Impacts of technology trends on physical attacks ?

P. Maurine

Context & motivation

1996 : Timing attack on 120 MHz Pentium
Technology node: 350nm

P. C. Kocher:
Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. CRYPTO 1996:

20 years only

2017 : core i7 7700 – 4.20 GHz
Technology node : 14nm ?

Integrated technologies have changed quickly
BUT
are at a crossroad !

Agenda

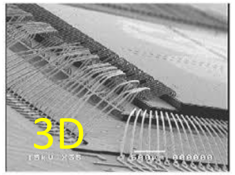
- **Integrated Circuits : evolution and trends**
  - CMOS technology evolution
  - Secure ICs of tomorrow

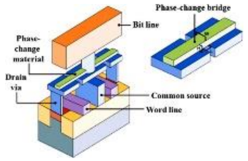
- **Technology trends and adversary challenges**
  - Current practice of Physical attacks
  - Adversary's Challenges

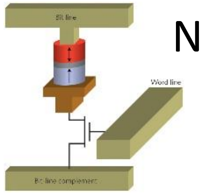
- **Conclusion & discussion**

CMOS technology evolution (processors and high end products)

CMOS technology helpers (flash scaling limits and costs)



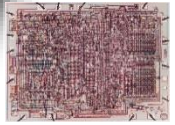




New NVMs

1970

10µm



Moore Law

Dennard scaling Law

Design methologies and CAD tools

Variability issues
Leakage issues
End of Vth and Vdd scalings

Power density issues

Multi-cores architectures
Adaptive design solutions

2001-2003

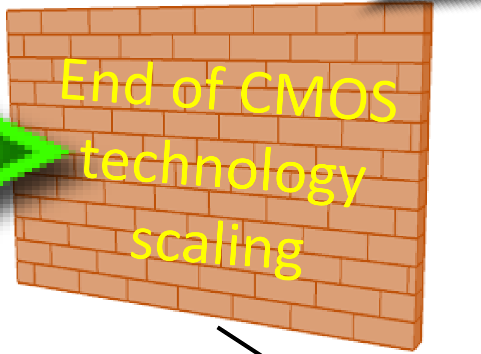
90nm

Litography wavelength / Transistor length
193nm > 2x90 nm

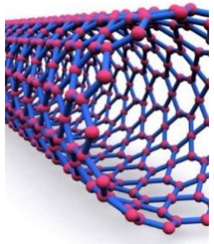
14nm

2021-2030

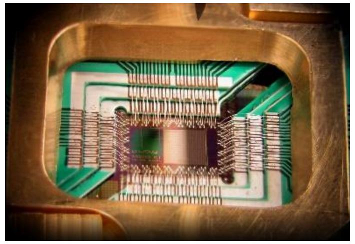
7nm



Beyond CMOS ?



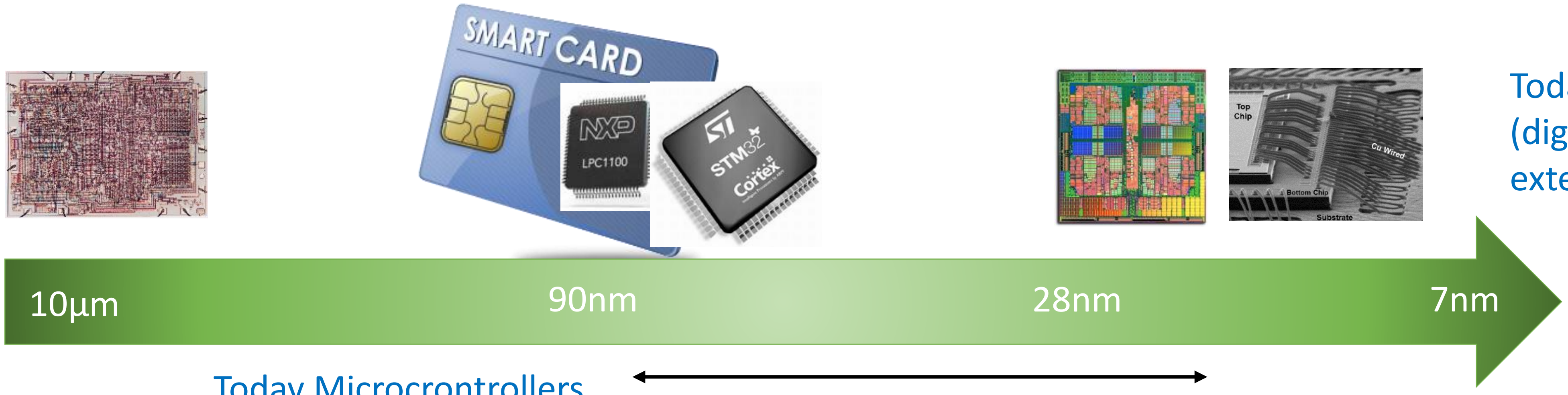
CNTs



Quantum computing

Is it a critical and urgent problem for us?

