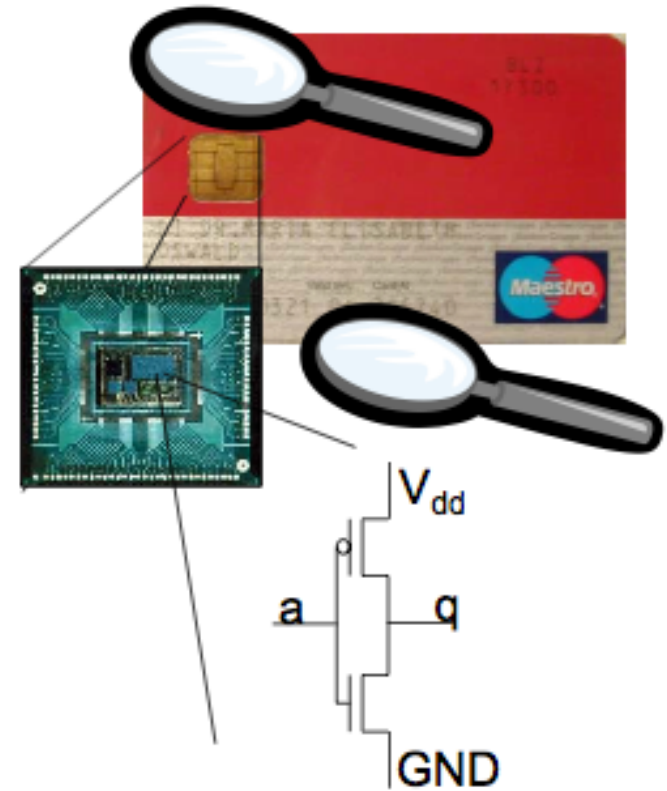


Les attaques

Physical Attacks : Principles

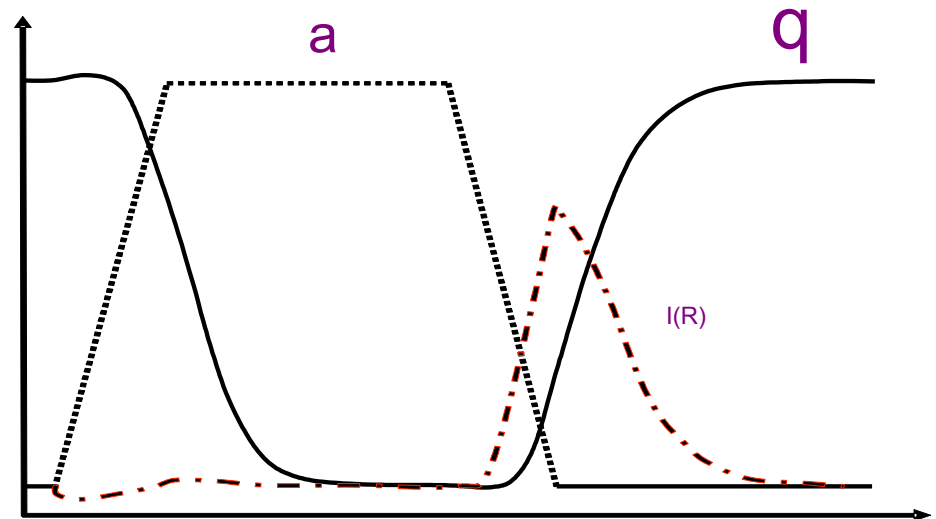
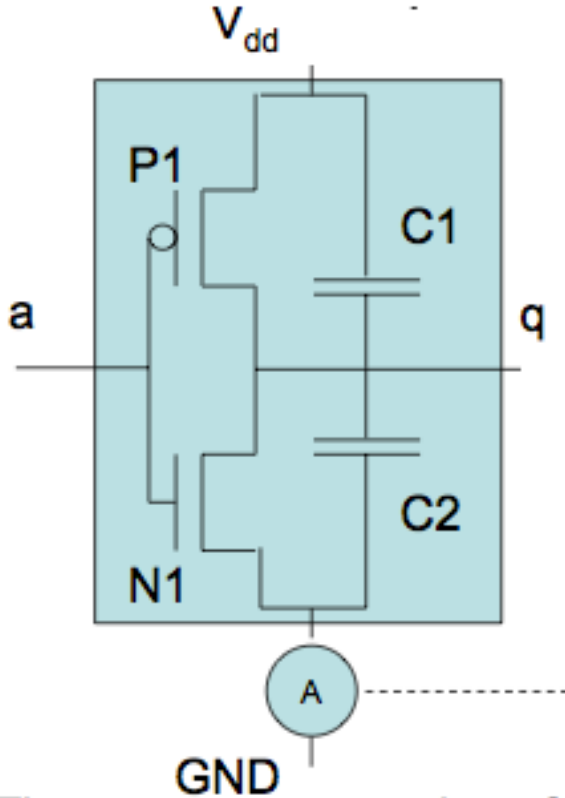
CMOS technology is the predominant technology for (cryptographic) devices

