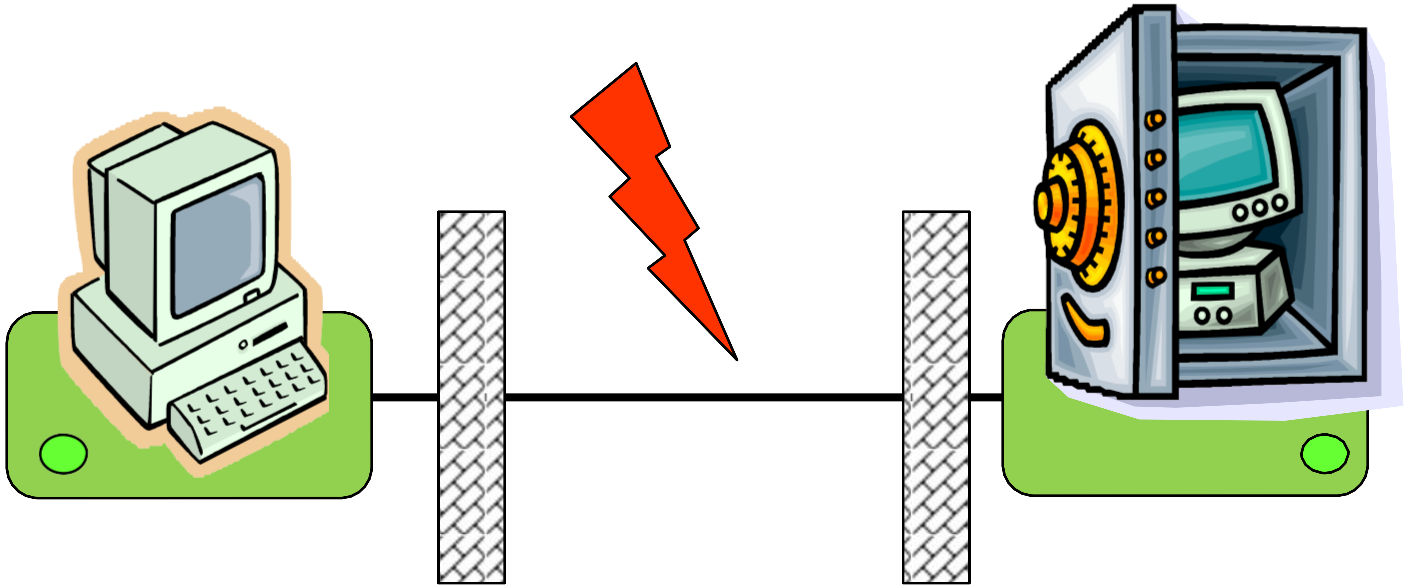
Chapter 8

Side Channel Attacks and Countermeasures

Introduction

- Classic cryptography views the secure problems with mathematical abstractions
- The classic cryptanalysis has had a great success and promise
  - Analyzing and quantifying crypto algorithms' resilience against attacks
- Recently, many of the security protocols have been attacked through physical attacks
  - Exploit weaknesses in the cryptographic system hardware implementation aimed to recover the secret parameters

Traditional Model (simplified view)



- Attack on channel between communicating parties
- Encryption and cryptographic operations in **black boxes**
- Protection by strong mathematic algorithms and protocols
- Computationally secure