Current Secure ICs (smartcards and µC) wrt CMOS scaling



Today high-end products (digital products with external memories)

Today Microcrontrollers and smartcards (Embedded memories)

Technology Gap : 5 to 7 technology nodes
(10 current smartcards on 1.5mm²)

eFlash scaling (required to secure data and keys) is difficult and has a cost !

µC and smartcards follow CMOS technology scaling with a latency of 5 to 7 technology nodes …. but they follow!

So we may think to have time before facing issues related to advanced technologies !! ... Really …? Well no !!

CMOS scaling benefits and … its impact on security !

Pentium

Year : 1993

239 DMIPS @133MHz

P/MHz= 75mW/MHz

3100 K transistors

L=800nm

Vdd=3V

20 years later only

STM32F4

Year : 2013

225 DMIPS @180MHz

P/MHz=40µW/MHz

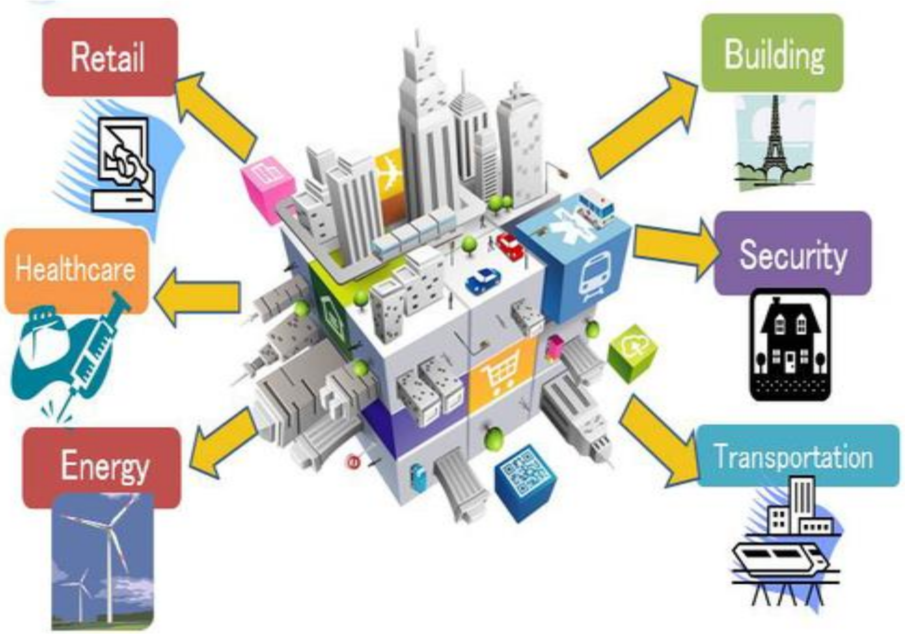
1246 Kgates

L=90nm

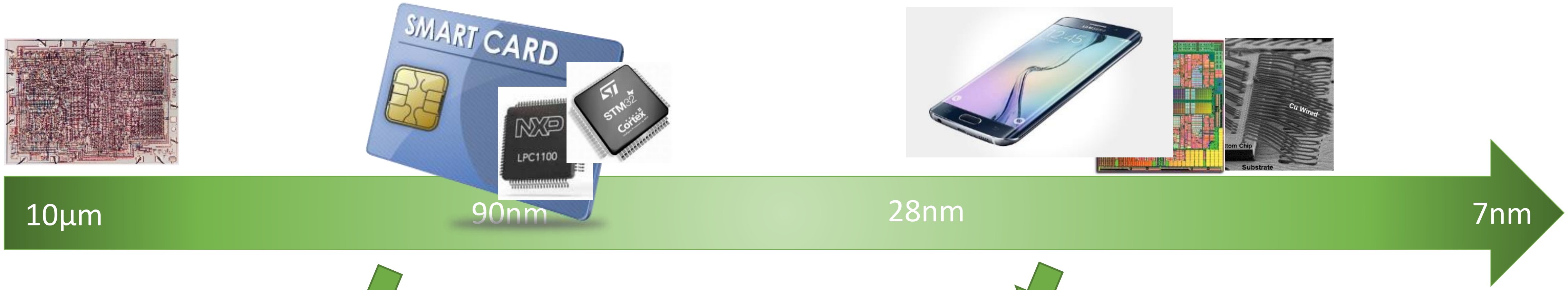
Vdd=1.2V

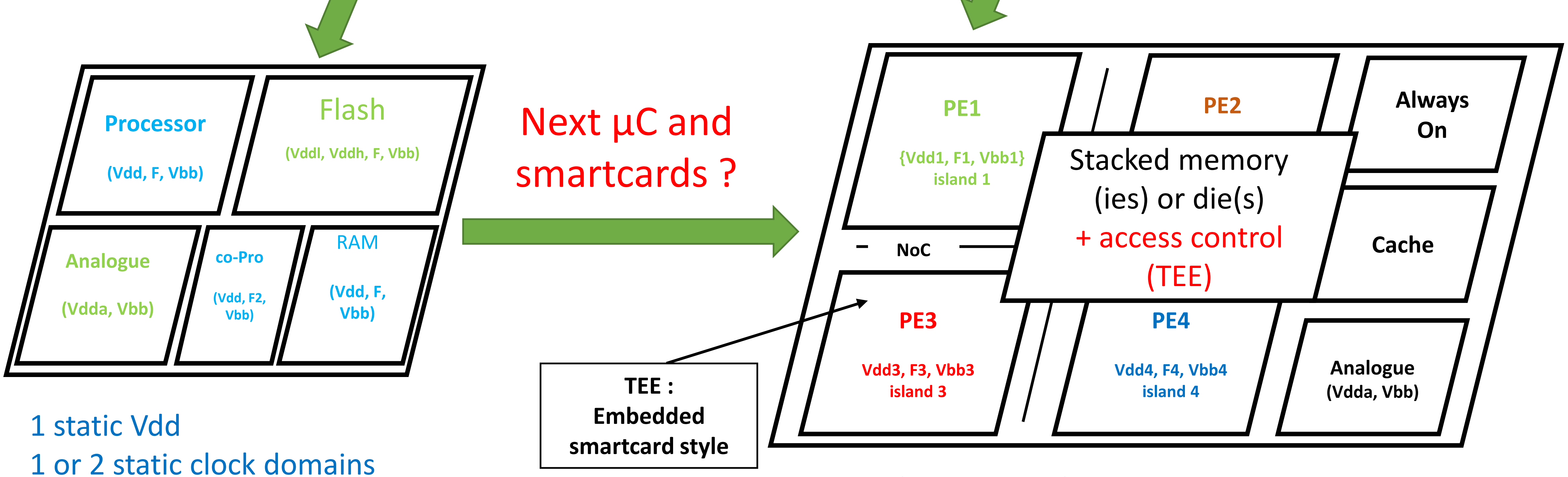
Huge and critical needs for security !

(ICs involved in the control of physical operations in the real world … with risks on property and persons ...)



Secure ICs of today and tomorrow





Processor

(Vdd, F, Vbb)

Flash

(Vddl, Vddh, F, Vbb)

Analogue

(Vdda, Vbb)

co-Pro

(Vdd, F2, Vbb)

RAM

(Vdd, F, Vbb)

Next µC and smartcards ?

PE1

{Vdd1, F1, Vbb1} island 1

PE2

Always On

Stacked memory (ies) or die(s)

+ access control (TEE)

NoC

Cache

PE3

Vdd3, F3, Vbb3 island 3

PE4

Vdd4, F4, Vbb4 island 4

Analogue (Vdda, Vbb)

