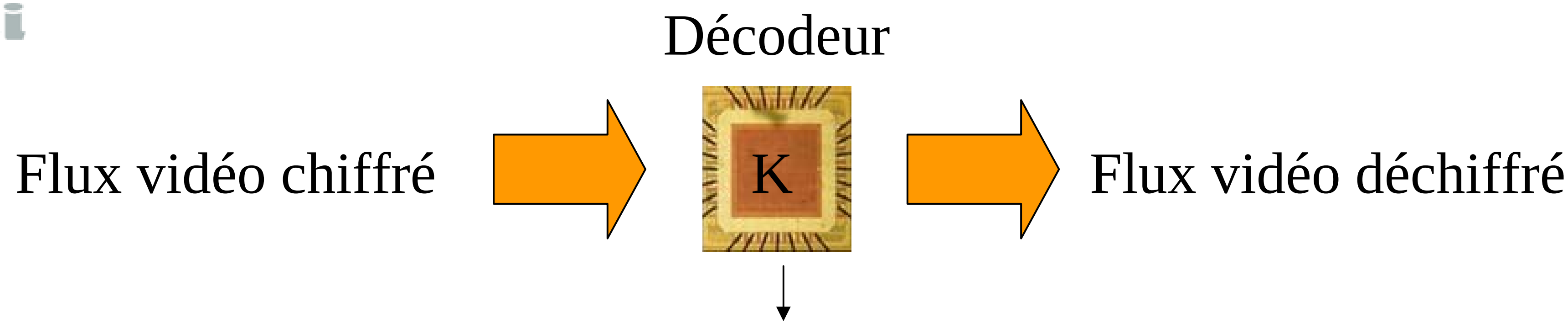
« Méthodologie de conception de circuits intégrés sécurisés»

Bruno ROBISSON
Assia TRIA

CEA-LETI/DCIS/SCME
Laboratoire de Conception de Circuits Sécurisés

SESAM Laboratory (joint R&D team CEA-LETI/EMSE),
Centre Microélectronique de Provence
Avenue des Anémones, 13541 Gardanne, France

Problématique



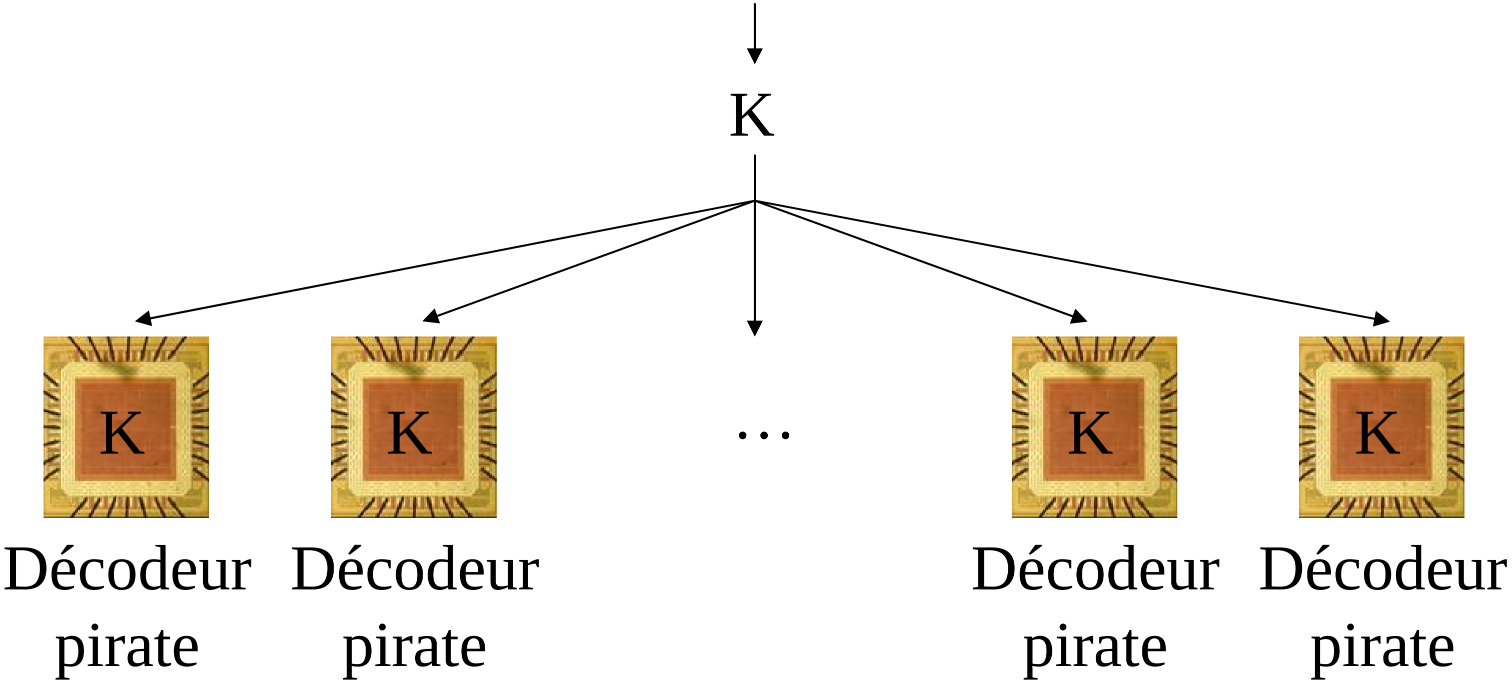
Décodeur

Flux vidéo chiffré

K

Flux vidéo déchiffré

« Attaque » = méthode permettant de récupérer les informations secrètes stockées dans les circuits intégrés