Power analysis attacks exploit the fact that the instantaneous power consumption of a device built in CMOS technology depends on the data it processes and the operations it performs.



CMOS Inverter

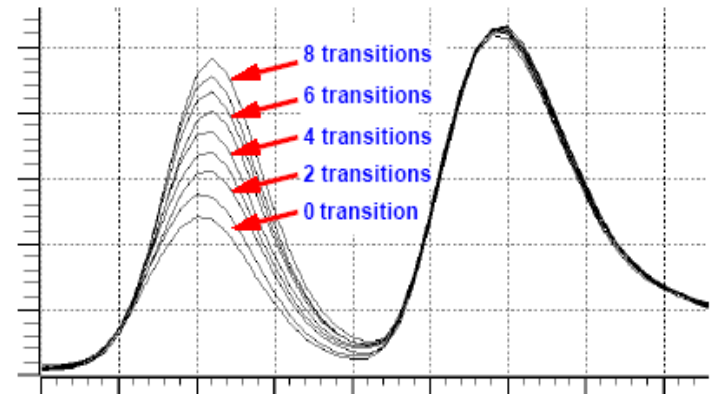
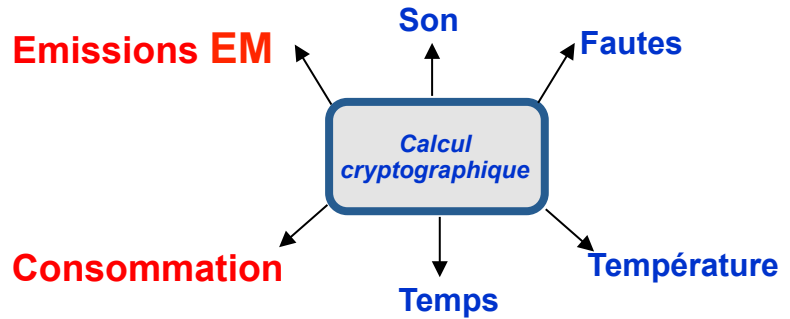
Physical Attacks : Principles

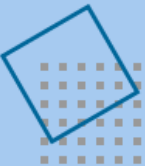


- The power consumption of a CMOS gate depends on the data:
 - q: 0→0 virtually no power cons.
 - q: 1→1 virtually no power cons.
 - q: 0→1 high power cons. (proportional to C2)
 - q: 1→0 high power cons. (proportional to C1)

Physical Attacks : Principles

- **Invasives Attacks**
 - Reverse engineering
 - Microprobing
- **Semi invasives Attacks**
 - Fault-Injection
 - Microscopy
 - Light Emission
- **Non-invasive Attacks**
 - Timing
 - Simple Power Analysis (SPA)
 - Differential Power Analysis (DPA)
 - Electromagnetic
 - Single Electromagnetic Attack (SEMA)
 - Differential Electromagnetic Attack (DEMA)
 - Sound





Les attaques matérielles

LES ATTAQUES MATÉRIELLES

INVASIVES

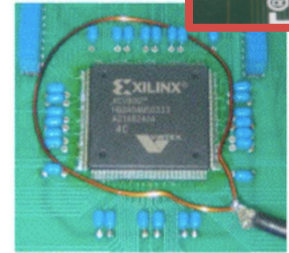
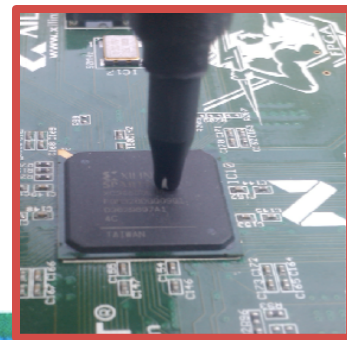
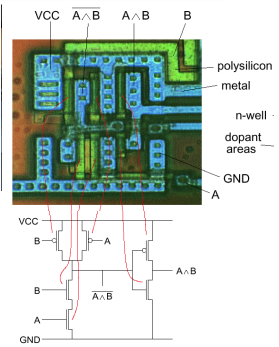
- **décapsulation** + contact CI
- **Ingénierie inverse** possible
- **Coût** de l'attaque : **élevé**