TEE : Embedded smartcard style

1 static Vdd
1 or 2 static clock domains
1 or 2 static Vbb

Many {Vdd, F , Vbb} islands
dynamic scaling of operating parameters

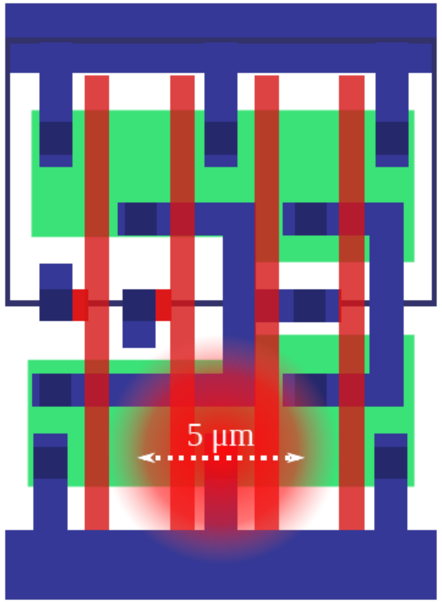
Current Practice of Physical Attacks

<table>
<tr><th>Fault Attacks</th><th>Side Channel Attacks</th></tr>
<tr><td>Physical access to the device (laser, BBI, EMFI, …)</td><td>Access to a leaking signal (Power, EM)</td></tr>
<tr><td colspan="2">Stability of the targeted instructions/signals in time
- constant Vdd, Vbb, Fclock</td></tr>
<tr><td colspan="2">Unique location for a given sensitive computations</td></tr>
<tr><td colspan="2">Moderated clock frequencies, few synchronous clock domains, synchronism of the different operations</td></tr>
<tr><td colspan="2">Moderated IC complexity (1 million equivalent gates)
Moderated computationnal noise</td></tr>
<tr><td colspan="2">90nm – 65nm technologies</td></tr>
</table>

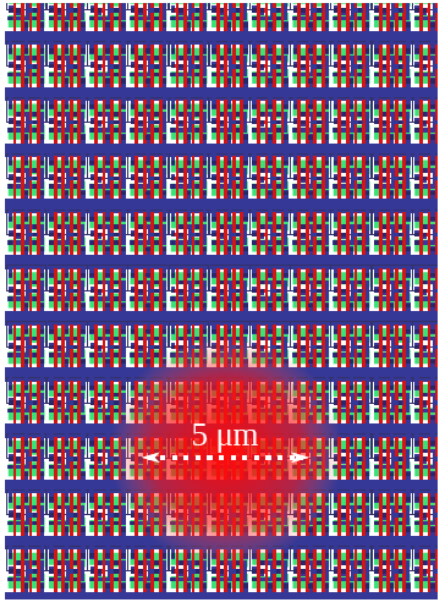
From 90nm to 28nm

	180nm	130nm	90nm	65nm	45nm	28nm
Vdd	1.8V	1.2V	1.1V	1V	1V	1V
Vth	0.4V	0.3V	0.3V	0.3V	0.3V	0.3V

No significant changes in I,V characteristics and gate delays



tech: 250nm - Hstd_cell: 12.5 µm



tech: 28nm - Hstd_cell: 1.2 µm

SCA Challenges :

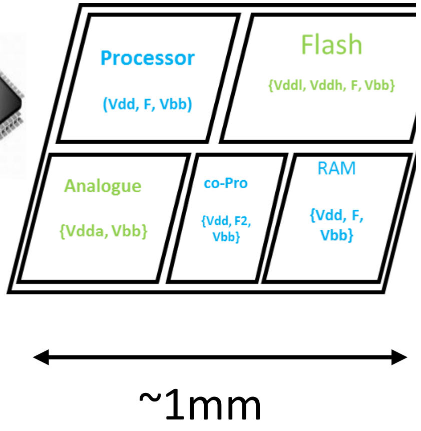
Scaling EM analysis probes

FA Challenges :

