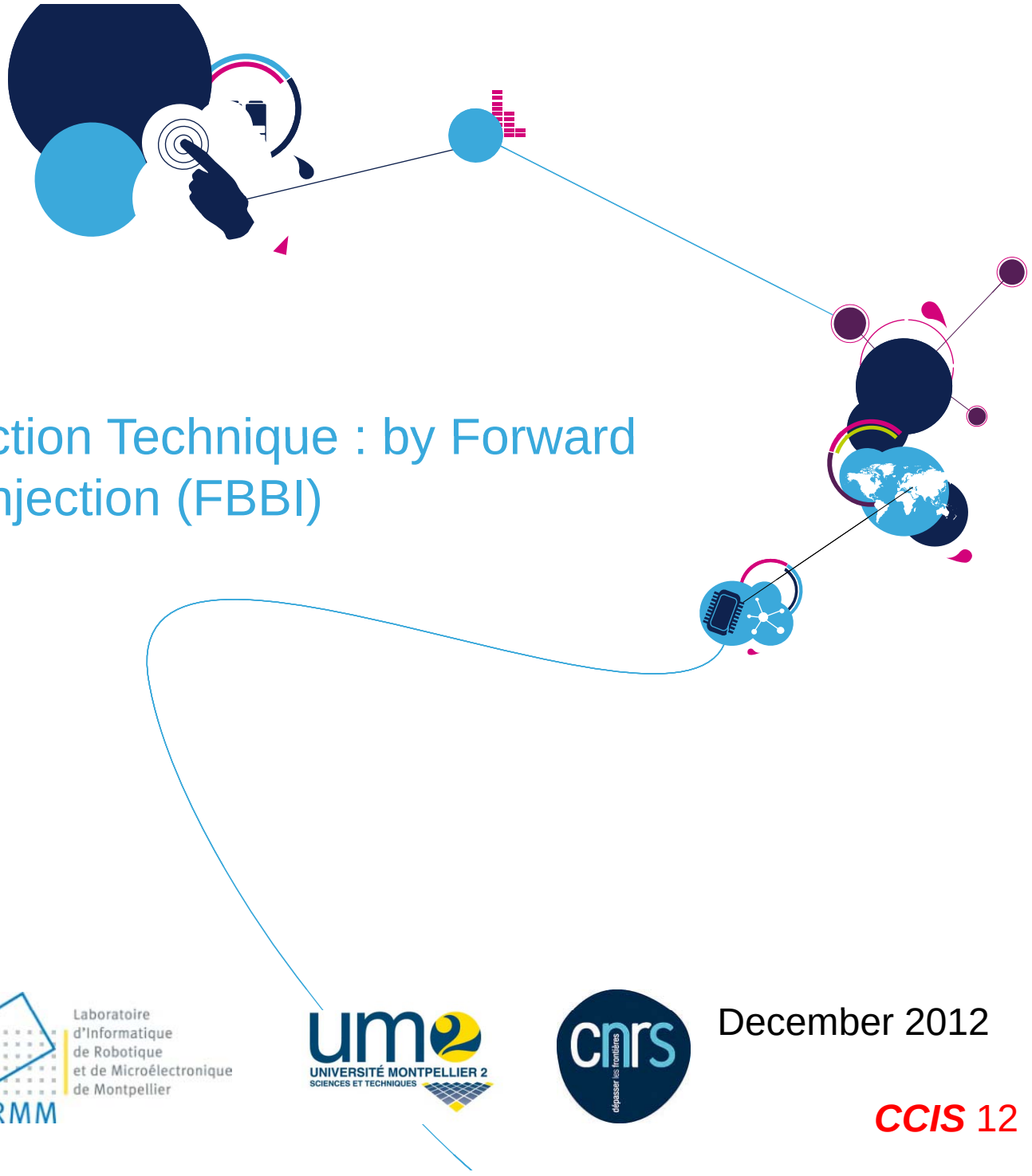


New Fault Injection Technique : by Forward Body Biasing Injection (FBBI)

Karim TOBICH
Pierre-Yvan LIARDET
Philippe MAURINE
Thomas ORDAS

life.augmented

Laboratoire d'Informatique de Robotique et de Microélectronique de Montpellier
LIRMM

UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

cnrs
dépasser les frontières

December 2012

General Context

Embedded applications
- Financial Services
- Government
- Transport
- Telecommunications
- …

Cryptography
- Identification
- Authentification
- Confidentiality

Standard Algorithms
- AES, DES
- RSA, ECC
- MD5…

Cryptanalysis

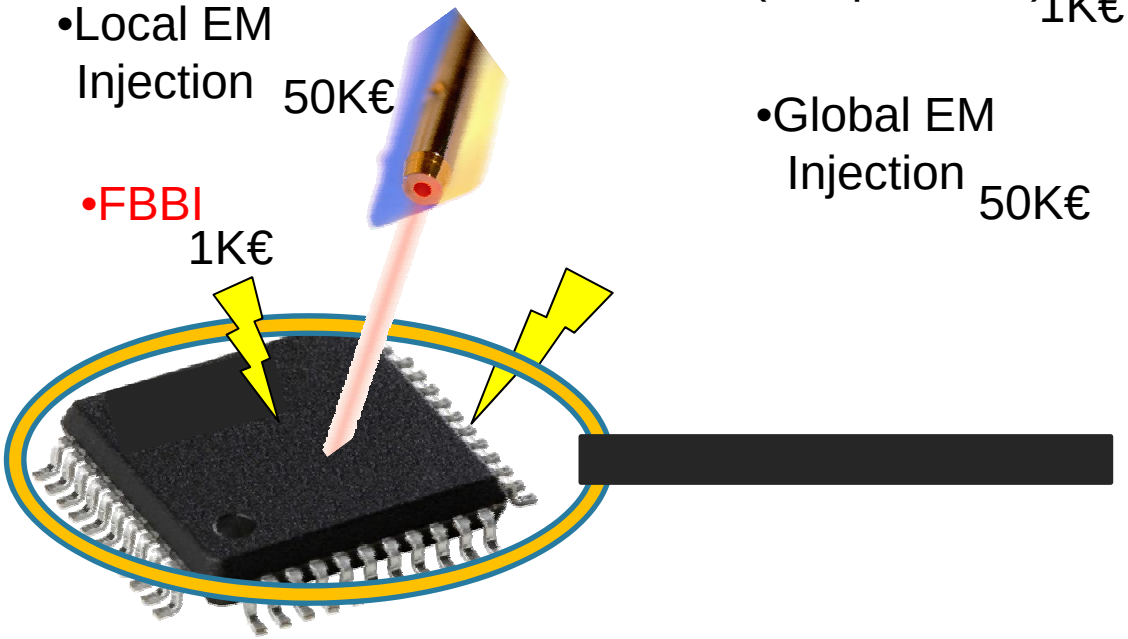
Classic attacks
- Brute Force
- Differential
- Linear
- Algebraic

Software attacks
- Code Injection
- Network attacks
  - Flooding
  - Smurfing
- Protocol attacks

Physical Attacks
- Observation
- Perturbation

Perturbation techniques

Invasive	Semi invasive	Non invasive
•Focus Ion Beam (FIB) 1M€	•Laser 100K€	•Glitches on pads (clk, power…) 1K€
•Micro probing	•Local EM Injection 50K€	•Global EM Injection 50K€
	•FBBI 1K€	



