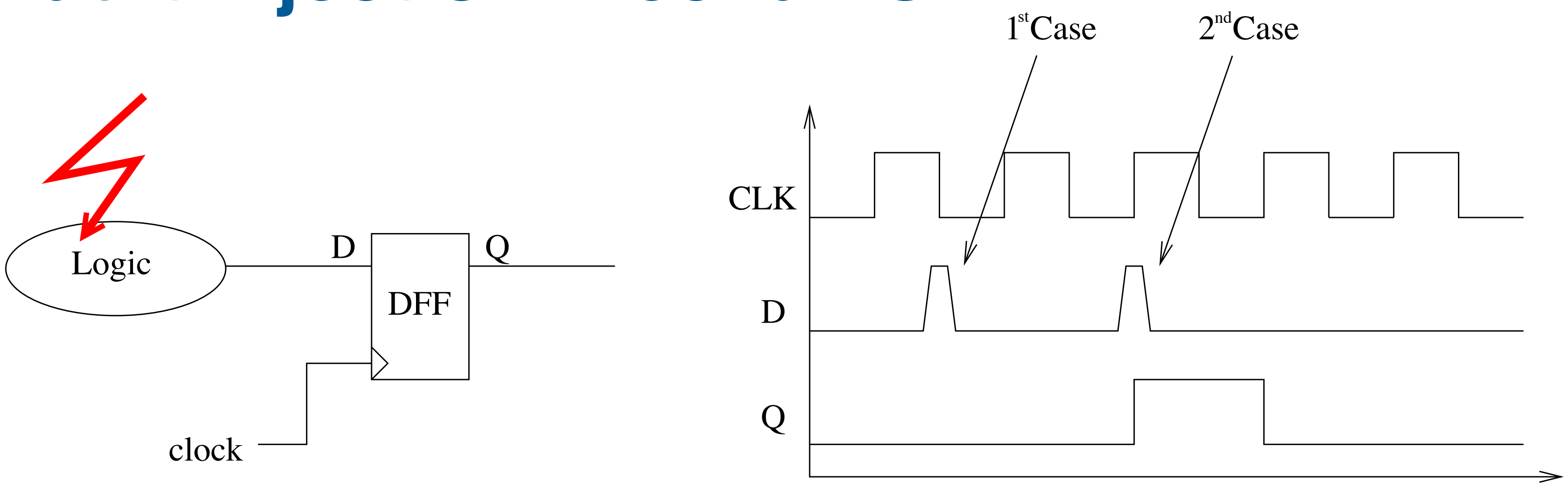
The sensitivity zone is the drain of the OFF PMOS transistors

Fault injection mechanism



- SET reaches the DFF's input outside the latching window
  - No effect on the DFF's output
  - No fault on the computational results

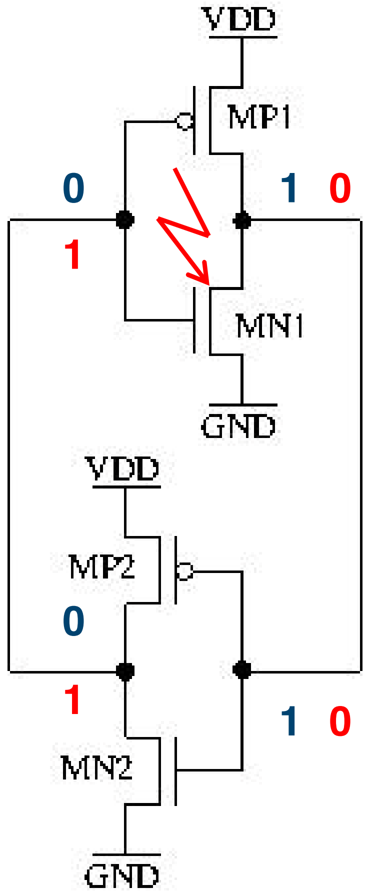
Fault injection mechanism



- SET reaches the DFF's input inside the latching window
  - DFF's output is changed
  - A fault occured on the computational results