K

K

K

…

K

K

Décodeur pirate

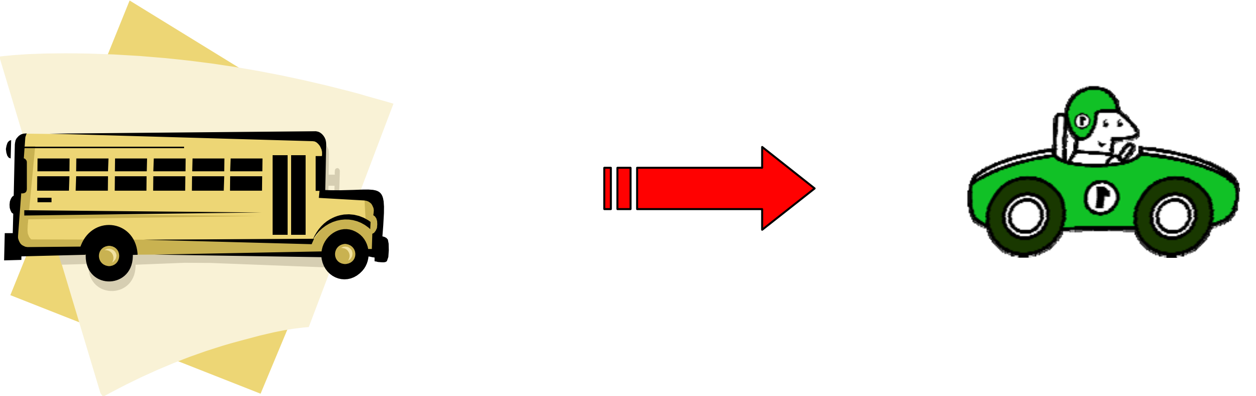
Décodeur pirate

Décodeur pirate

Décodeur pirate

Plan de la présentation

Attaques versus contre-mesures

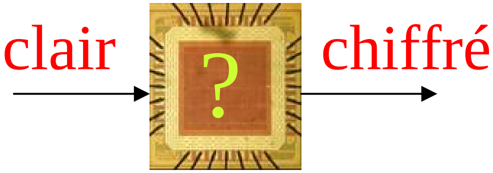


Sécuriser les circuits d'aujourd'hui

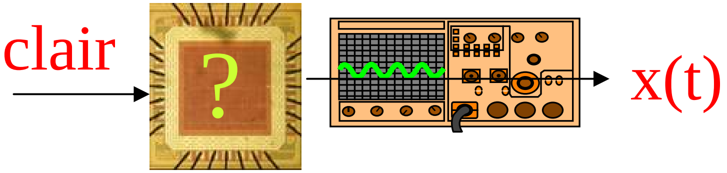
Sécuriser les circuits de demain

Attaques

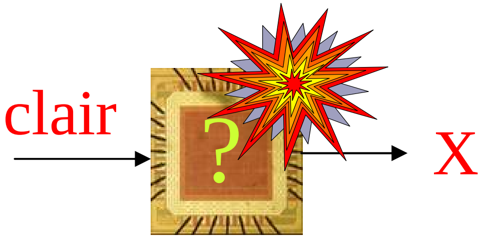
Cryptanalyse : analyse mathématique à partir des textes clairs et chiffrés



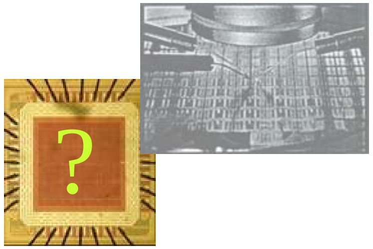
<u>Attaques en observation</u> : analyse des modifications de l’environnement induites par la puce lorsqu’elle manipule les données sensibles



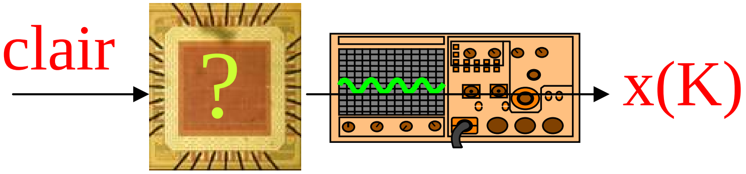
<u>Attaques en faute</u> : mise hors de conditions normales de fonctionnement de la puce pour contourner ses protections



<u>Attaques invasives</u> : récupération des signaux internes à la puce



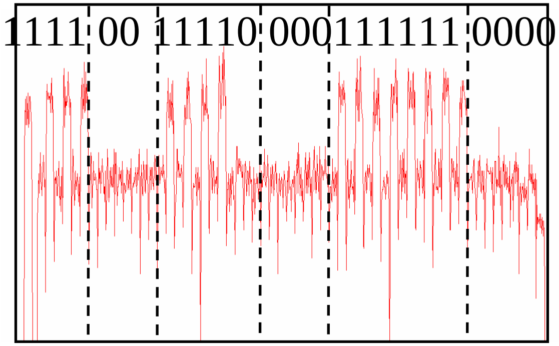
Attaques en observation



- Temps de calcul
- Puissance consommée
- Rayonnement électromagnétique

Simples (SPA) Différentielles (DPA)

K=



X(k)

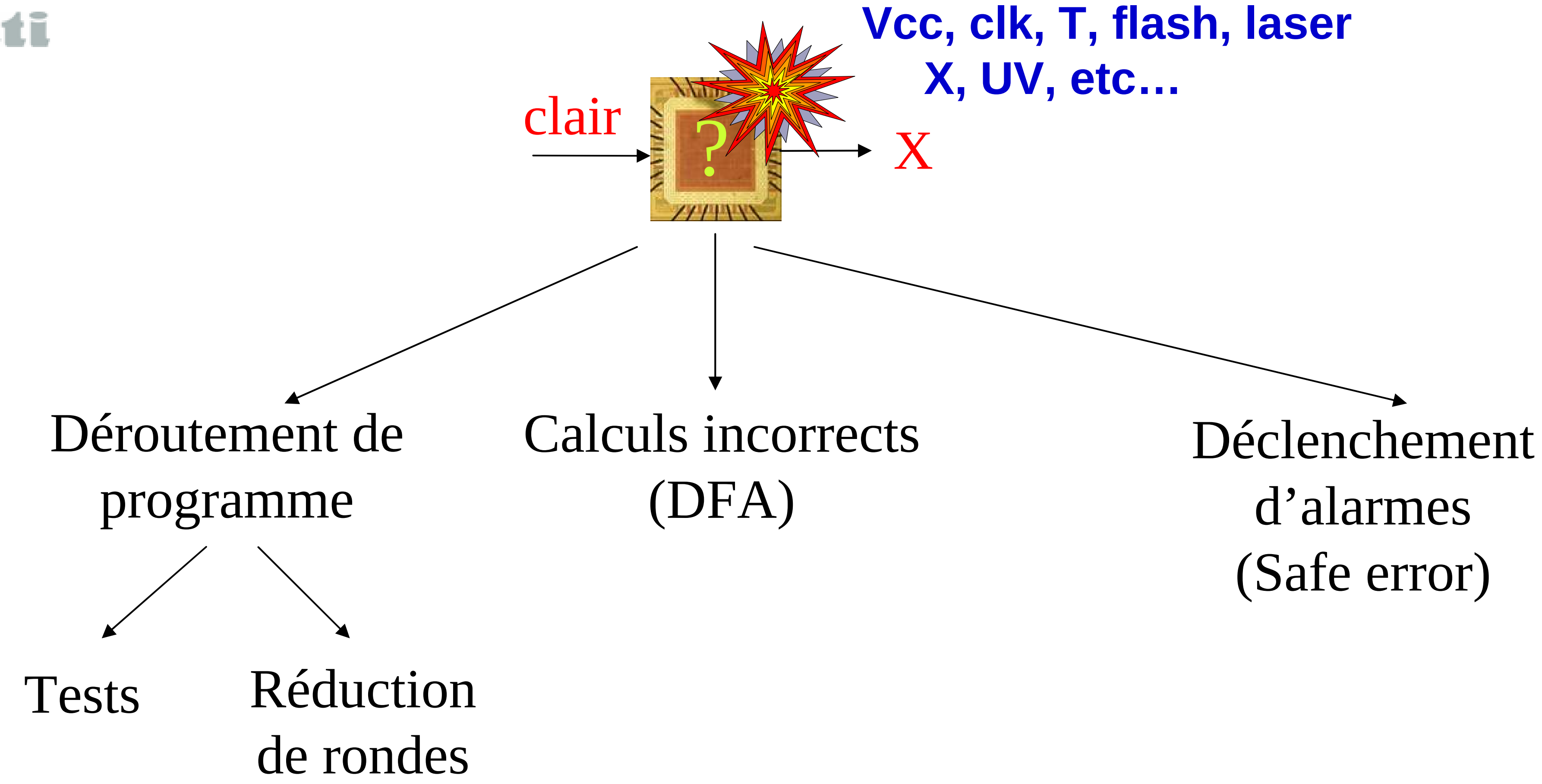
x(K)

Corr(X(k),x(K)) **max pour k=K**

Syndrome:

Le temps de calcul, la consommation, le rayonnement électromagnétique d'une puce est fonction de données qu'elle manipule

Attaques en faute



clair

?