Context packaging

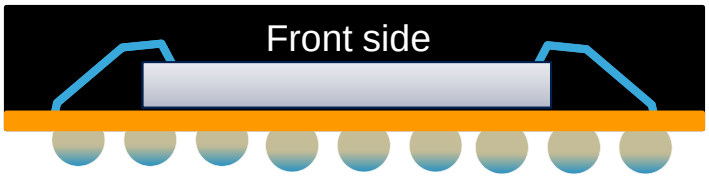
Embedded cryptography

- Symetric crypto-blocks
- Modular arithmetic accelerator
- TRNG …

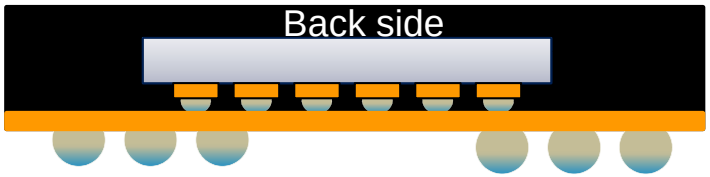
Embedded Countermeasures

- Internal clock generator
- Voltage regulators / Sensors
- Light sensors …

Wire bonded BGA



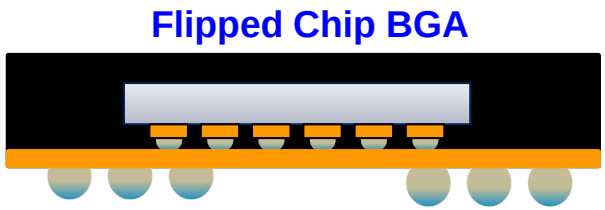
Flipped Chip BGA



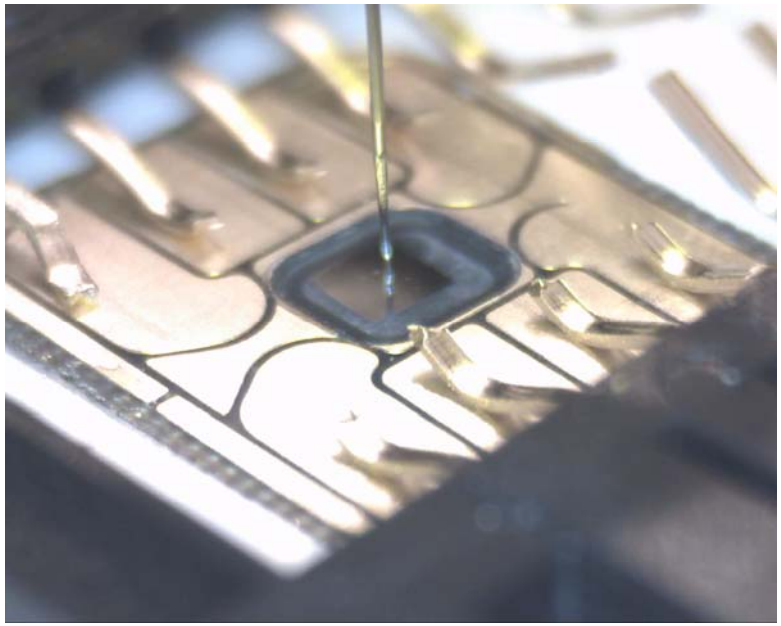
How to inject faults into such components?

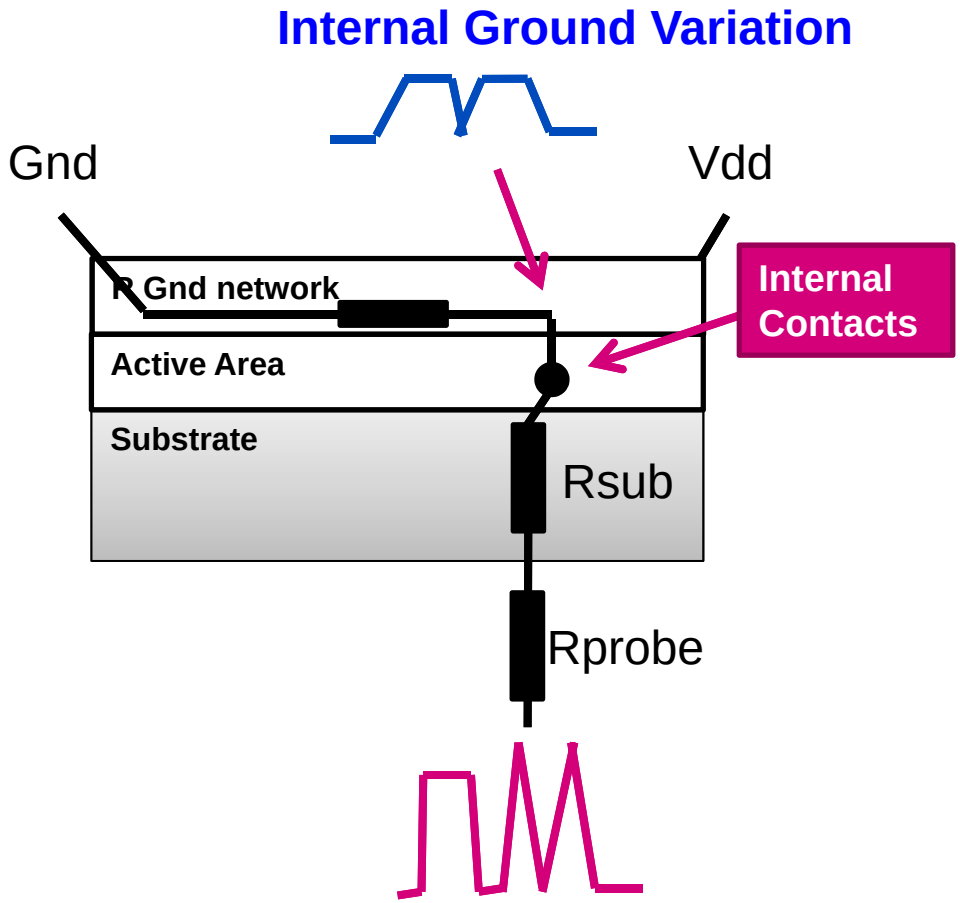
Summary

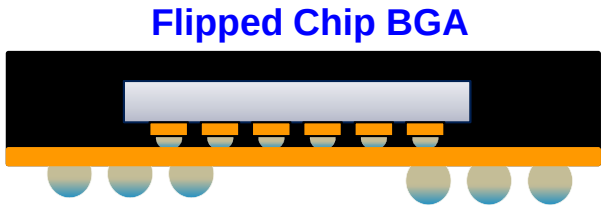
- Idea and model
- Platform and target
- Results analysis
- Conclusion



Idea and model







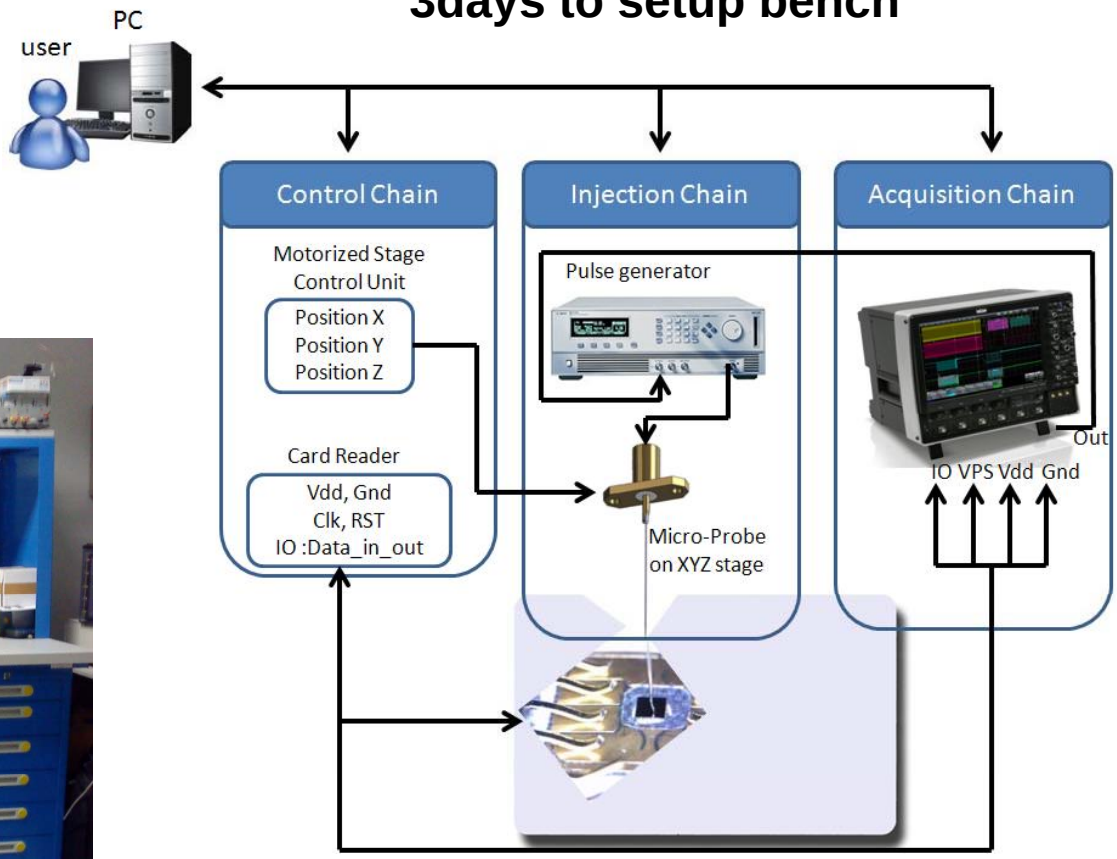
Targets

Targets	Analog Blocks		Digital Blocks
	Internal Clock Generator	TRNG	logic and memories
Goal	Increase the frequency to produce timing fault	Dynamically bias TRNGs (locking and latching)	Generate timing fault (setup time constraint)
How	Providing directly and locally Power to the P/G network	Providing a frequency on the P/G network	pulse / Voltage drop / timing violation
FBBI Injection Type	**Harmonic or periodic Injection** Intense & long duration & local Electrical variation		**Pulse Injection** Intense & local & short & sudden electrical variation