SEMI INVASIVES

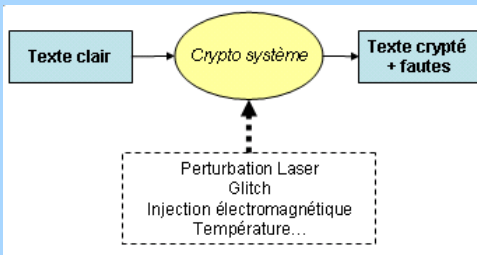
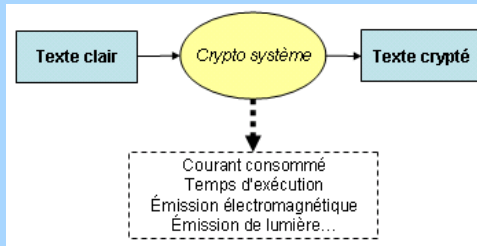
- **Décapsulation** sans contact CI
- Attaque par **laser** possible (amincis.)
- **Coût** de l'attaque : **moyen**

NON INVASIVES

- **sans décapsulation**
- difficiles à détecter (**mesures EM**)
- nécessitent beaucoup de mesures
- **Coût** de l'attaque : **réduit**



Les attaques matérielles : principes



Attaques non-invasives

Canaux auxiliaires

Fautes / glitch

Force brute

Attaques semi-invasives

Fautes laser

Sondage laser

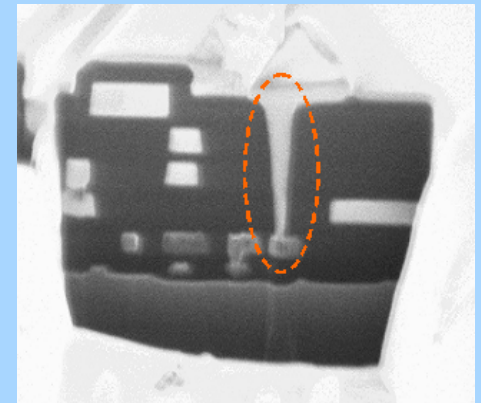
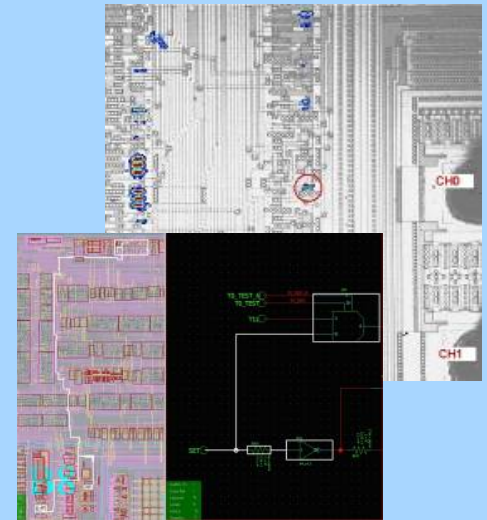
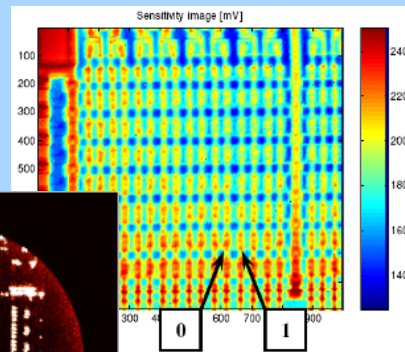
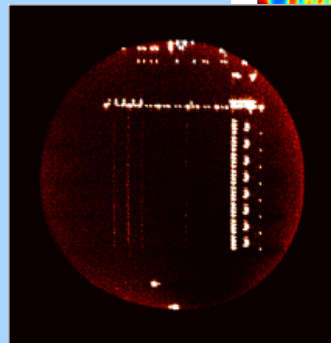
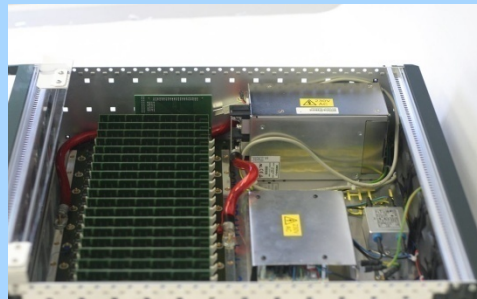
Emission de lumière