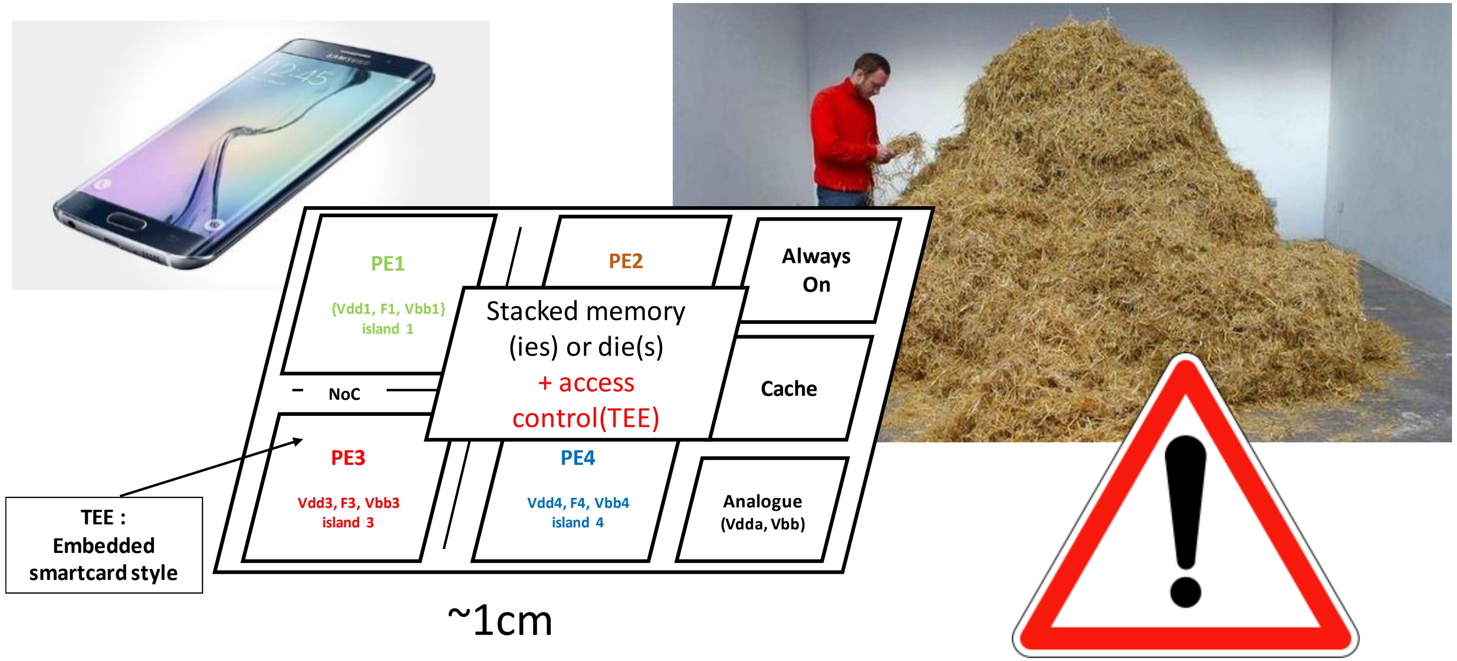
Scaling EMFI probes

Scaling laser spots

Design complexity (die size but not only) and Physical Attacks



Unexpected increase of smartcard size !!
Potential decrease of smartcard size ?



SCA Challenges :

Computational noise
Interpretability of noise

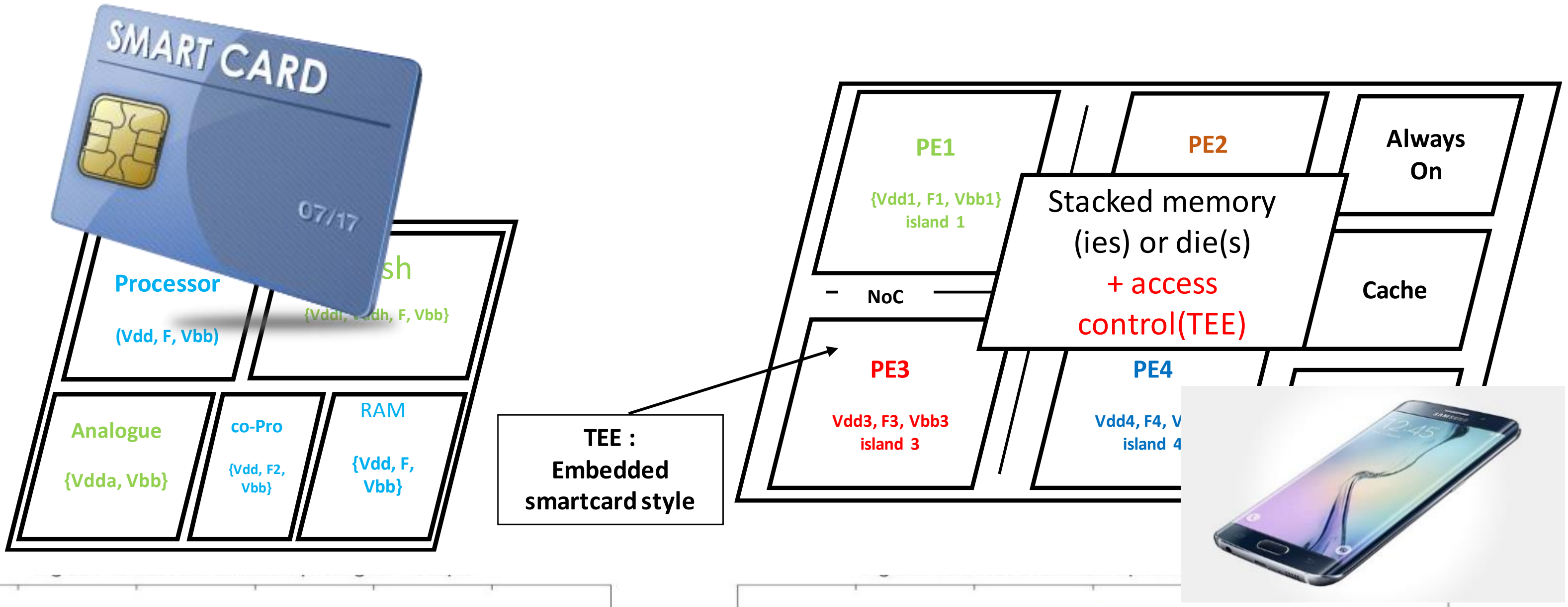
FA Challenges :

Interpretability of traces ?
Granularity of injection means ?