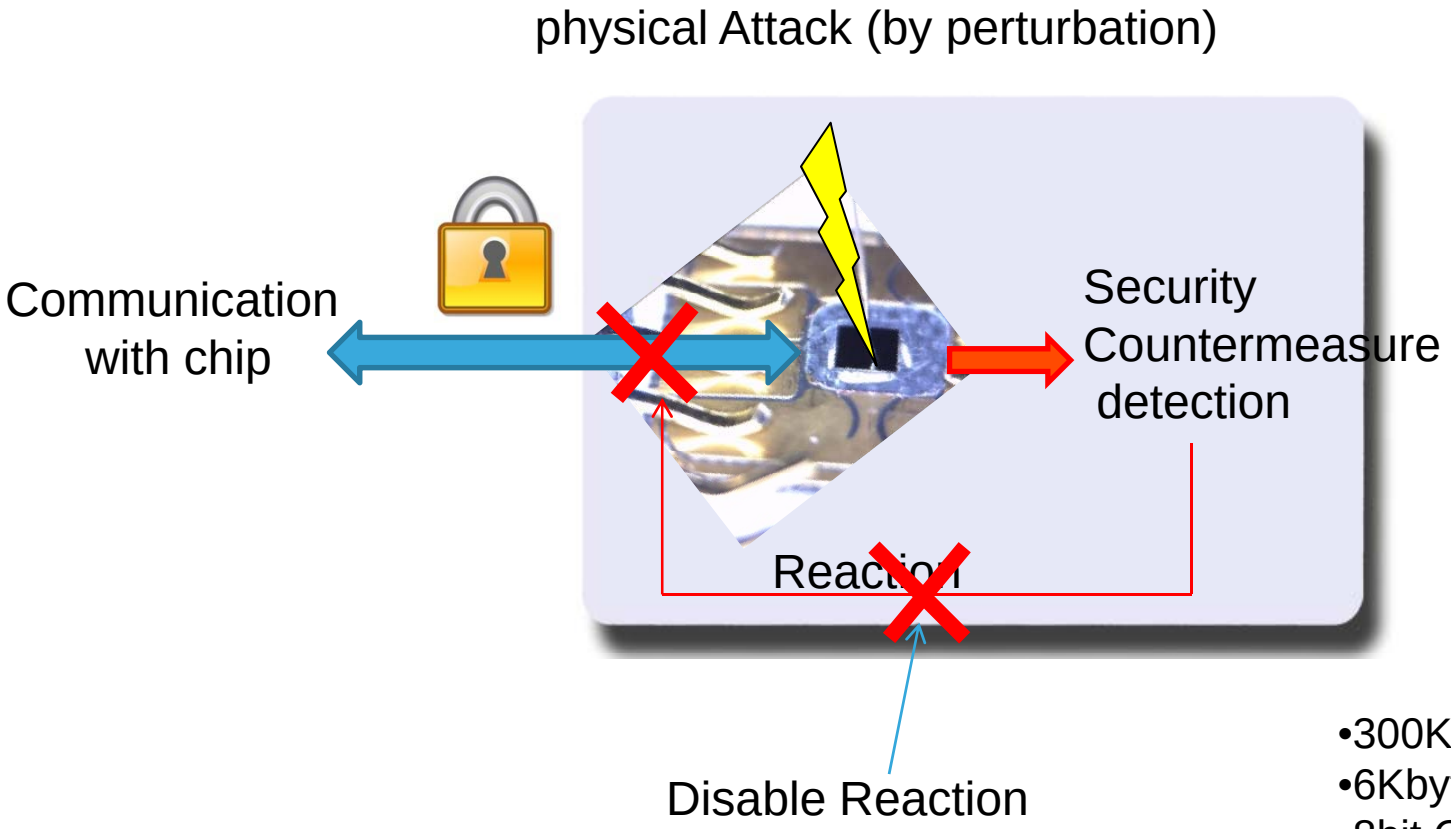
RSA computation
Based on 90nm
Techno

Injection Platform

3days to setup bench

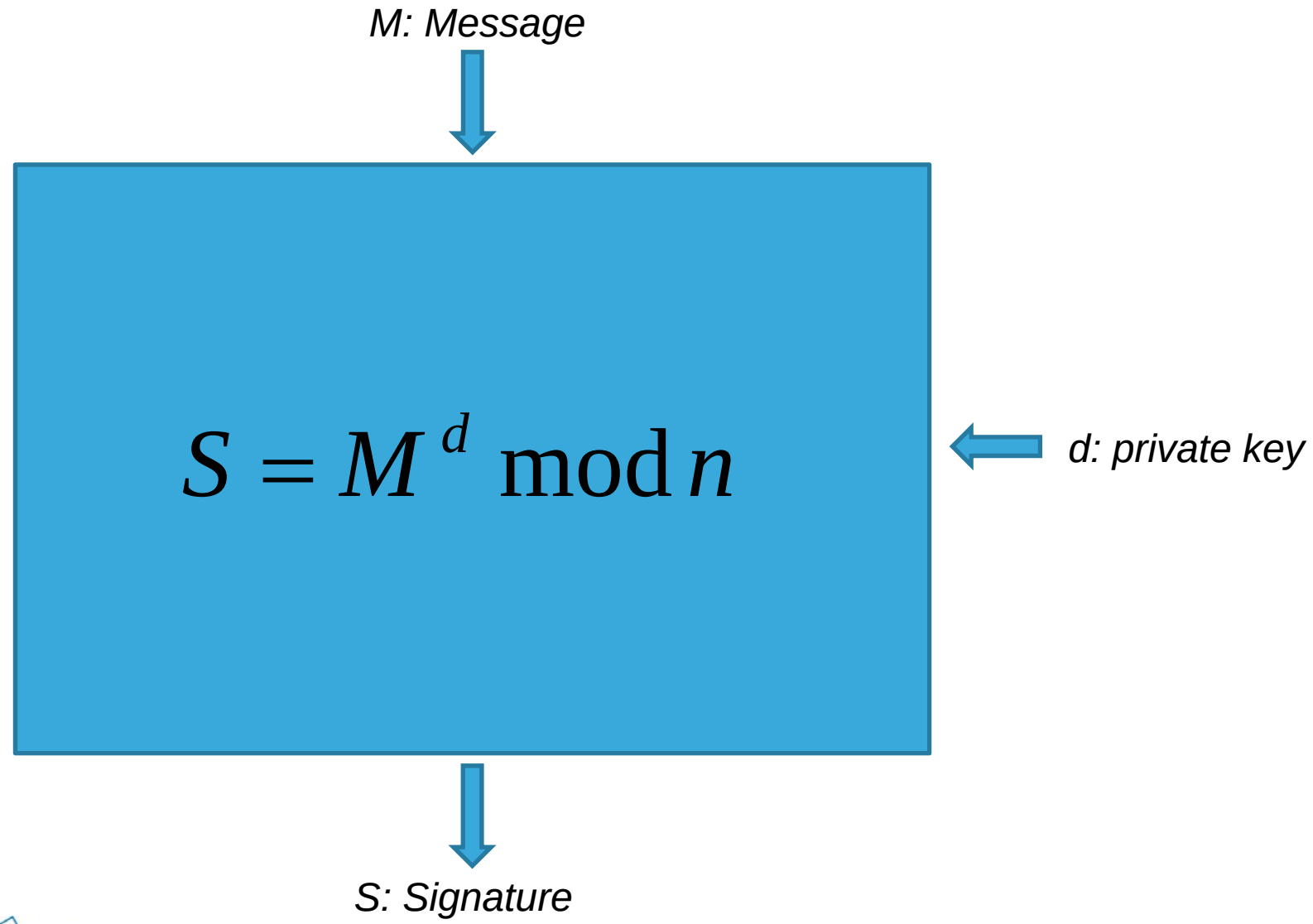


Application to a secure chip

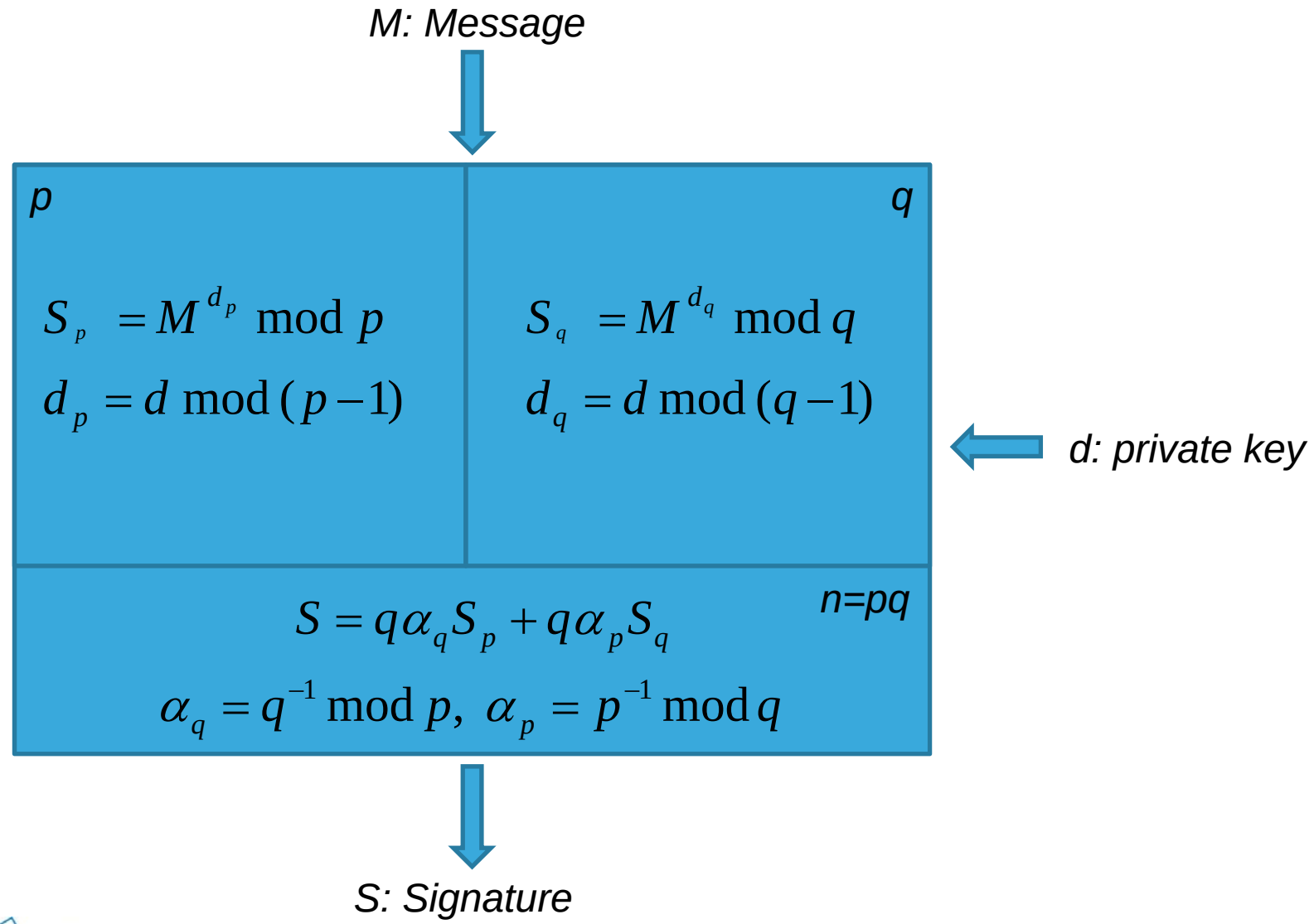


- 300Kbytes ROM
- 6Kbytes RAM
- 8bit CPU core
- 48Kbytes EEPROM
- Crypto-Coprocessor
- Different Security features
- Techno 90nm