Embedded Cryptographic Devices

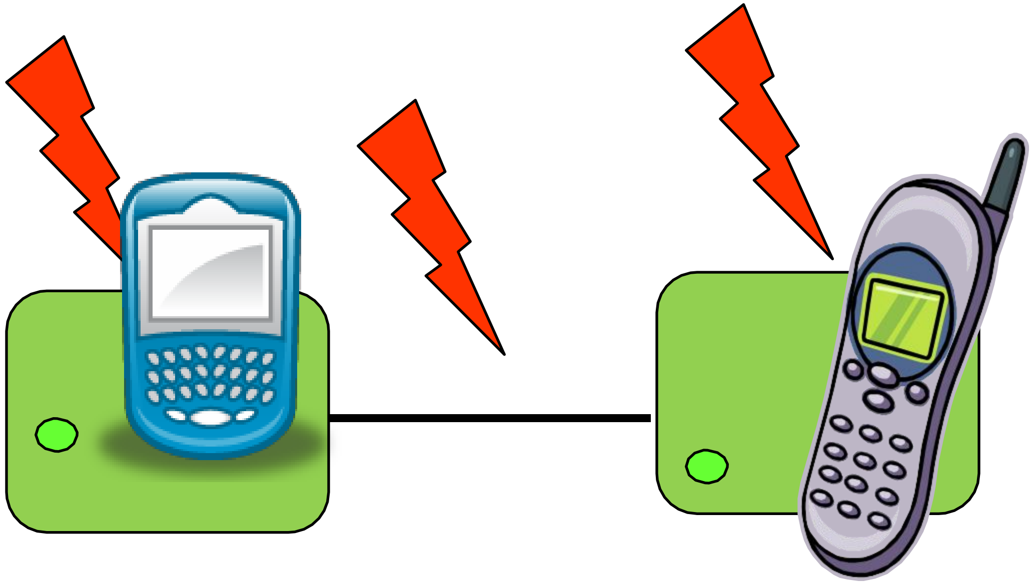
- A *cryptographic device* is an electronic device that implements a cryptographic algorithm and stores a cryptographic key. It is capable of performing cryptographic operations using that key.

IDENTIFICATION PAYMENT COMMUNICATION MULTIMEDIA

…

- *Embedded*: it is exposed to adversaries in a hostile environment; full physical access, no time constraints
  - Remark: the adversary might be a legitimate user!

How is Embedded Security Affected?



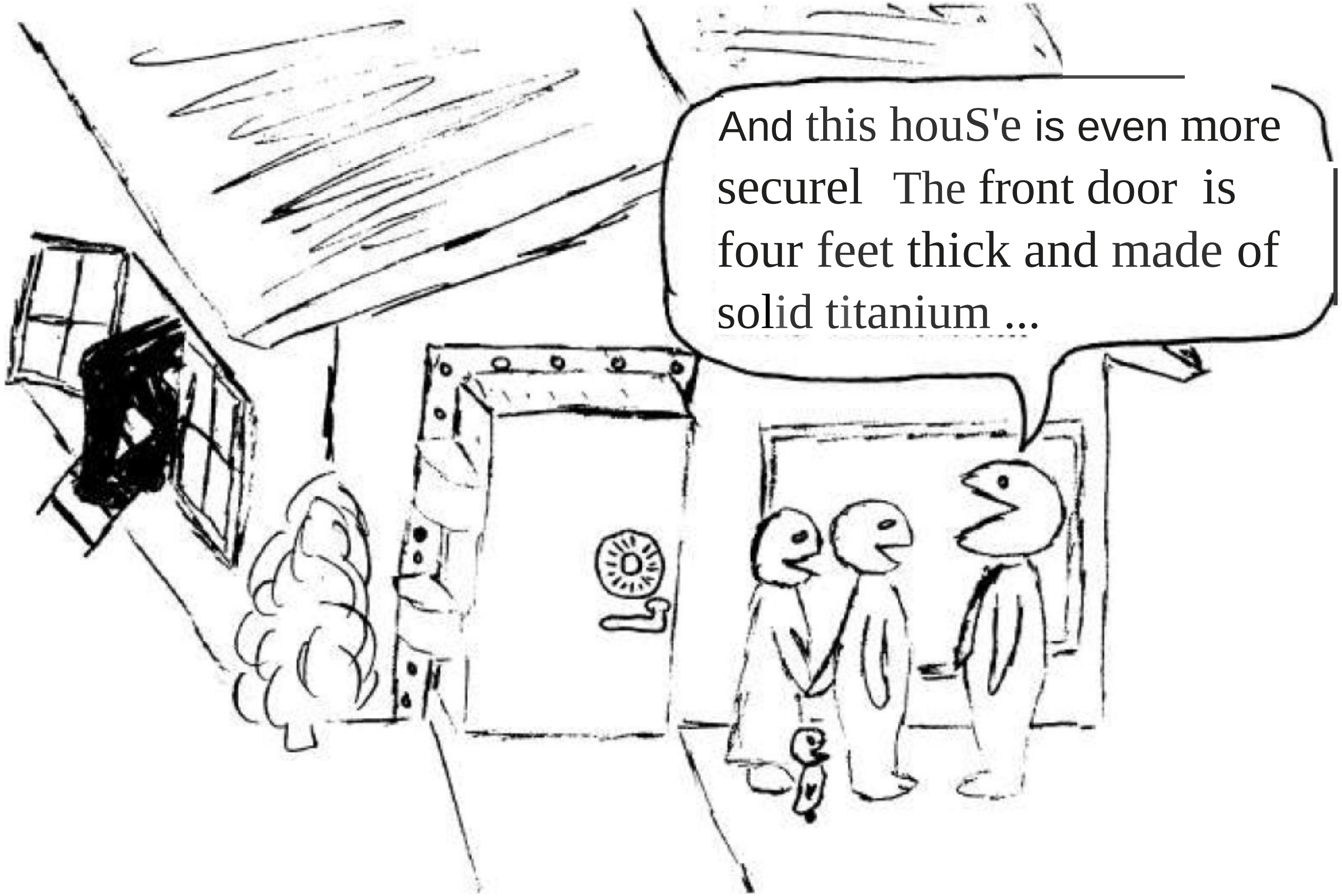
- New Model (also simplified view):
  - Attack on channel and endpoints
  - Encryption and cryptographic operations in **gray boxes**
  - Protection by strong mathematic algorithms and protocols
  - **Protection by secure implementation**