Adaptive designs (varying Vdd, F, CLK frequency) and Physical Attacks

Cryptographic algorithm execution parallelized on several potential asynchronous processing units working with:

- **Time varying clock frequency**
- **Time varying Vdd and body bias**



SMART CARD

07/17

Processor

(Vdd, F, Vbb)

sh

{Vddf, Vddh, F, Vbb}

Analogue

{Vdda, Vbb}

co-Pro

{Vdd, F2, Vbb}

RAM

{Vdd, F, Vbb}

TEE : Embedded smartcard style

PE1

{Vdd1, F1, Vbb1} island 1

PE2

Always On

Stacked memory (ies) or die(s) + access control(TEE)

NoC

Cache

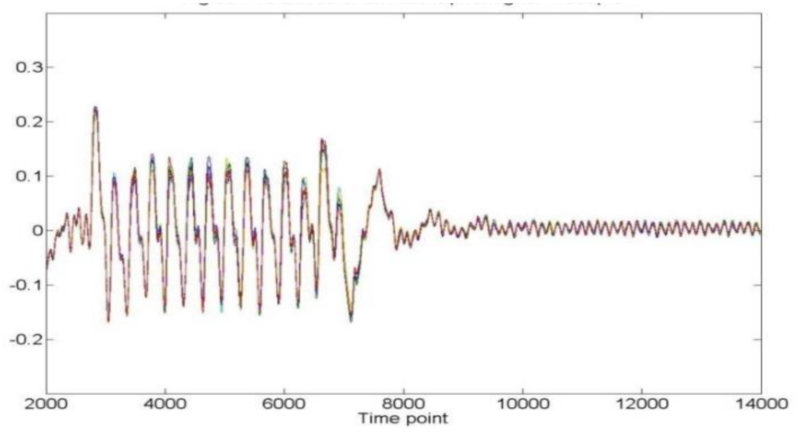
PE3

Vdd3, F3, Vbb3 island 3

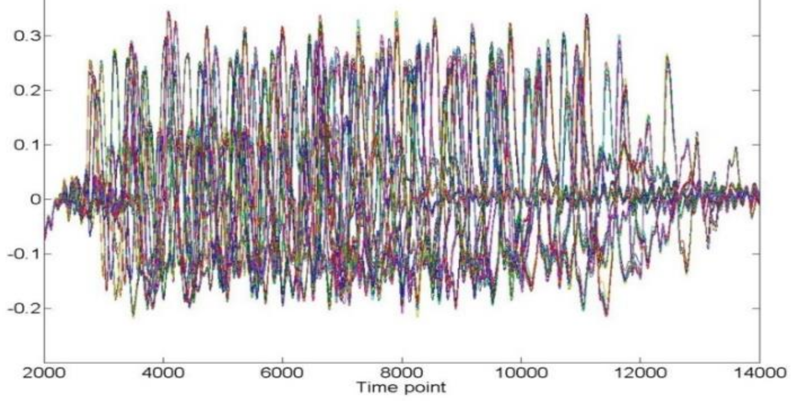
PE4

Vdd4, F4, V island 4

A single AES on FPGA ☹ (working at quite low frequency ; few couples {Vdd, F} avalaible)