X

Vcc, clk, T, flash, laser X, UV, etc…

Déroutement de programme

Tests

Réduction de rondes

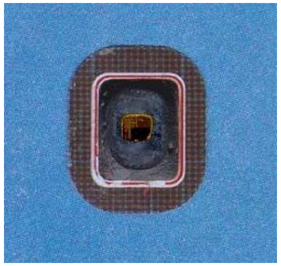
Calculs incorrects (DFA)

Déclenchement d'alarmes (Safe error)

Syndrome :

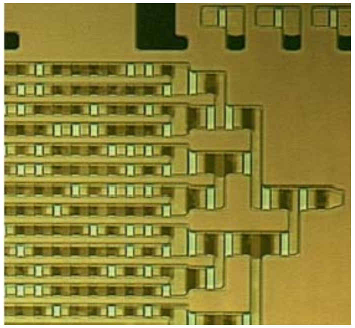
Le fonctionnement du circuit peut être perturbé par la modification de son environnement

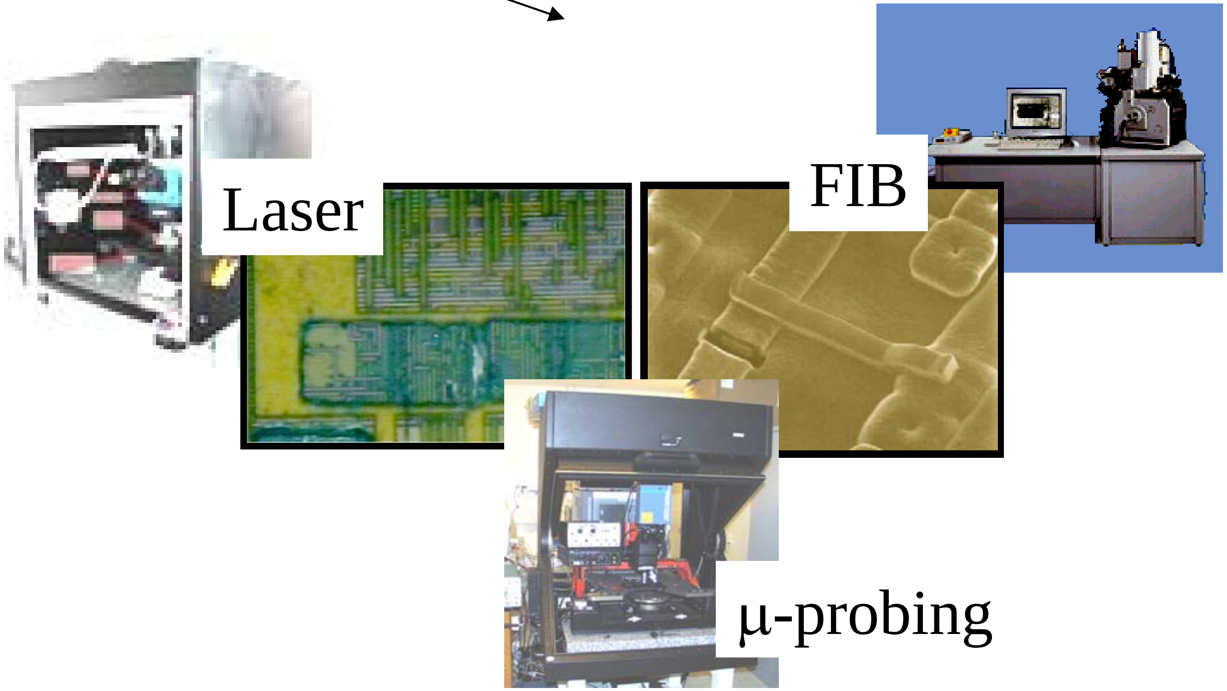
Attaques invasives



Passives

Actives

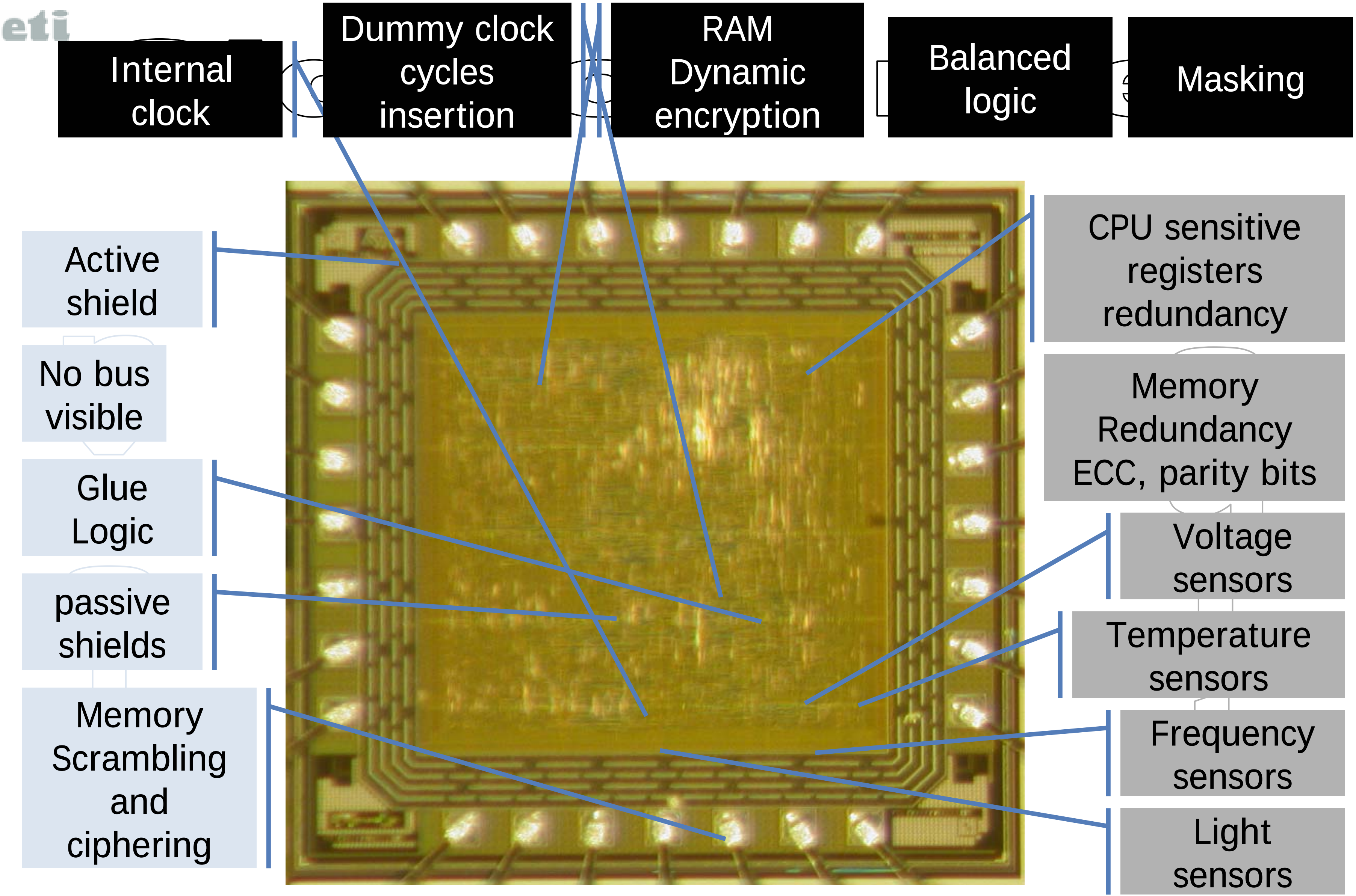




Syndrome :