Attaques invasives

Reverse engineering

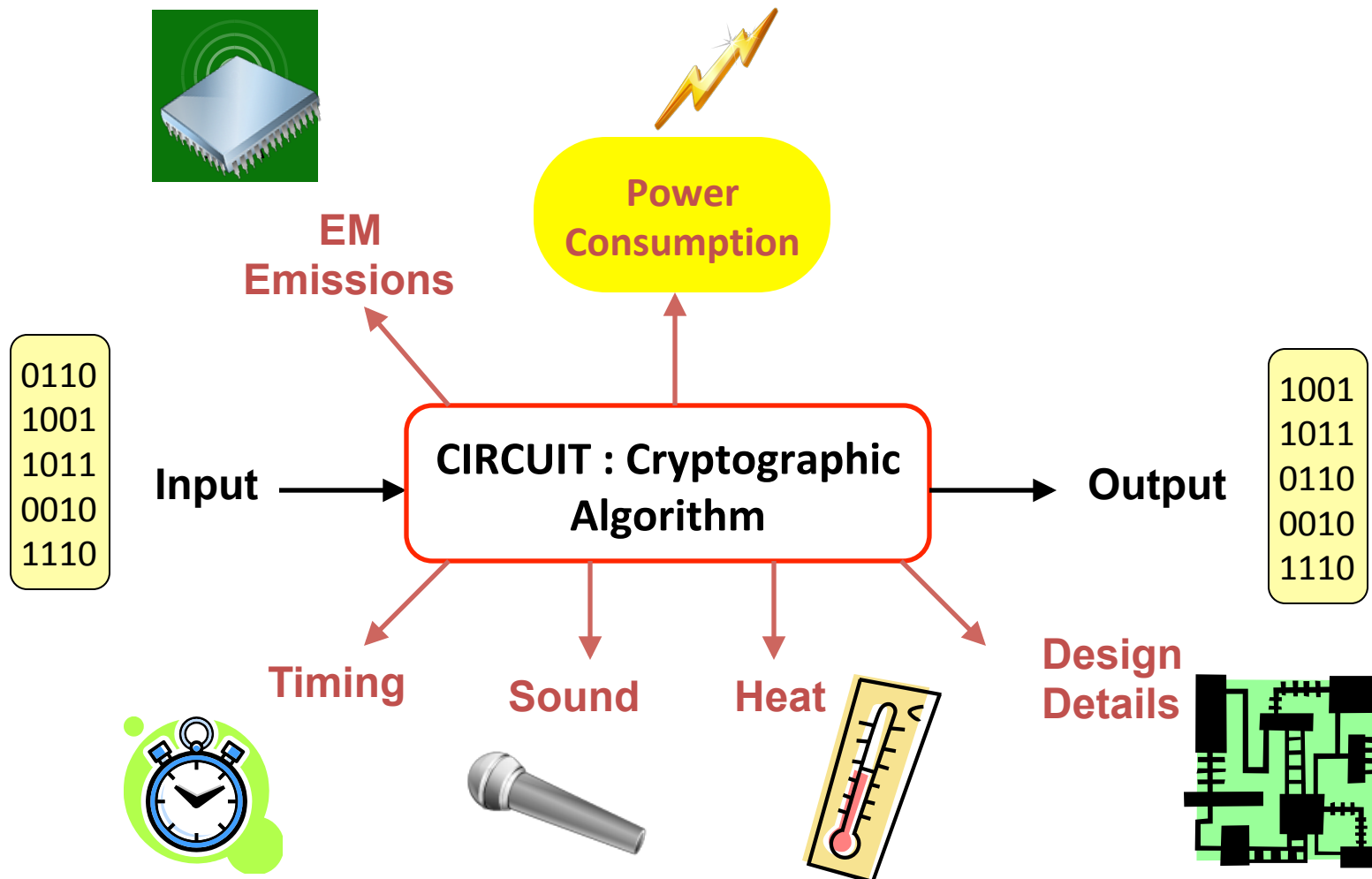
Attaque en « probing »