Fault injection mechanism

- SET reaches the DFF itself or an SRAM
  - Memory constructed with cross-coupled inverter
  - The SET will propagate through the inverters
  - The memorized data is inverted
  - **A fault is injected**



Laser Fault model

- Laser spot strike one sensitive area
  - Fault data-dependent
  - Bit-Set/Bit-Reset fault model
  - Allow to mount safe error attacks
- Questionable with advanced CMOS IC
  - Smallest laser spot of 1μm
  - Several transistors reaches by the spot
  - Impact of metal layers

Laser Fault model

- Possible Bit-flip
- Most of injection on rear side with small spot
  - Time consuming
  - Chip preparation
- Front side
  - Easy
  - But not consistent with bit-set/reset

- **Investigation of fault type in front side with large spot**

Laser test bench

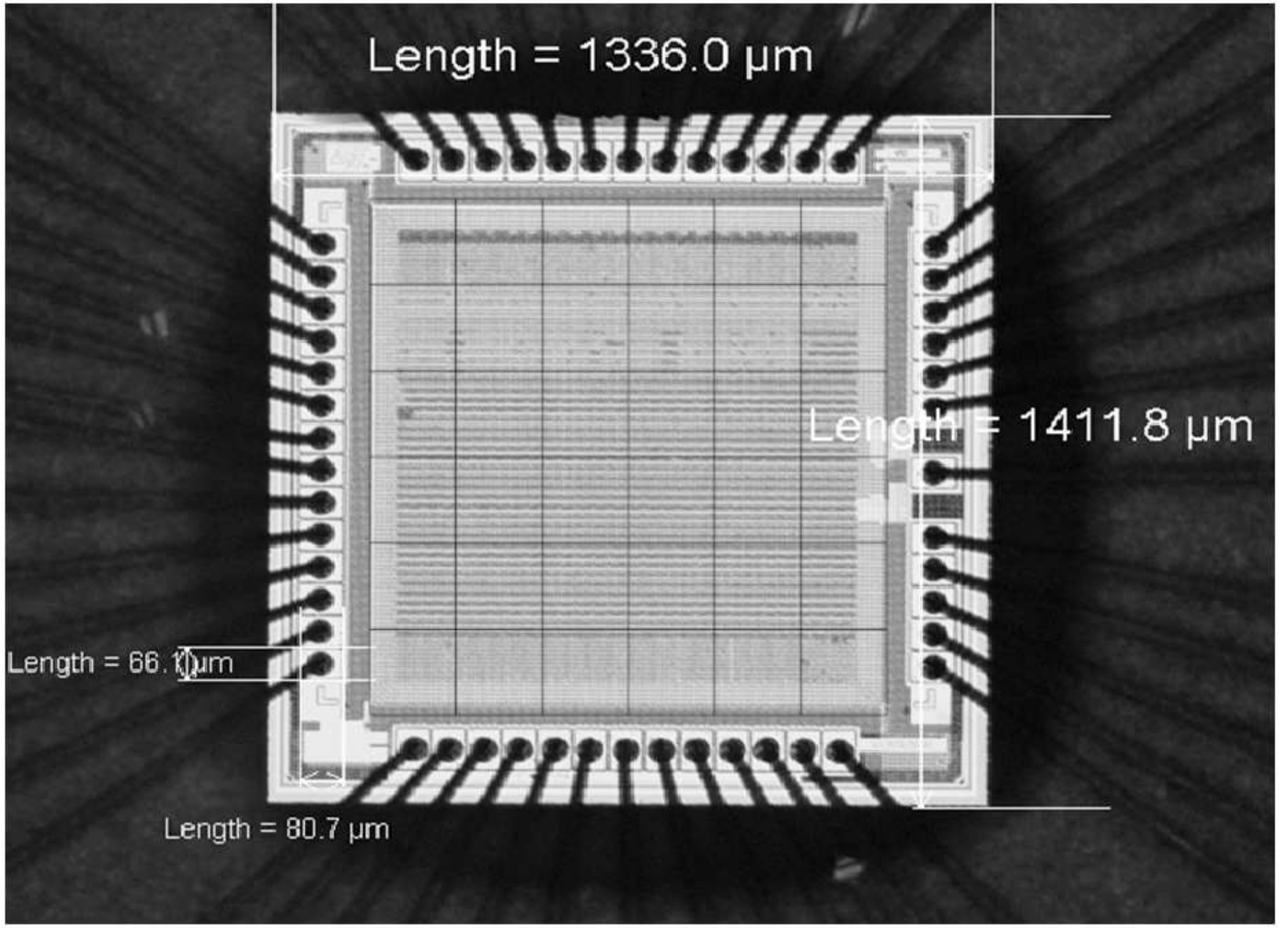
- Front side fault injection
- Wavelength of 532nm
- Laser pulse of 5ns
- Square laser spot of 125µmx125µm
- Energy density of 17pJ/µm²
- Laser shoot syncronized with *AES* encryption
  - Jitter of 5ns
  - Laser shoot during the last round of the AES