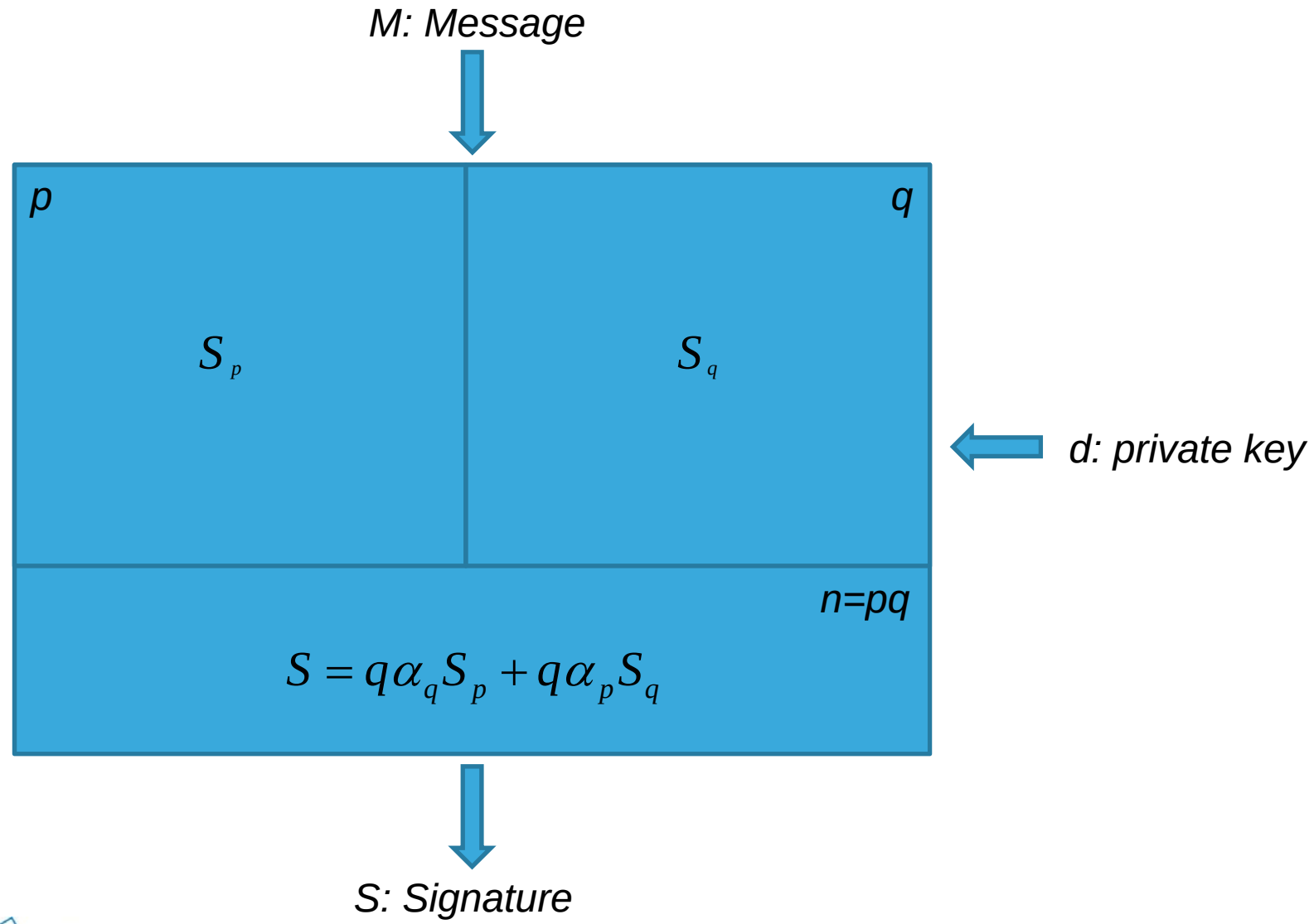
RSA computation



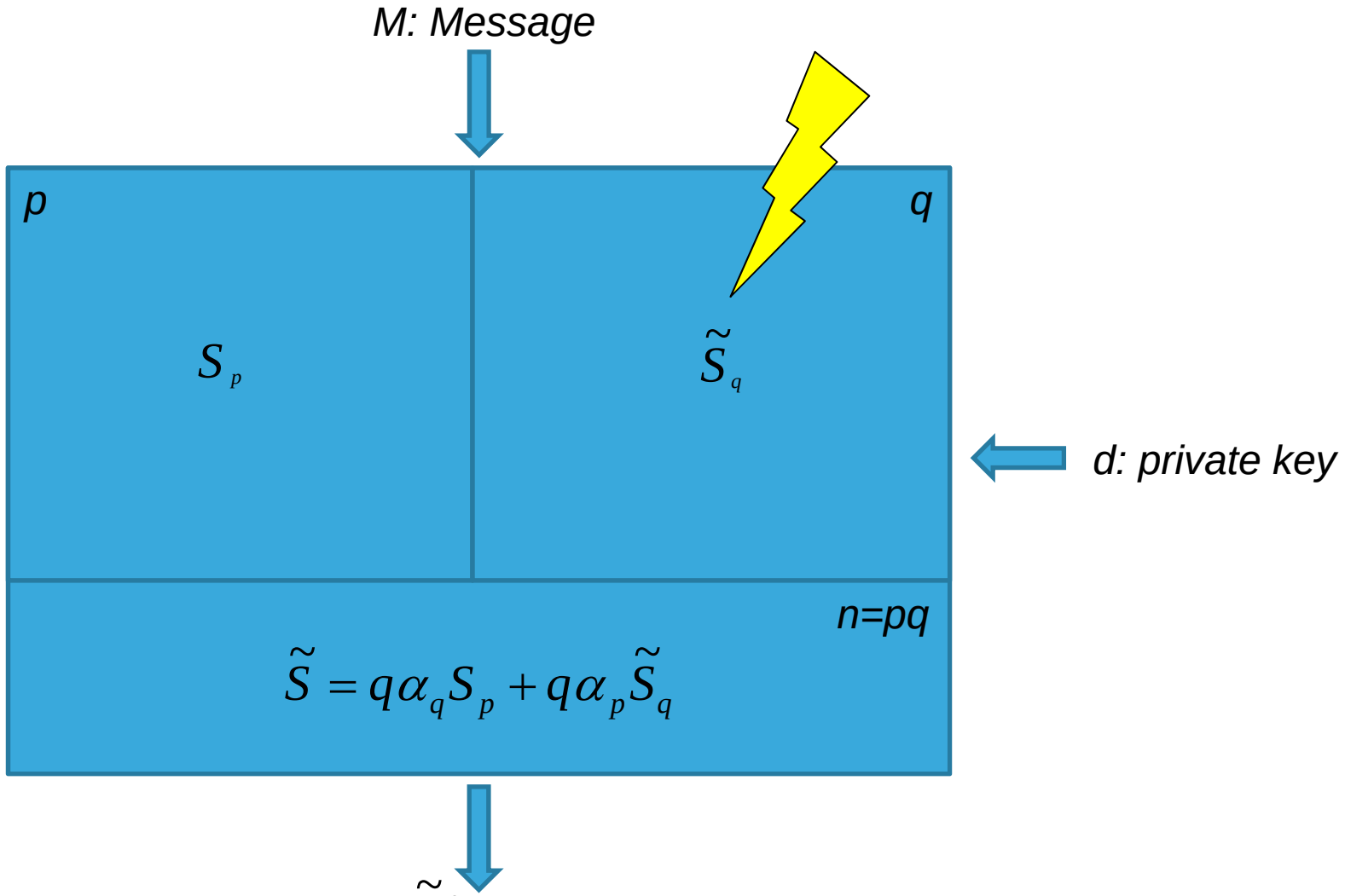
RSA computation



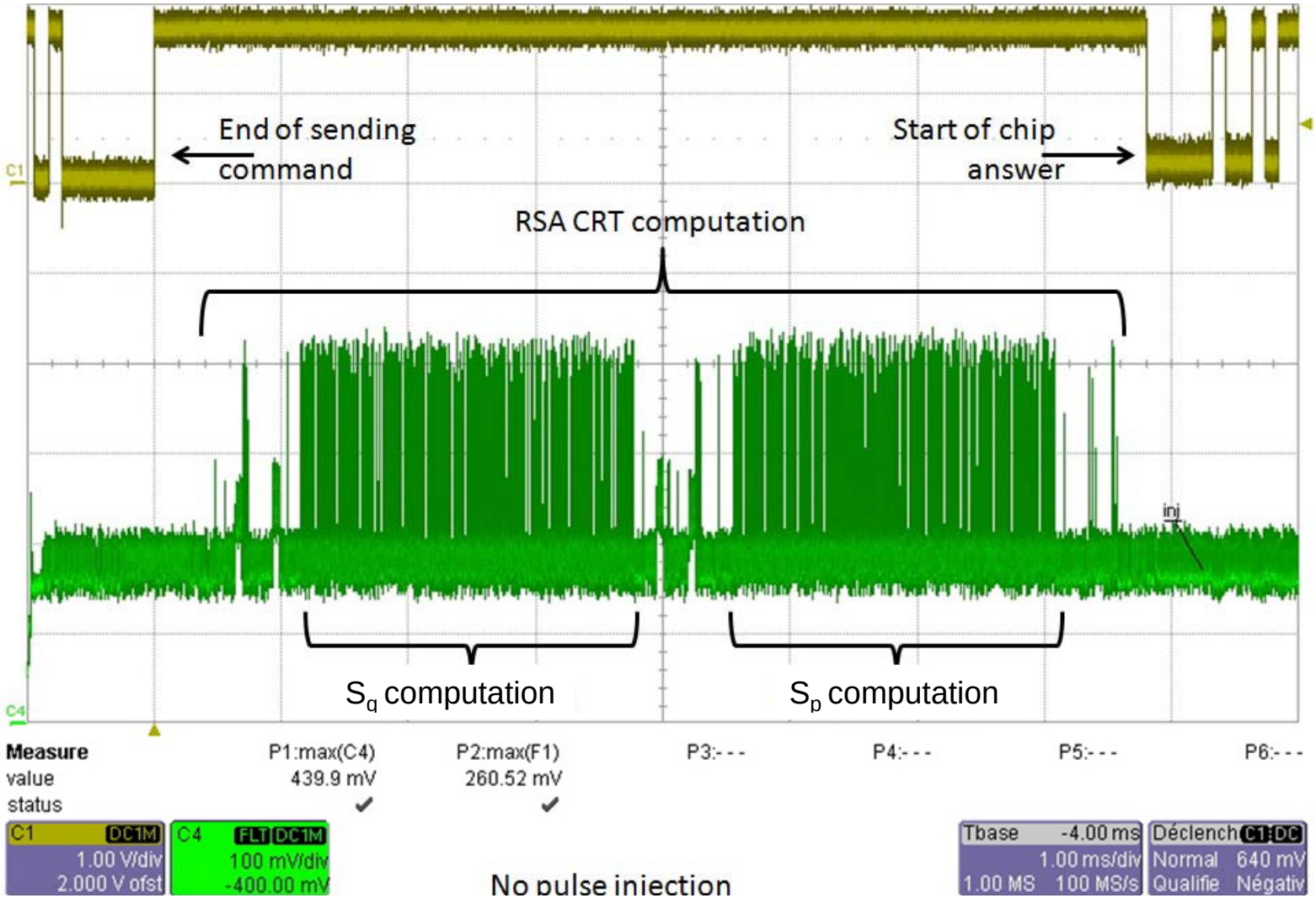
RSA perturbation



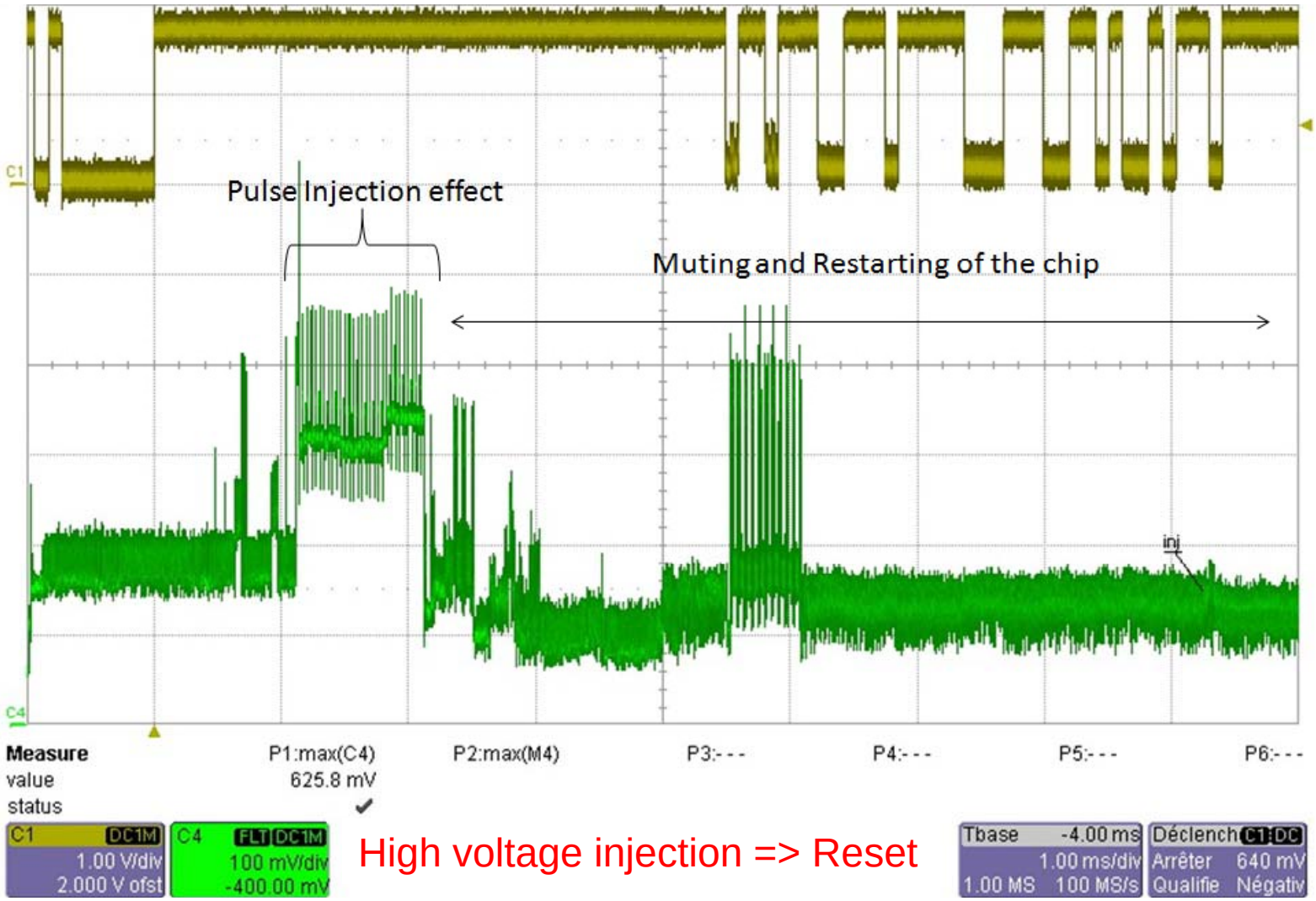
RSA perturbation



RSA-CRT trace without perturbation



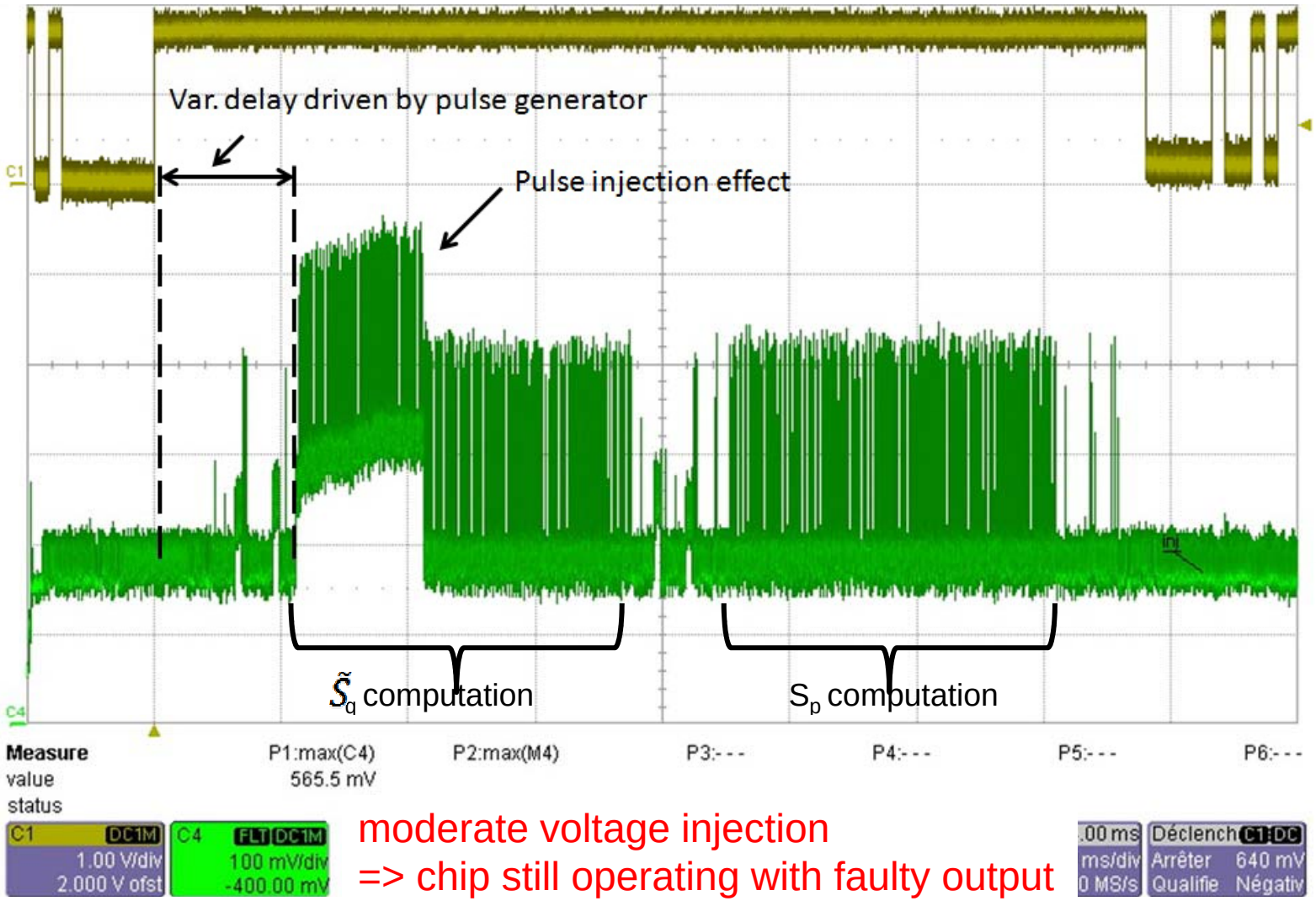