Les calculs se font sur un composant intégré…

Chip security evolution:counter measures



Internal clock

Dummy clock cycles insertion

RAM Dynamic encryption

Balanced logic

Masking

Active shield

No bus visible

Glue Logic

passive shields

Memory Scrambling and ciphering

CPU sensitive registers redundancy

Memory Redundancy ECC, parity bits

Voltage sensors

Temperature sensors

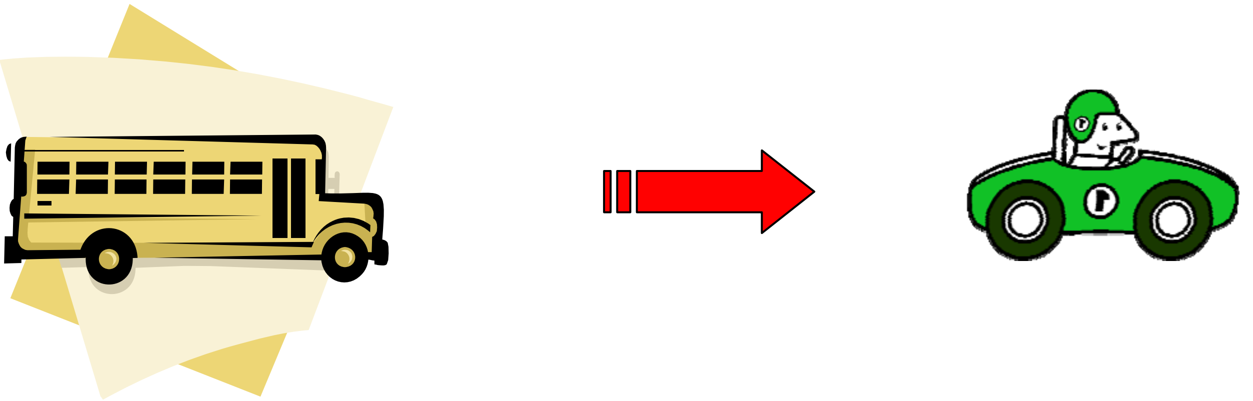
Frequency sensors

Light sensors

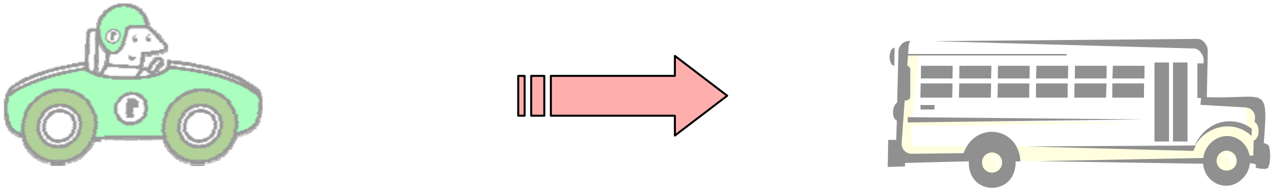
Plan de la présentation

Attaques versus contre-mesures

Sécuriser les circuits d’aujourd’hui



Sécuriser les circuits de demain



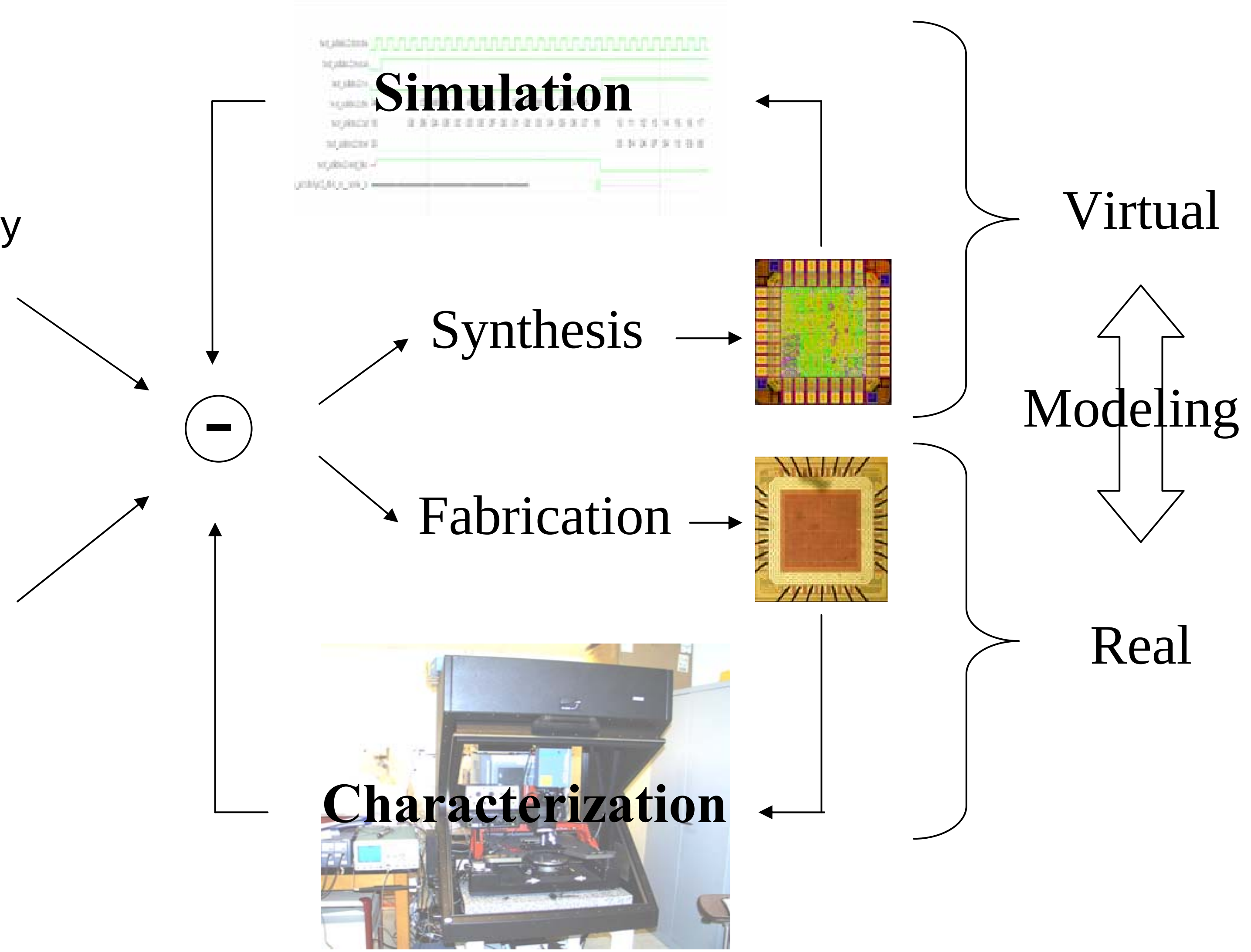
Integrated Circuit « Classical » Design Flow

Specifications:

- ✓ Fonctionnality
- ✓ Power,
- ✓ Speed,
- ✓ Price

Technology:

- ✓ CMOS
- ✓ SOI
- ✓ Molecular
- ✓…



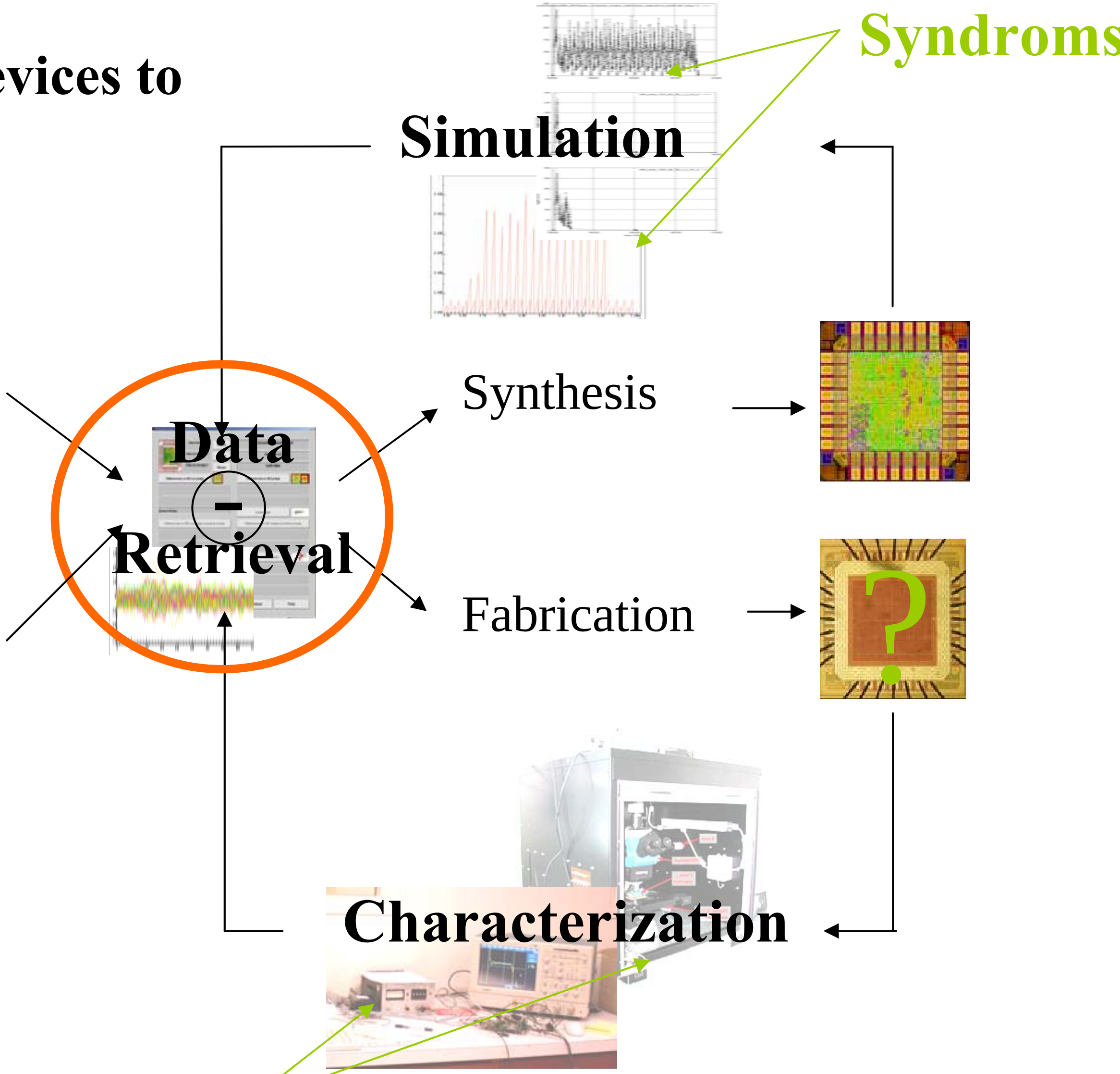
Securing today's devices

How to secure devices to known attacks?

<u>Specifications:</u>

X - resistance

<u>Technology</u>



Syndroms

Simulation

Data - Retrieval

Synthesis

Fabrication

?

Characterization

DFA and DPA test benches

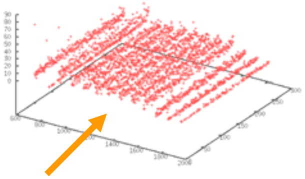
Example: Securing AES against DFA

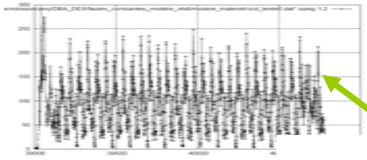
Specifications:

- DFA-resistant
- DPA-resistant

Technology:

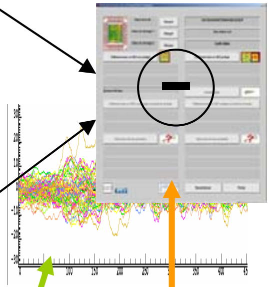
- CMOS

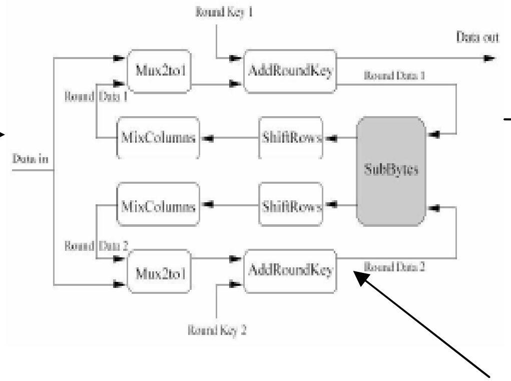


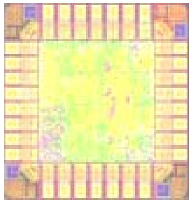


Commercial logic simulators

ad hoc and commercial power estimation tools







Matlab Implementation of main DFA

C Implementation of CPA/DPA

Error detection via spatial duplication

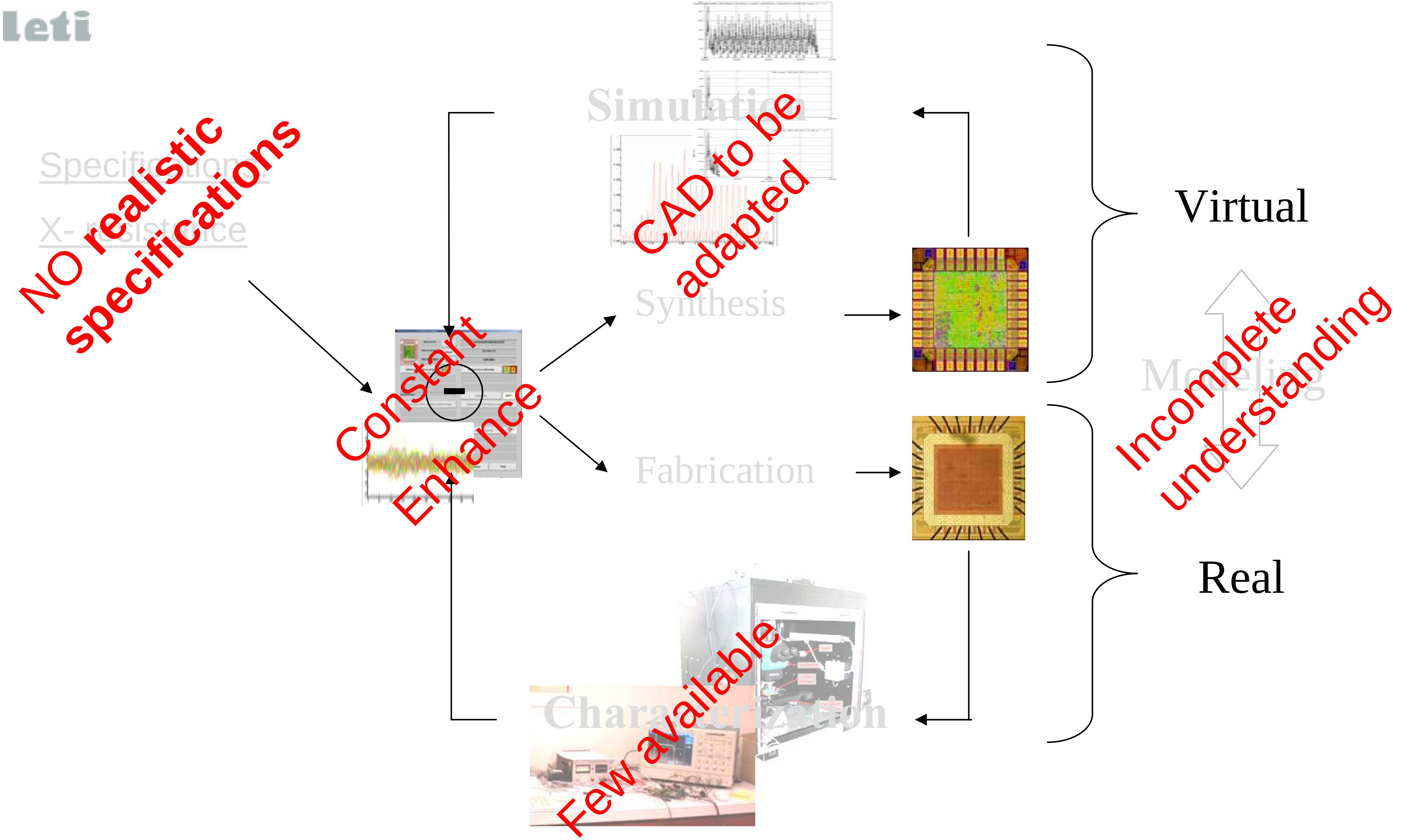
+ Error spreading

+ Balancing

Counter-measures validated

Detecting sensitivity to round reduction attacks

Securing today’s devices : the challenges



Specifications

X- resistance

Simulation

Synthesis

Fabrication

Characterization

Virtual

Modeling

Real

–

NO realistic specifications

CAD to be adapted

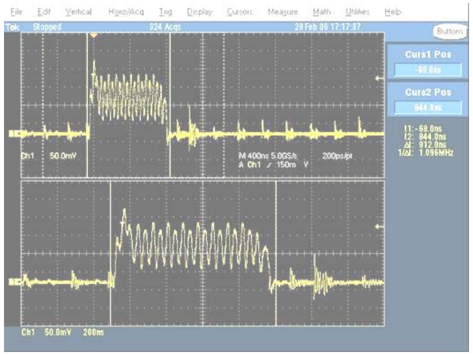
Constant Enhance

Incomplete understanding

Few available

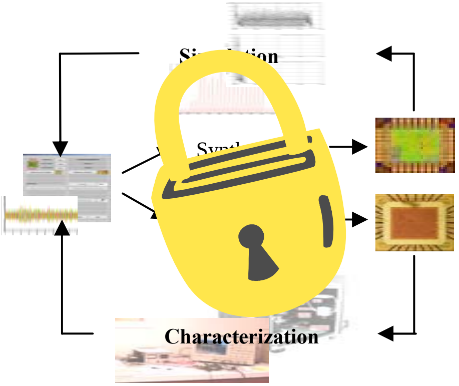
Securing today’s chip: Adressing the challenges

- Characterization
  - Sharing equipments
  - Publications should describe experimental protocols and equipments
  - Towards an *a minima* standardization of security measurments (devoted to R&D’s activities)



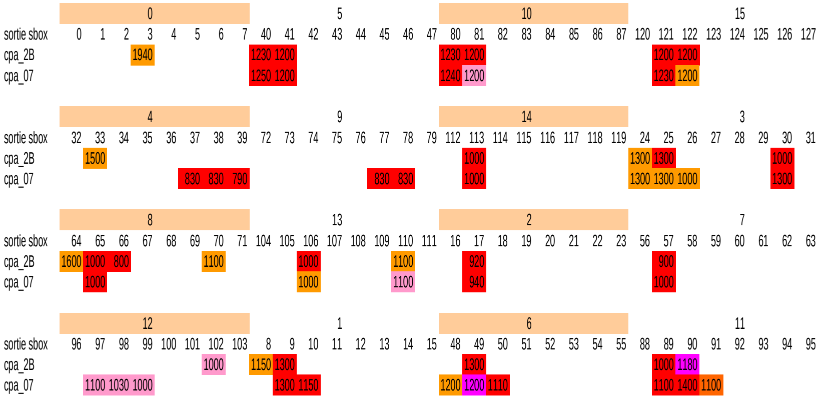
- Physics of attacks
  - Modeling physical phenomena which make attacks possible (faults, EM)
  - Dedicated test IC

- CAD tools to be adapted (simulation and synthesis)
  - Simulators should support models dedicated to security
  - Development of *ad hoc* verification tools (based on formal methods)
  - Formalization of security constraints
  - Towards automatic synthesis of circuits verifying such constraints



Securing today’s chip: Adressing the challenges

- Data retrieval
  - Data base of physical signals (power and EM waveforms, faulty executions traces)
  - Challenges from this data base to improve data retrieval algorithms
  - Open library of optimized cryptographic primitives (DPA, DFA and cryptanalysis)

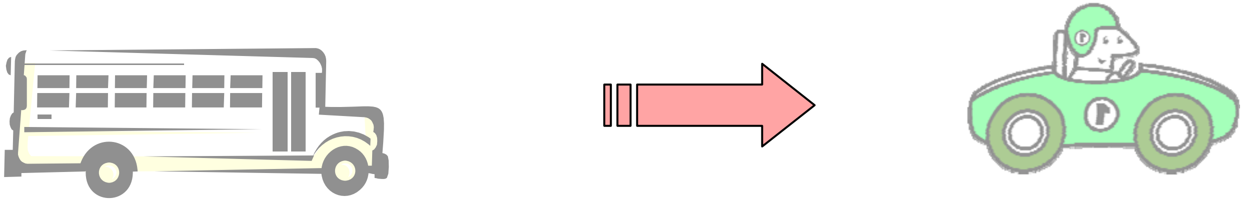


				0								5								10									15			
sortie sbox	0	1	2	3	4	5	6	7	40	41	42	43	44	45	46	47	80	81	82	83	84	85	86	87	120	121	122	123	124	125	126	127
cpa_2B				1940					1230	1200							1230	1200								1200	1200					
cpa_07									1250	1200							1240	1200								1230	1200					
				4								9								14									3			
sortie sbox	32	33	34	35	36	37	38	39	72	73	74	75	76	77	78	79	112	113	114	115	116	117	118	119	24	25	26	27	28	29	30	31
cpa_2B		1500																1000							1300	1300					1000	
cpa_07						830	830	790						830	830			1000							1300	1300	1000				1300	
				8								13								2									7			
sortie sbox	64	65	66	67	68	69	70	71	104	105	106	107	108	109	110	111	16	17	18	19	20	21	22	23	56	57	58	59	60	61	62	63
cpa_2B	1600	1000	800				1100				1000				1100			920								900						
cpa_07		1000									1000				1100			940								1000						
				12								1								6									11			
sortie sbox	96	97	98	99	100	101	102	103	8	9	10	11	12	13	14	15	48	49	50	51	52	53	54	55	88	89	90	91	92	93	94	95
cpa_2B							1000		1150	1300								1300								1000	1180					
cpa_07		1100	1030	1000						1300	1150						1200	1200	1110							1100	1400	1100				

- Specifications
  - Take care of « naive » counter-measures
  - Take into account all the known attacks
  - Always test counter-measures on real devices