FIB

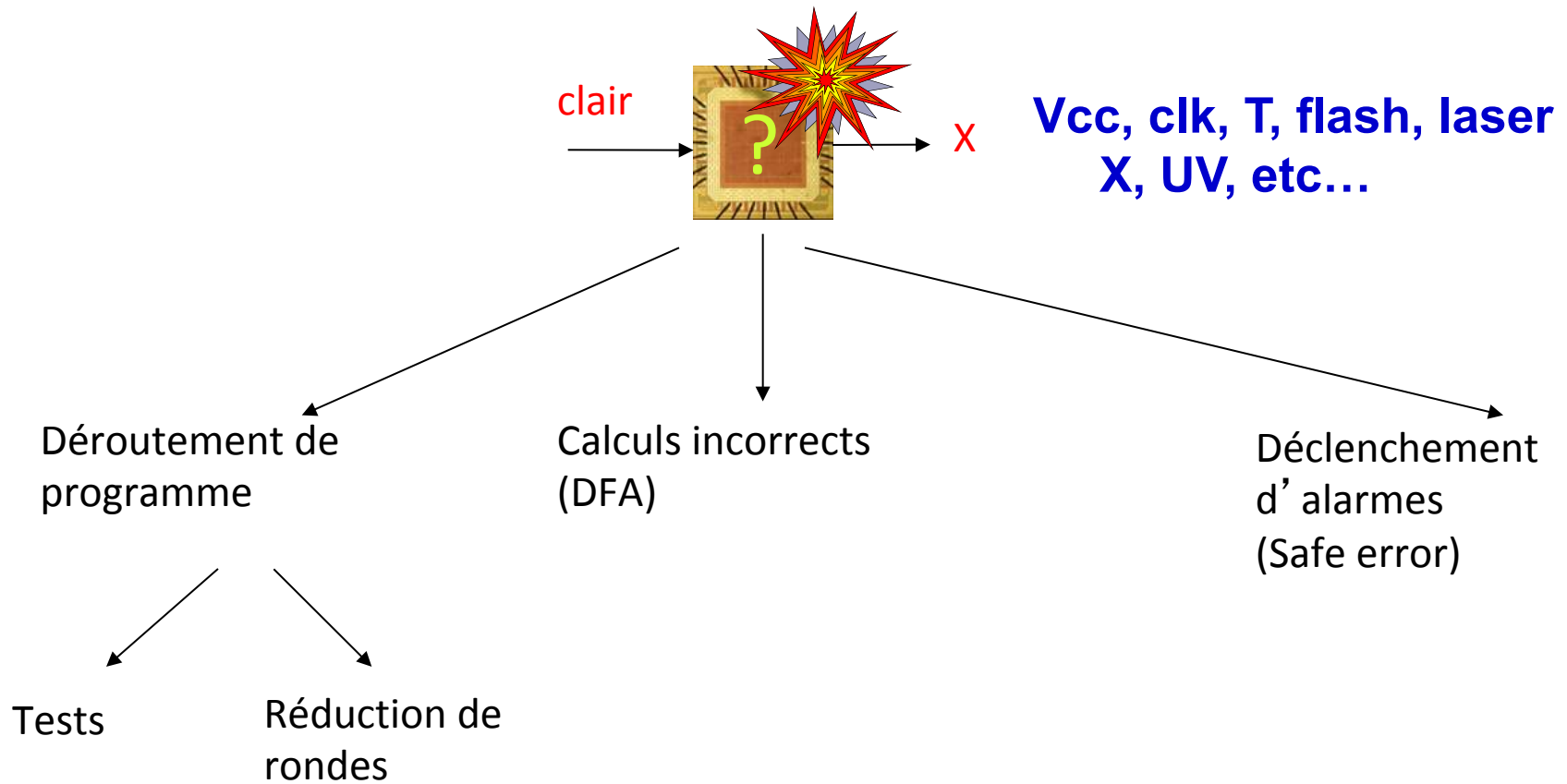


Side-Channel Attacks

Attaques par canaux cachés



Attaques en faute



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