RSA under FBBI attacks



High voltage injection => Reset

K.TOBICH, P MAURINE, P-Y. LIARDET, T. ORDAS V3

RSA under FBBI attacks

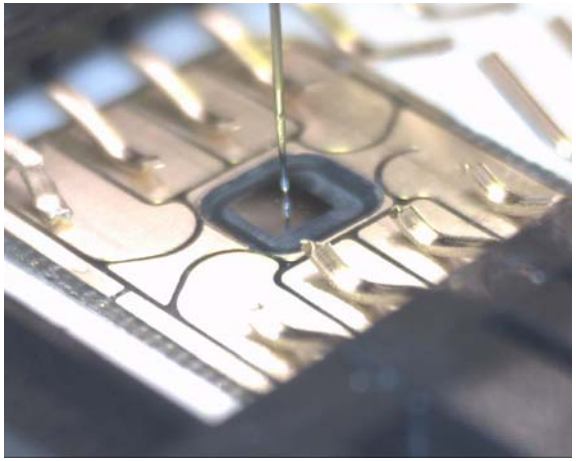


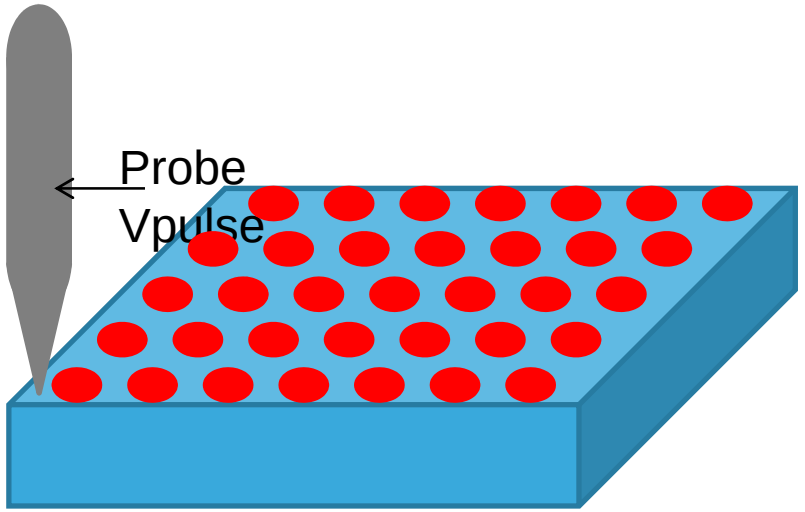
moderate voltage injection
=> chip still operating with faulty output

K.TOBICH, P MAURINE, P-Y. LIARDET, T. ORDAS V3

Cartography (Chip Scanning)

1 Cartography=1day
=> N cartographies du to Voltage, width and delay pulse parameters
=> 3weeks (for success perturbation)





Circuit =1900x1900µm, Probe diameter =20µm. Step 100µm
For each scanning point 10 pulses injection are done.