- ***Need secure implementations not only algorithms***

Keep in Mind

A system is as secure as its weakest link

A system is as secure as its weakest link



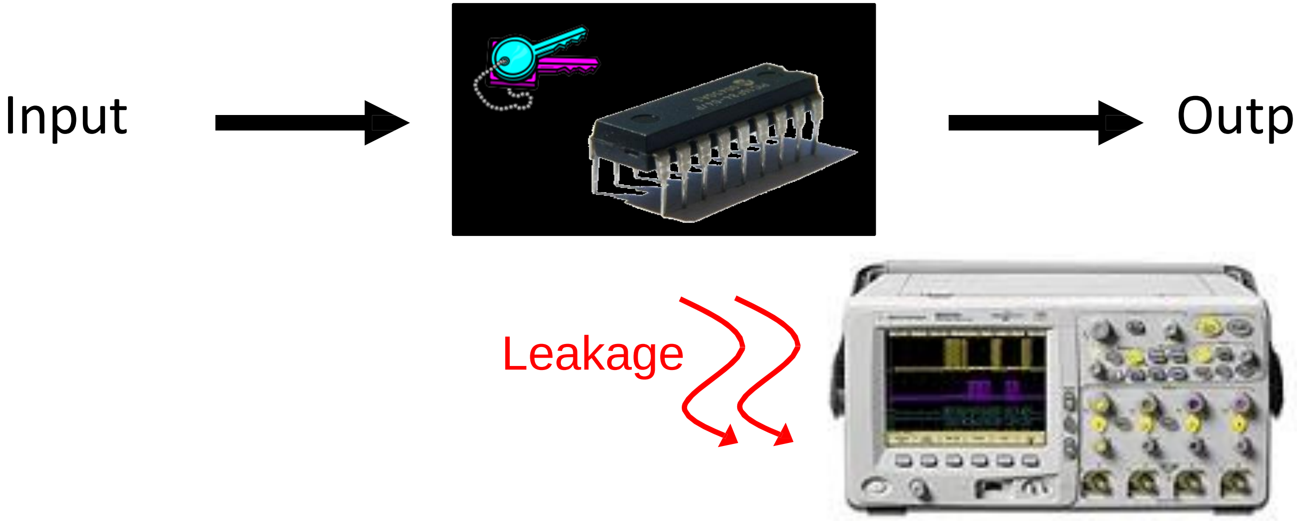
source: Paul Kocher

Side-Channel Leakage

Physical attacks ≠ Cryptanalysis

(gray box, physics) (black box, maths)

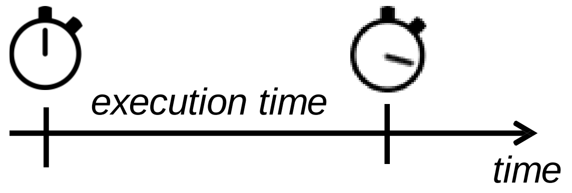
- Does not tackle the algorithm's math



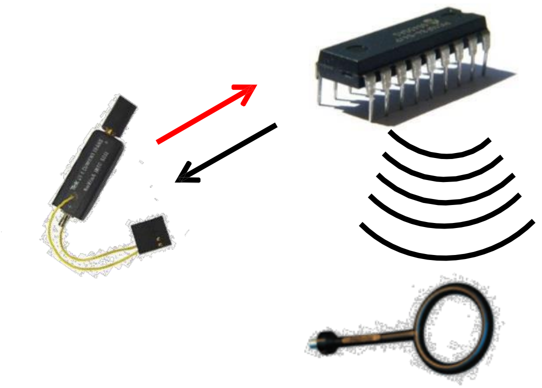
- Observe physical quantities in the device's vincinity and use additional information during cryptanalysis