Target device

•

•

•



Fault injection on *AES*' last round

- Surface of the chip divided on 36 positions
- 10,000 encryptions for each position
- Same key used for all encryption

- Comparison between faulted and correct cipher text
- Fault value recovered by reversing the faulted encryption(the key was known)

Results

Fault injection on *AES*' last round

byte #	Error injection rate	Single-bit error rate	Most common fault rate
0	4.8%	79%	74%
1	3.2%	100%	99%
2	3.1%	98%	92%
3	67.8%	49%	48%
4	9.4%	99.7%	90%
5	2.1%	79%	58%
6	0.5%	100%	99%
7	4.6%	65%	64%
8	23%	64%	42%
9	7.2%	91%	80%
10	4.3%	99%	98%
11	15.,5%	97%	97%
12	12.2%	98%	96%
13	3.1%	87%	55%
14	0.2%	100%	100%
15	7%	99.2%	99%

Results

Fault injection on *AES*' last round

byte #	Error injection rate	Single-bit error rate	Most common fault rate
0	4.8%	79%	74%
1	3.2%	100%	99%
2	3.1%	98%	92%
3	67.8%	49%	48%
4	9.4%	99.7%	90%
5	2.1%	79%	58%
6	0.5%	100%	99%
7	4.6%	65%	64%
8	23%	64%	42%
9	7.2%	91%	80%
10	4.3%	99%	98%
11	15.5%	97%	97%
12	12		96%
13	3.		55%
14	0.		100%
15	7		99%

- Low Injection rate
- High repetitively rate

Fault injection on *AES*' last round

- 1,000 encryption on byte #5

Faults occurrence rate	Occurrence rate of fault '0x80'	Occurrence rate of other faults
7.1%	94%	6%

- Single bit fault of 0x80
- Faulted bit : "0" ➡ "1"
- Bit-Set fault type
- If only Bit-Set fault is considered
  - From 7.4% to 14.2% occurrence rate

Fault injection on *AES*' last round

- 1,000 encryption on byte #5 with chosen plain text

Faults occurrence rate	Occurrence rate of fault '0x80'	Occurrence rate of other faults
16.8%	97%	3%

- Timing constraint
  - Clock period of 40 ns
  - Jitter of 5 ns
- **Bit-set fault model relevant**

Fault injection on *AES*' last round

- Analysis on byte #3
  - 34.2% fault occurrence on bit N° 2
  - 66% fault occurrence on bit N° 1
  - Bit N° 2 only impacted by Bit-Set fault type
  - Bit N° 1 impacted by Bit-flip fault type

Fault value $b_7 \ldots b_4\ b_3 b_2 b_1 b_0$	# of occurrence
0000 0110	3285
0000 0010	3228
0000 1110	93
0000 1000	70
0000 0100	51
0000 0001	40
0000 1001	13
0000 0011	4

- **Some faulted bits are data-dependant**

Fault injection on *AES*' last round

- Bit-set/reset and Bit-flip fault model are relevant with large spot size and front side laser fault injection
- Metal fills act as shutter on laser beam
  - Hides some sensitive area
- Low injection rate but high repetitively of fault value
  - Comparison of two DFA schemes with these data