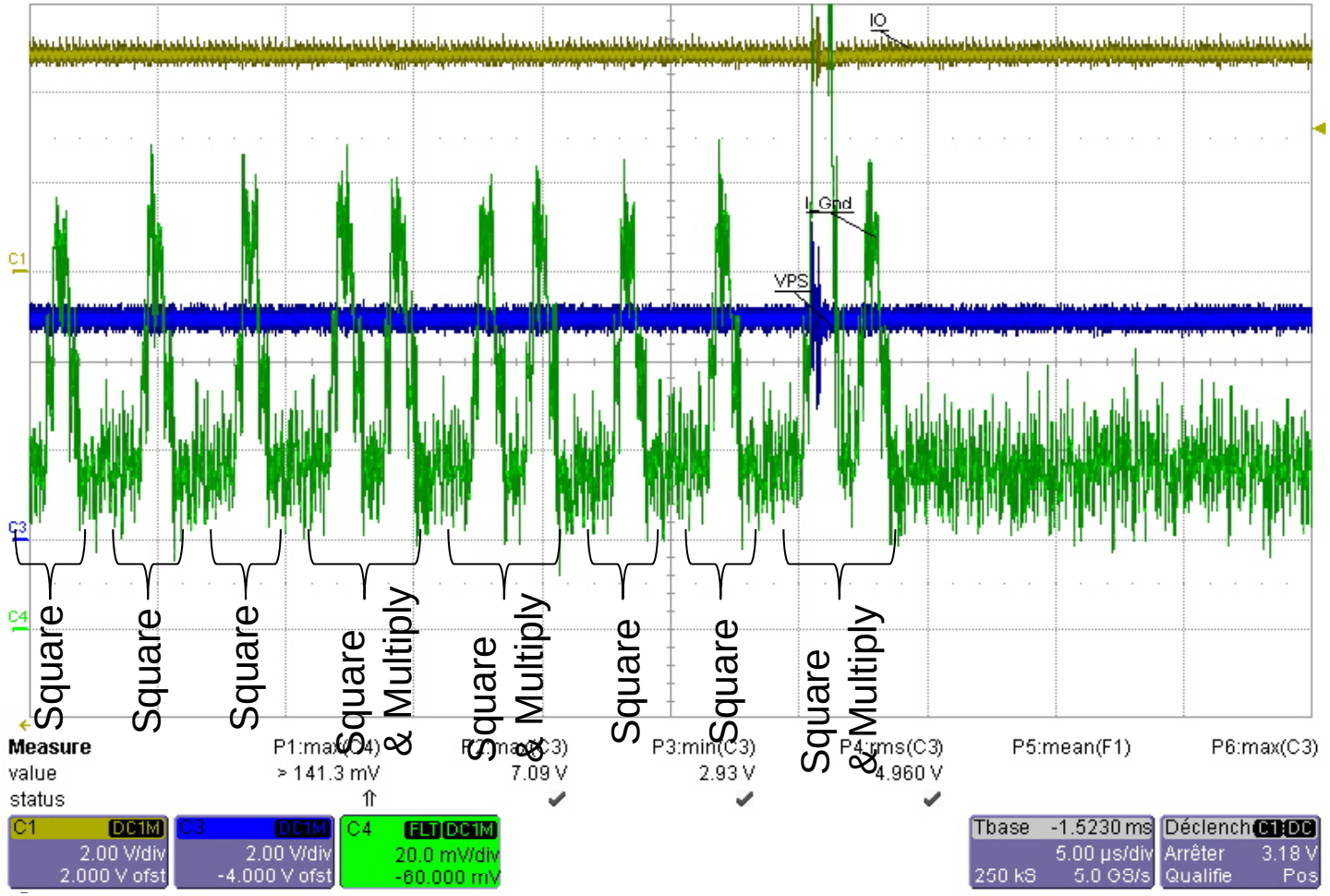
Analysis of results

Log information	%
Numbers of Injections: 19830	100%
Correct answers	66%
No answers (Mutes)	6%
Faulty but non exploitable answers	27.78%
Faulty and exploitable answers	0.22%

For the Bellcore attack

Analysis of trace

- Exploitable faulty outputs obtained on RSA activity peaks

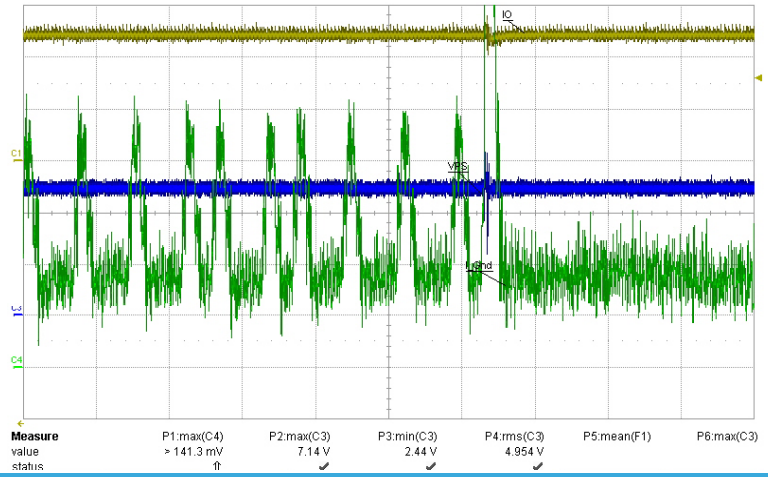


Analysis of results

Log information	%
Numbers of Injections: 19830	100%
Correct answers	97.1%
No answers (Mutes)	0.5 %
Faulty but non exploitable answers	0%
Faulty and exploitable answers	2.37 %

For the Bellcore attack

Fail occurrence



Faults	%
2CDEB075949B82DD3011E6F9AA9B0F95F9F9DAAD92EBD	3.65
01CF582035C5F277CA1D4F8ED123C4352AE655B6E59DD	7.31
0E095170386BAF04368074F22A3557045A1C25A4E5705A	12.9

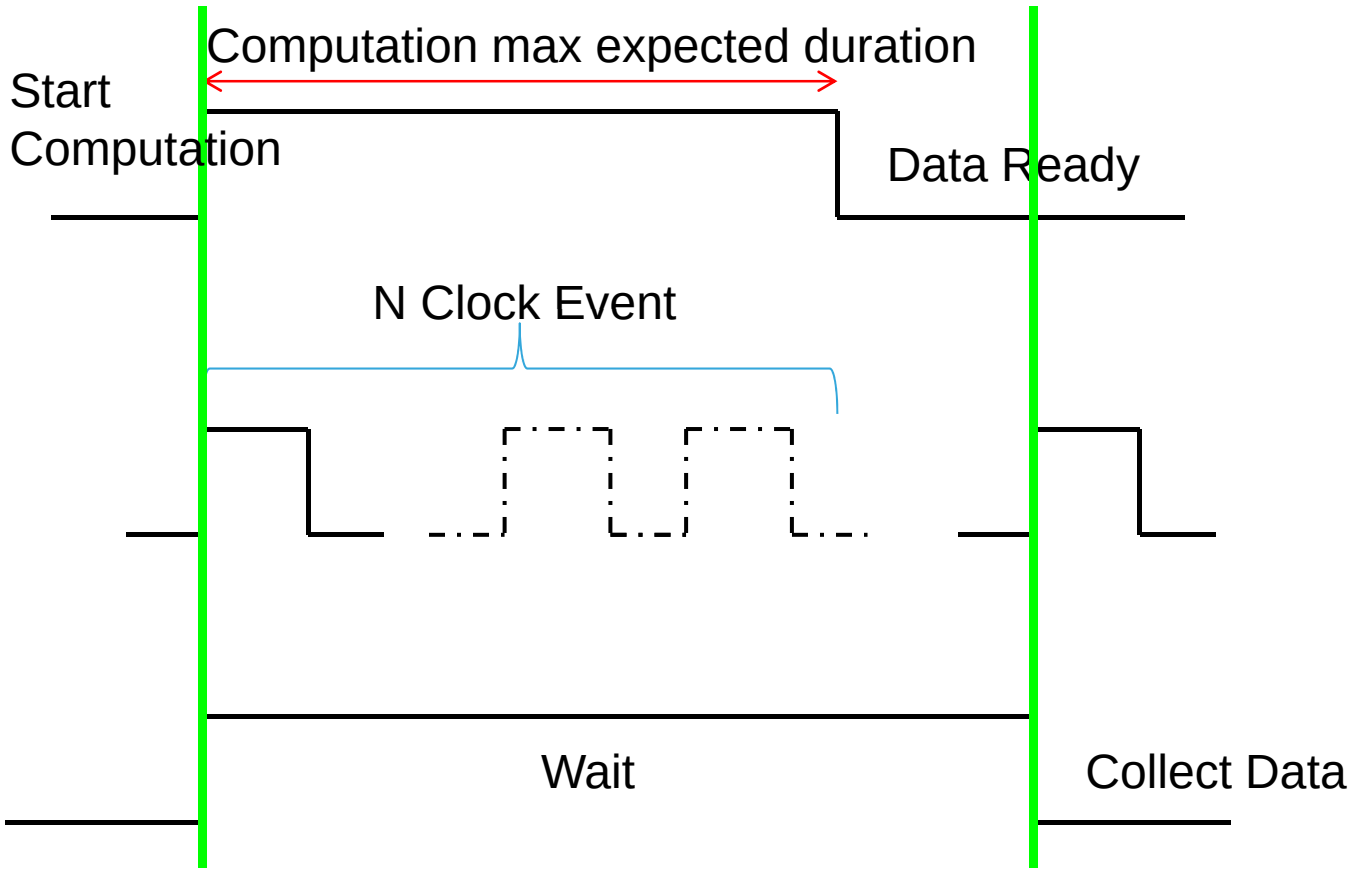
Despite the jitter !!