Some Side-Channels (not exhaustive)

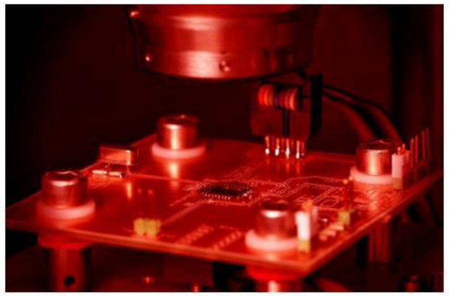
- <u>Passive</u>:
  - o Timing
    - Overall or “local” execution time



  - o Power, Electromagnetic (EM) radiation
    - Predominant CMOS technology
    - Dynamic power consumption
    - Electric current induces an EM field

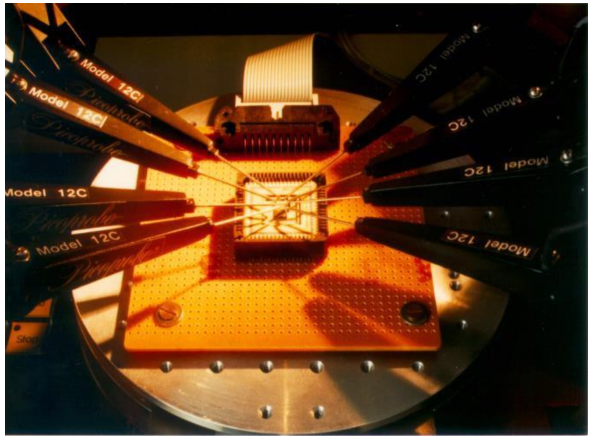


  - o More exotic but shown to be practical
    - Sound, temperature, …
- <u>Invasive</u>: Photonic emissions



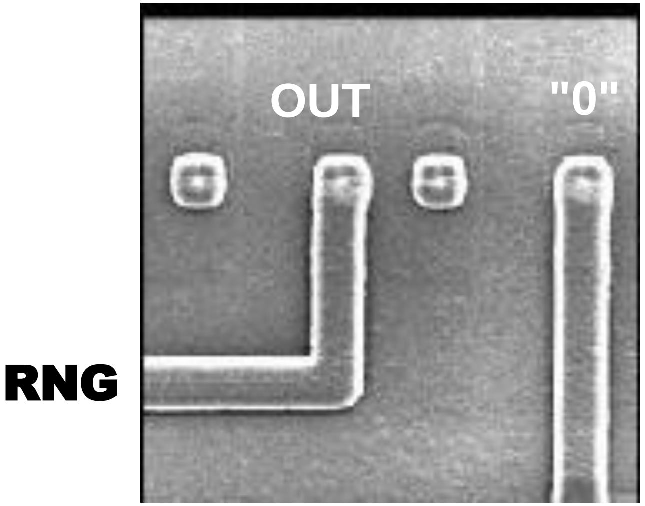
Invasive Attacks

- <u>Passive</u>: micro-probing
  - Probe the bus with a very thin needle
  - Read out data from bus or individual cells directly
  - Several needles concurrently