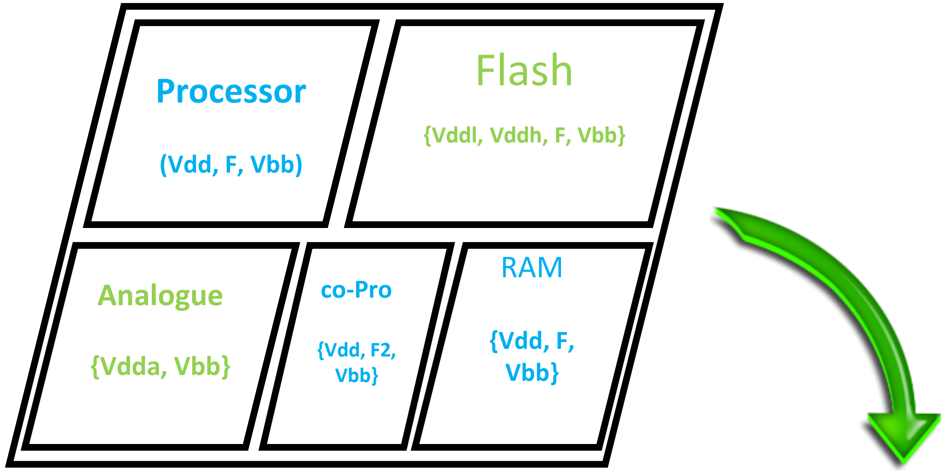


Vdd, F constant



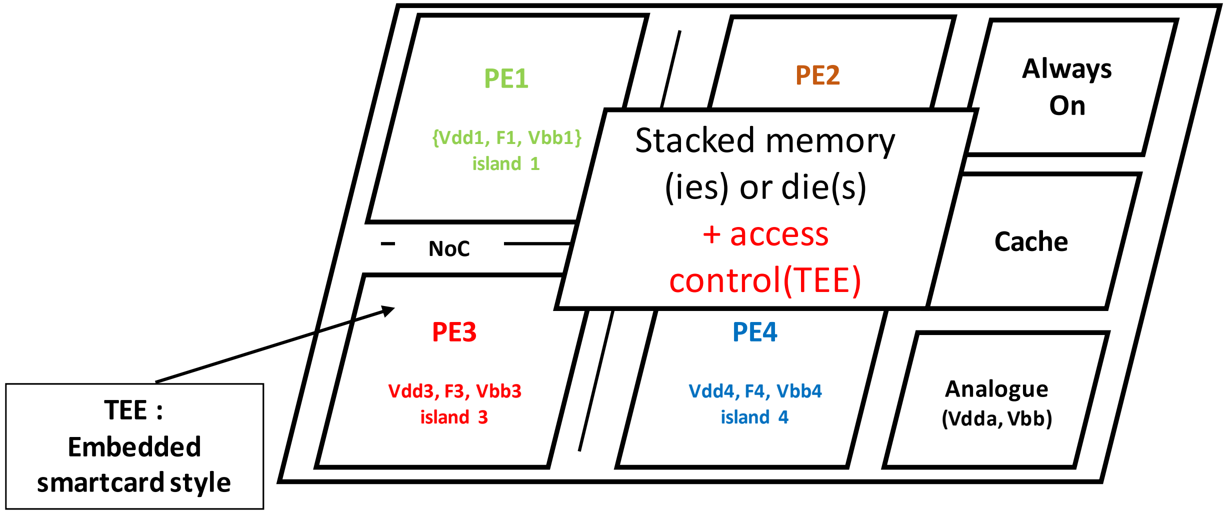
Varied Vdd, F

Adaptive designs (varying Vdd, F, CLK frequency) and Physical Attacks



Cryptographic algorithm execution parallelized on several potential asynchronous processing units working with:

- **Time varying clock frequency**
- **Time varying Vdd and body bias**



SCA Challenges :

Interpretability of traces (SPA) ?

Mixtures of leakages ?

Validity of HD and HW models ?

Alignment of traces ?

FA Challenges :

Synchronization of fault injection means ?

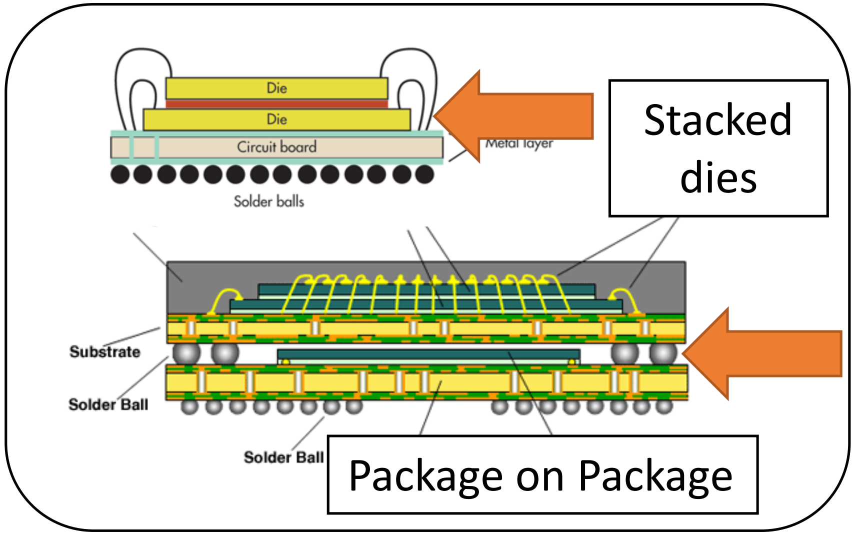
Problem to inject multiple faults ?

reproducibility of faults ?