Voltage & Timing Slack vs clock Frequency

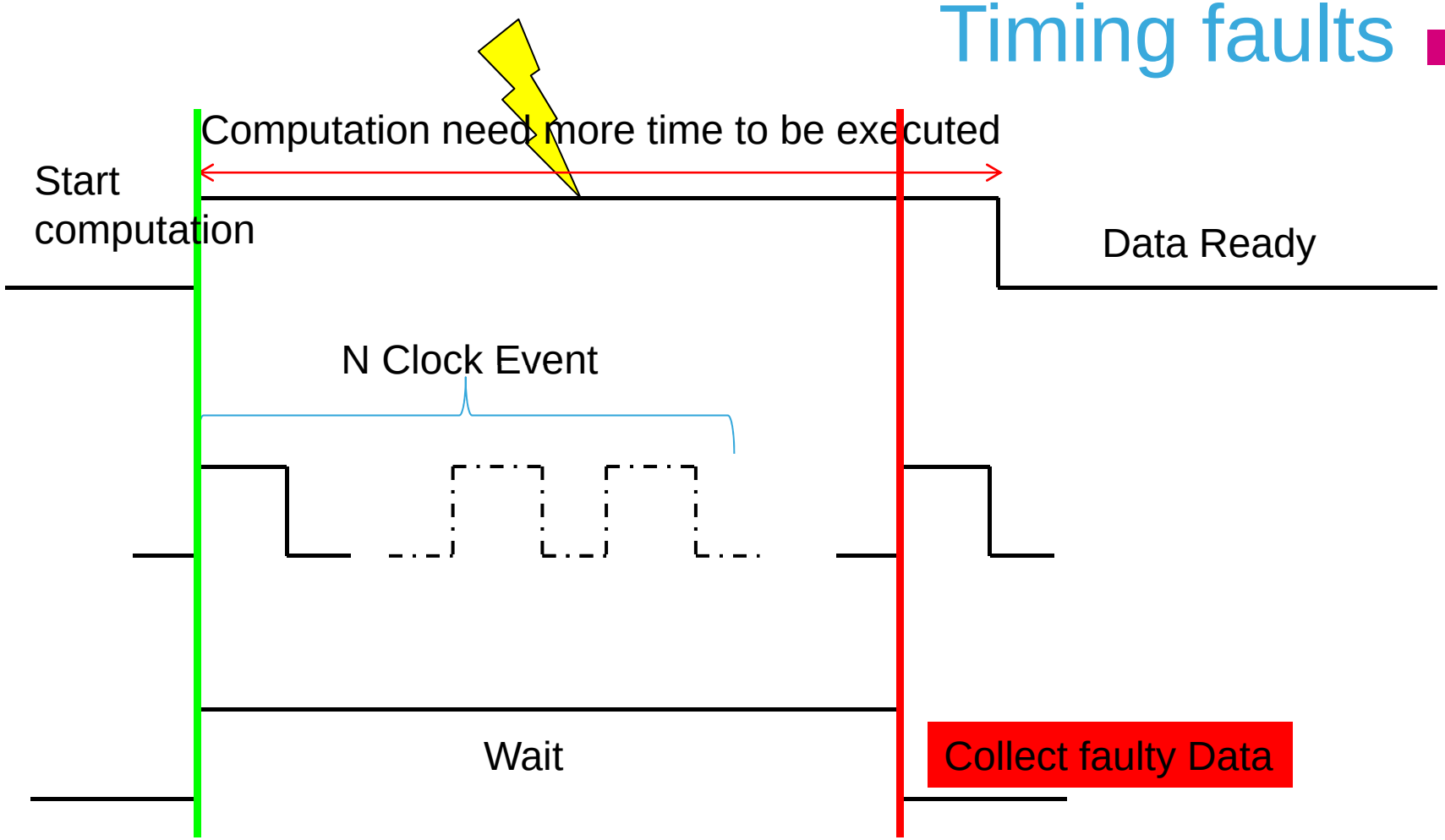
Log Information	Clock Frequency			
Faulty and exploited answers	2 FCK ref	Fck	1/8 FCK ref	1/16 Fck ref
Vpulse (en Volts)	Vmin1	Vmin2	Vmin2	Vmin2
Timing Slack / reference (ns)	- 8.70	0	52.2	121

Timing faults

Normal time operating



Timing faults



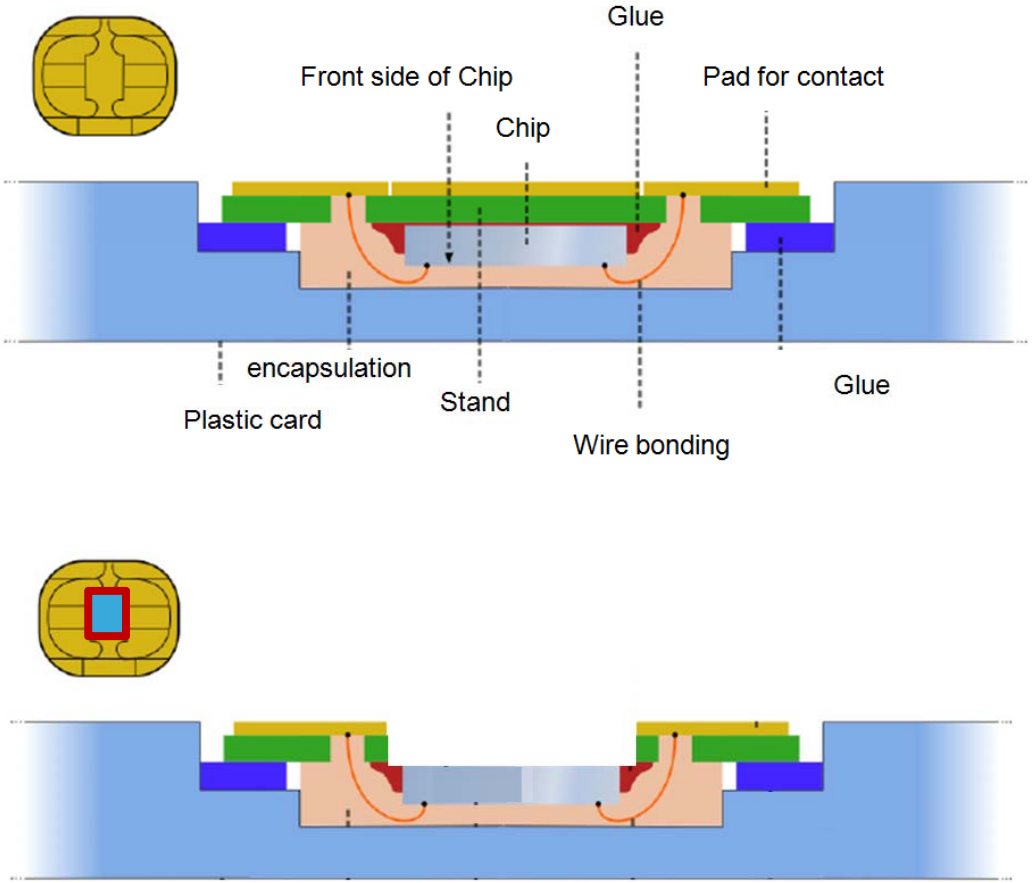
Conclusion

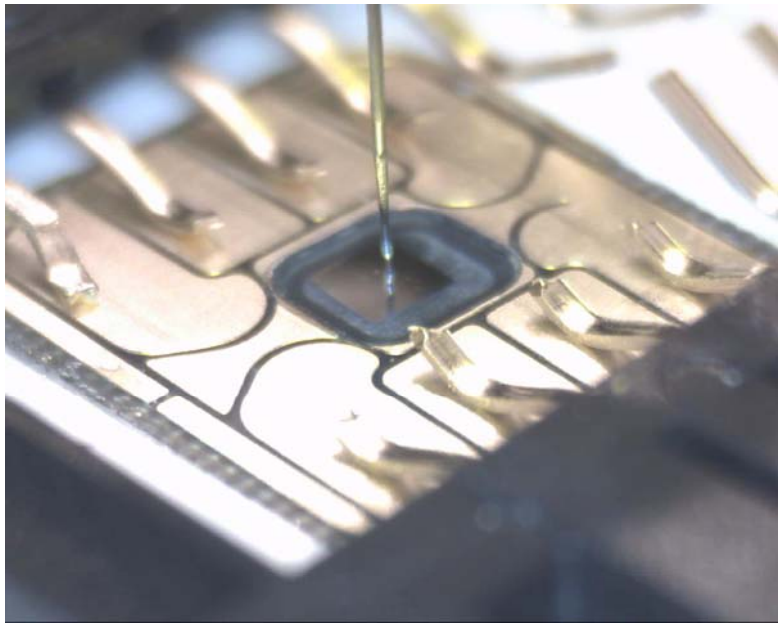
- FBBI proof of concept
  - Obtain exploitable faults (Bellcore Attack)
  - Is a Low cost technique (1K€)
  - Is Easy to setup (3days for bench, 3weeks for pulse generator, some seconds to secret)
- BUT
  - Flagged by security detector (on this component)
  - Requires timing precision
  - Local effect (allow implement counter-measure)
- Further works
  - Improve the Bench
  - Apply FBBI technique on different technologies
  - Apply FBBI technique to induce faults during different algorithms execution…

Thank you for
your attention.

Questions?

Chip preparation





FBBI simplified Model