Giraud's mono-bit

- Need a single bit fault injection on byte before the last round of the AES
- Success rate of 97% with 3 pairs of Correct/Faulted cipher text
- Only 3 bytes correspond with this statement
  - Bytes 1,6 and 14
- 13 bytes are mono-bit occurrence close to 80%
  - Correct/Faulted cipher text needed increases
- 3 bytes close to 65% or above 50%
  - Not the most efficient schemes

DFA Results

Roche et al. DFA

- Need constant fault injection
- 3 pairs of Correct/Faulted cipher texts to have a succes rate of 90%
- With our data:
  - 9 bytes need 6 or less pairs
  - 4 byte need at least 15 pairs
- More data needed to succeed compared to Giraud
- Fault model less constraining

Simplification of an existing DFA

- Byte-wise analysis of the error injected
- Equation of the AES's last round for the correct and faulted ciphertext:

$$C = K10 \oplus SB(M9)$$
$$D = SB(M9 \oplus e) \oplus K10$$

- The equation of the error is:

$$e = SB^{-1}(C \oplus K10) \oplus SB^{-1}(D \oplus K10)$$

- For each pairs:
  - Computation of *e* for all possible *K10*
  - Construction of an error table

Simplification of an existing DFA

- E
- E ... ct and f

Realization i	K10 hypothesis k				
	'0x00'	'0x01	'0x02'	$\cdots$	'0xFF'
0	$e_{0,0}$	$e_{0,1}$	$e_{0,2}$	$\cdots$	$e_{0,255}$
1	$e_{1,0}$	$e_{1,1}$	$e_{1,2}$	$\cdots$	$e_{1,255}$
2	$e_{2,0}$	$e_{2,1}$	$e_{2,2}$	$\cdots$	$e_{2,255}$
...	...	...	...	...	...

- The equation of the error is:

$$e = SB^{-1}(C \oplus K10) \oplus SB^{-1}(D \oplus K10)$$

- For each pairs:
  - Computation of *e* for all possible *K10*
  - Construction of an error table

Simplification of an existing DFA

- Only one column correspond to the right key hypothesis
- Visual discrimination between right and false hypothesis
- Easy to identify pattern from random value

- Only 3.5 faulted text with repeatability of 50%
  - More efficient than two previous attack schemes
  - Convenient for fault with distinctive pattern or low repeatability

DFA Results

Simplification of an existing DFA

- Only … ey hypothesis
- Visua … se hypothesis
- Easy

Realization i	K10 hypothesis k					
	'0x00'	'0x01'	⋯	**'0xCD'**	⋯	'0xFF'
0	'0x63'	'0x61'	⋯	**'0x02'**	⋯	'0x15'
1	'0xB2'	'0x0A'	⋯	**'0x06'**	⋯	'0x59'
2	'0x0C'	'0xBF'	⋯	**'0x02'**	⋯	'0x1E'
⋯	⋯	⋯	⋯	⋯	⋯	⋯
158	'0x51'	'0xFF'	⋯	**'0x06'**	⋯	'0x1A'
⋯	⋯	⋯	⋯	⋯	⋯	⋯
3,578	'0xF2'	'0x49'	⋯	**'0x08'**	⋯	'0x82'
⋯	⋯	⋯	⋯	⋯	⋯	⋯
10,000	'0x09'	'0x3B'	⋯	**'0x0A'**	⋯	'0x33'

- Only 3.5 faulted text with repeatability of 50%
  - More efficient than two previous attack schemes
  - Convenient for fault with distinctive pattern or low repeatability

Fault injection

- With large spot size (125μmx125μm)
  - Bit-flip fault model observed
  - Bit set/reset observed too
    - Unexpected
- Metal fills act as shutter on the laser beam
- Single-bit injected thanks to the metal coverage
- Laser injection
  - Data dependent
  - Time dependent

Exploitation of the data with DFA

- **Efficiency with high repeatability**
  - Giraud and Roche's DFA are not the most efficient

- Simple application of a DFA proposed
  - More efficient with low repeatability
  - Exploit fault injection pattern

Thank you for your attention

Questions?