Plan de la présentation

Attaques versus contre-mesures

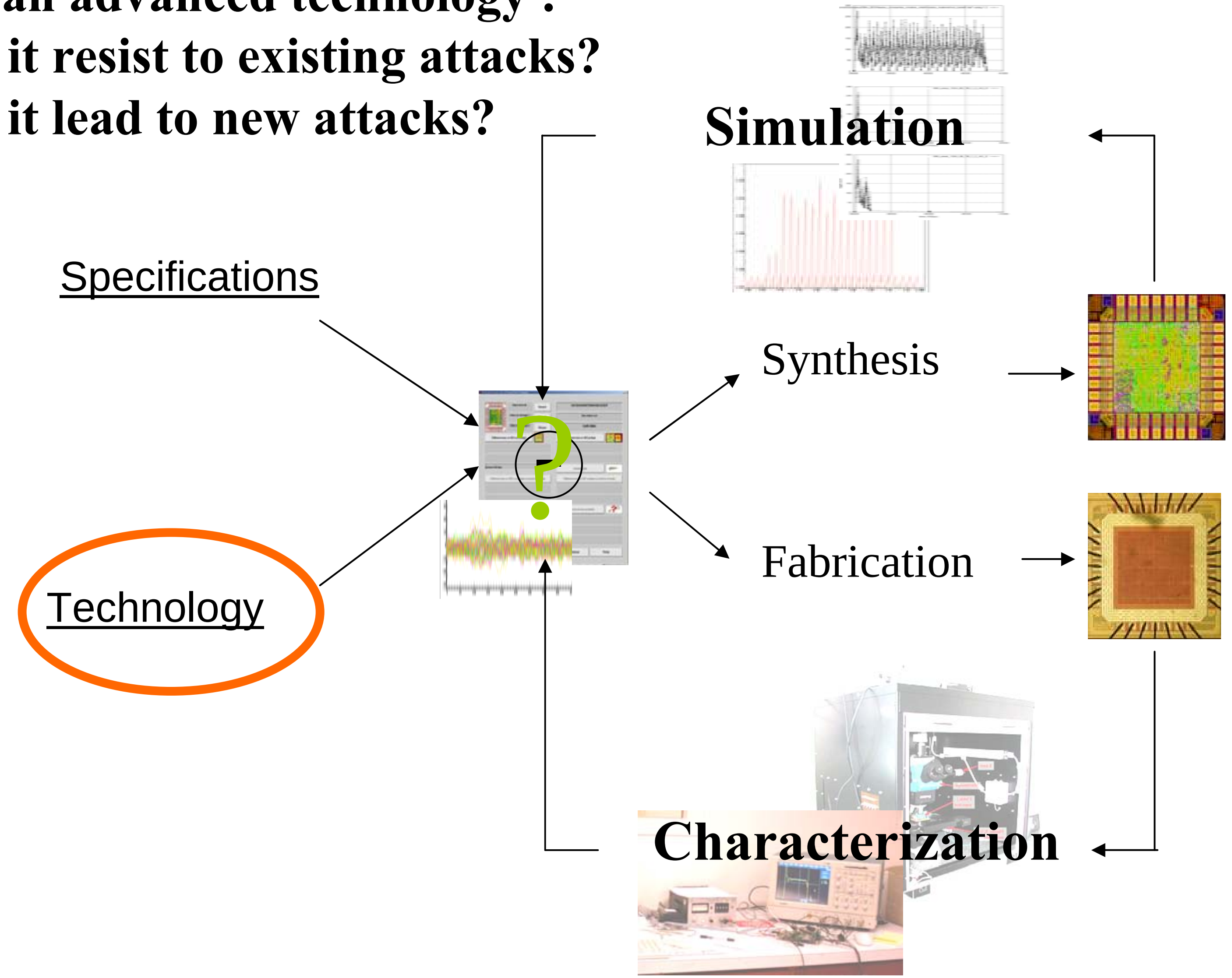


Sécuriser les circuits d’aujourd’hui

Sécuriser les circuits de demain

Securing tomorrow’s devices

Given an advanced technology :
- **Will it resist to existing attacks?**
- **Will it lead to new attacks?**



Simulation

Specifications

Technology

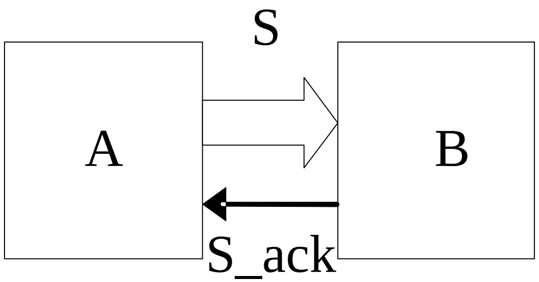
?

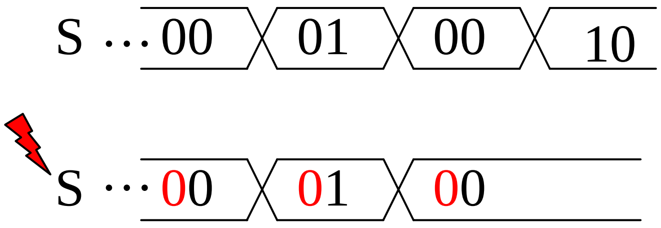
Synthesis

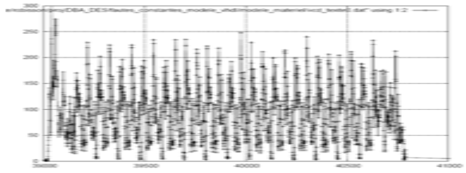
Fabrication

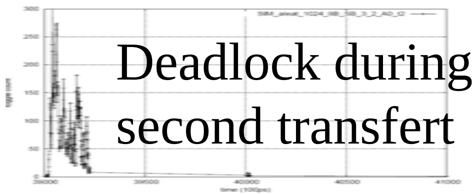
Characterization

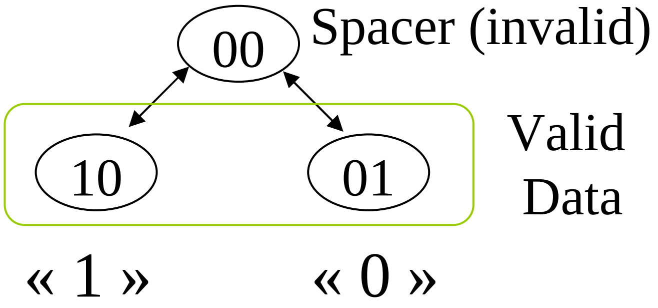
Example: QDI asynchronous circuit

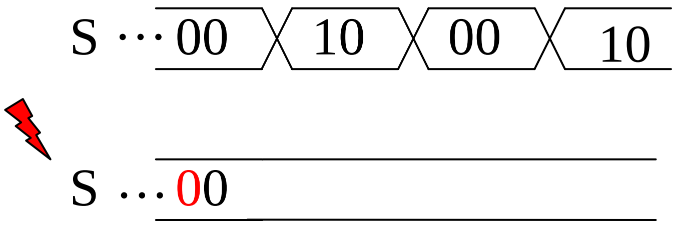


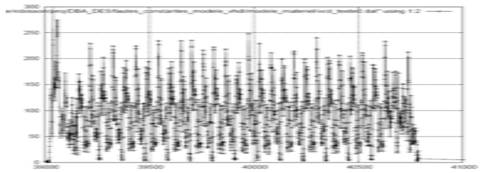


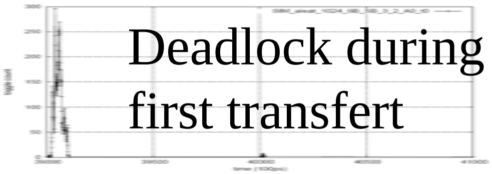



Deadlock during second transfert








Deadlock during first transfert

- Permanent « stuck-at zero » on a wire of a dual rail may induce deadlock
- Deadlock instants depend on the data values
- Deadlock instants may be easily detected by monitoring the power consumption