3D Integration and Physical access

3D IC Packaging

In mass production

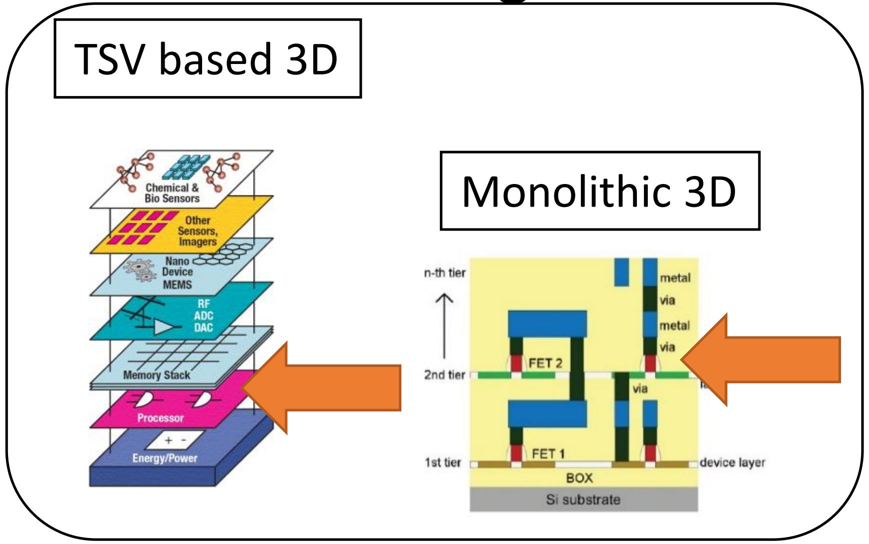


Stacked dies

Package on Package

3D IC Integration

Research aera



TSV based 3D

Monolithic 3D

Cryptographic blocks embedded in an IC enclosed between others ICs

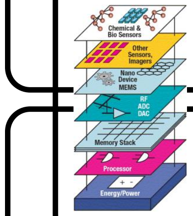
SCA Challenges :

Conducted leaking signal ?
SCA at board level ?
Alternative side channel ?
Dedicated equipment ?

FA Challenges :

De-assembly ?
New injection means ?
Conducted perturbations ?

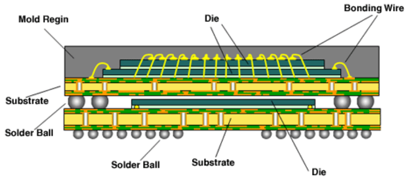
Adversary challenges ?

	Access to the device or leaking signals	CMOS scaling	Architecture and advanced design solutions	Die size and complexity	
	😉	😉	AVFS Multicores asynchrony 😟	😉	SCA
	😉	😉	AVFS Multicores asynchrony 😐	😉	FA
	 Chemical & Bio Sensors Other Sensors, Imagers Nano Device MEMS RF ADC DAC Memory Stack Processor Energy/Power 😟	😉	😟	😟	SCA
	😫	😉	😐	😫	FA

Adversary solutions ?

	Physical access to device or leaking signals	CMOS scaling	Architecture and advanced design solutions	Die size and complexity	
			Advanced SP, SCA Modelling		SCA
					FA
	Conducted leakage signals ? Jump in the fire !?		Advanced SP, SCA Modelling	Advanced SP, SCA Modelling, Reverse	SCA
	Conducted perturbations ? Jump in the fire !?			Advanced SP, SCA Reverse	FA

3D Integration and ~~Physical~~ access



Jump in the fire :

Get access to a SCA signal or inject faults through software routines or accessible and controllable hardware resources (cache, counters, embedded monitors …)

Known examples :

- Timing attaks
- RowHammer attacks

those attacks allows to circumvent the problem of identification of the hardware ressources and of getting access to sensitive computations.

Conclusion

Diversification of Integrated Systems processing sensitive data

- smartcards
- smartphones
- smart objects

Several challenges for adversaries related to:

- the scaling of smartcards
- the packaging of smart devices
- the complexity of smart devices

Increasing role of embedded software in attacks… to jump in the fire ! ??

‘In a sense’ … back 20 years before … to timing like attacks !