DBA principles

Safe-error

Key bits leak only through the information whether the device has a normal **behavior** or not in presence of fault

+ DPA

Correlating a power model parameterized by the value of a small number of bits of the key (the partial key) to power measurments

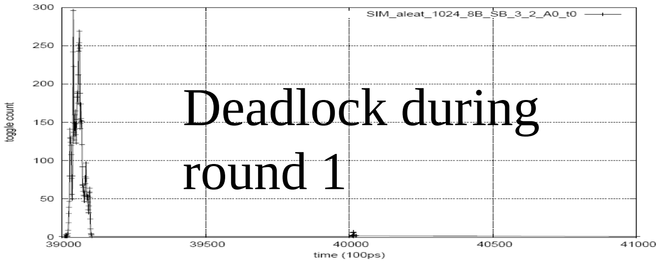
---

Differential **B**ehavioral **A**nalysis

Correlating a functional model parameterized by the value of a partial key to **behaviors** of the device in presence of faults

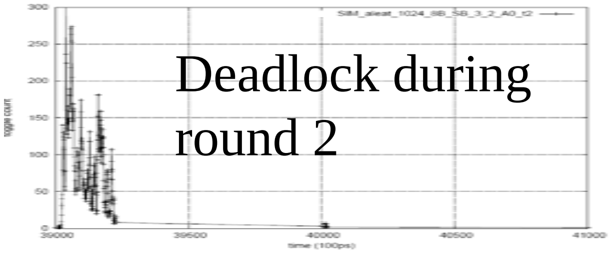
DBA hypothesis

- DPA hypothesis
  - Known cryptographic algorithms,
  - Known plain texts (or cipher texts)
  - There must exist intermediate variables that can be expressed as functions depending on the plain texts and on only a small number of key bits
- Fault injection
  - Type : Stuck-at zero (or one)
  - Location : On one bit in the set of the attack bits defined in DPA
  - Duration : Permanent (or transient)
  - Repetitivity : Same fault, at same time, on same bit
- Detecting behavior between faults which create an error during round one or during another round



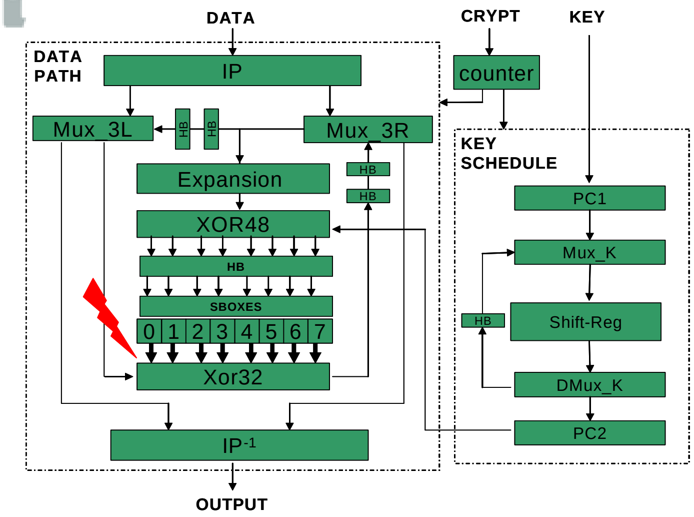
Deadlock during round 1

≠



Deadlock during round 2

DBA on a QDI asynchronous DES



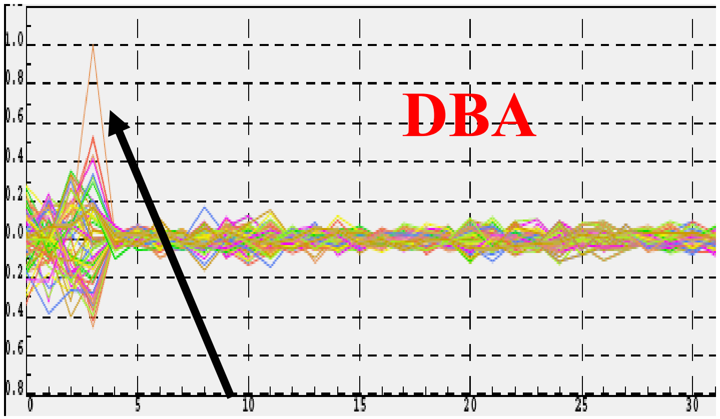
Design

QDI asynchronous DES
DPA counter-measures (logical balancing)
Standard cells
0.13 µm STMicroelectronics
180 ns for DES encryption
0.94mm^2 with interfaces

Faults injected on a bit at the output of the Sboxes

15 faulty executions with random values but known plain texts

Simulation

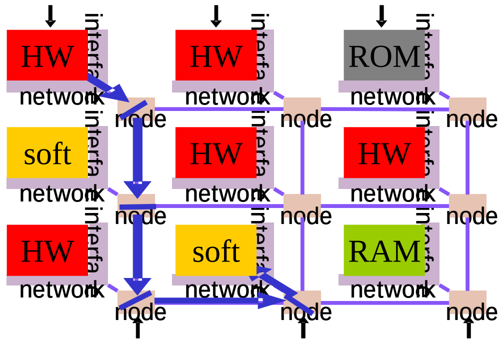


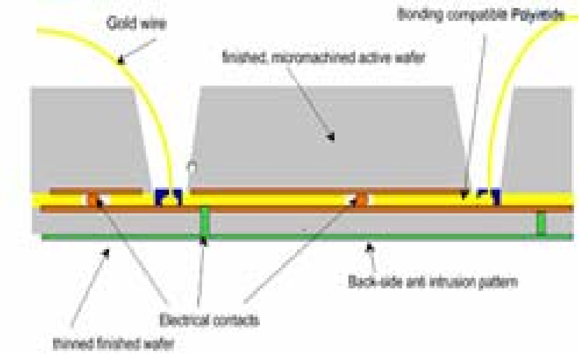
DBA

Value of the partial key (6 bit long)
Location of the faulty bit
Value of the faulty bit
Repetitivity of the fault injection

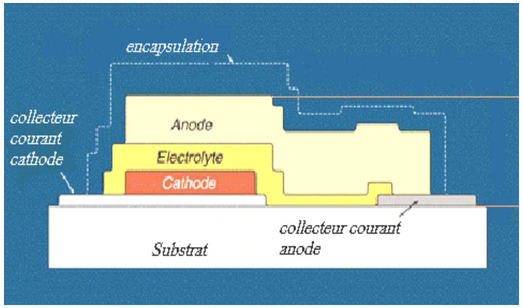
Securing tomorrow's chip

- Evaluate advanced architectures
  - Asynchronous circuits, GALS
  - Reconfigurable devices
  - SOC, NOC
  - …




Gold wire
Bonding compatible Polyimide
finished, micromachined active wafer
Back-side anti intrusion pattern
Electrical contacts
thinned finished wafer

- Evaluate advanced technologies
  - SOI
  - Memories MRAM
  - Technology shrinking
  - Nano-technologies
  - Above-IC power sources
  - Smart packaging
  - …



- Anticipate attacker's means
  - Equipments
  - Towards hybrid attacks

Conclusion

- A lot of work…

- Towards a more collaborative approach
  - Sharing some competences and equipments
  - Objective comparison of counter-measures

- But with incorporate industrial constraints
  - Fears and secrets around cryptographic developments
  - Time and cost constraints