source: Helena Handschuh

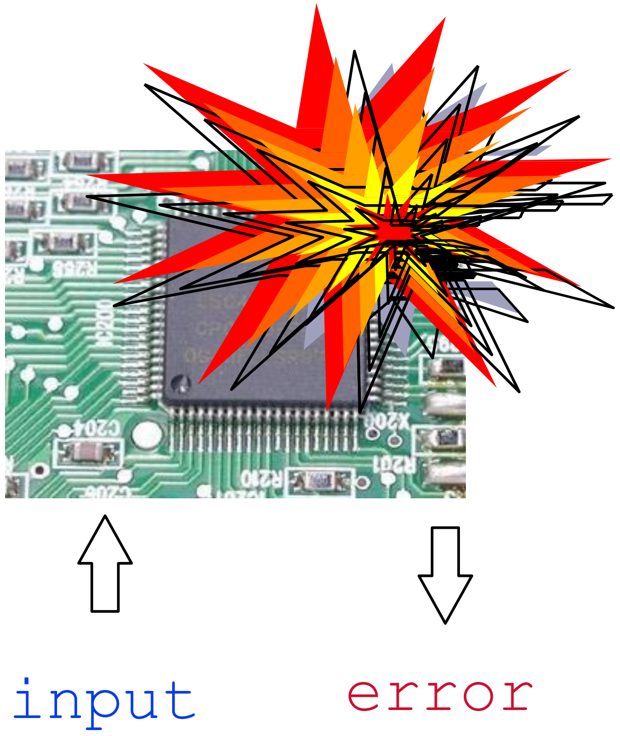
- <u>Active</u>: circuit modification
  - Connect or disconnect security mechanism
    - Disconnect security sensors
    - RNG stuck at a fixed value
    - Reconstruct blown fuses
  - Cut or paste tracks with laser or focused ion beam
  - Add probe pads on buried layers



[www.fa-mal.com]

Fault Injection Attacks (I)

- <u>Non-(semi)invasive</u>: apply combination of unaccounted environmental conditions
  - Vcc
  - Glitch
  - Clock
  - Temperature
  - UV
  - Light
  - X-Rays
  - ...



- And bypass security mechanisms or infer secrets

slide source: Helena Handschuh

Fault Injection Attacks (II)

- Invasive: exploit faulty behavior provoked by physical stress applied to the device

- Laser fault injection allows to target a relatively small surface area of the target device
- Laser pulse frequency ~ 50Hz
- Fully automated scan of chip surface

- Once you have a weak spot: perturbate and exploit

source: www.new-wave.com

Side-Channel Emissions In This Lecture

- **Power Consumption** -- Logic circuits typically consume differing amounts of power based on their input data.
- **Electro-Magnetic** -- EM emissions, particularly via near-field inductive and capacitive coupling, can also modulate other signals on the die.
- **Optical** -- The optical properties of silicon can be modulated by altering the voltage or current in the silicon.
- **Timing and Delay** -- Timing attacks exploit data-dependent differences in calculation time in cryptographic algorithms.
- **Acoustic** -- The acoustic emissions are the result of the piezoelectric properties of ceramic capacitors for power supply filtering and AC to DC conversion.

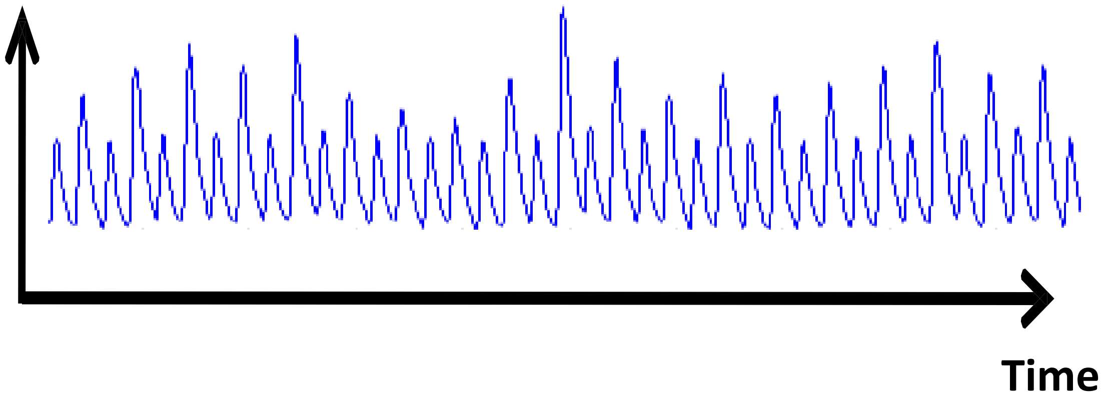
So What Really is Side-Channel Attack?

- Side-Channel attacks aim at side-channel inputs and outputs, bypassing the theoretical strength of cryptographic algorithms

- Five commonly exploited side-channel emissions:
  - Power Consumption
  - Electro-Magnetic
  - Optical
  - Timing and Delay
  - Acoustic

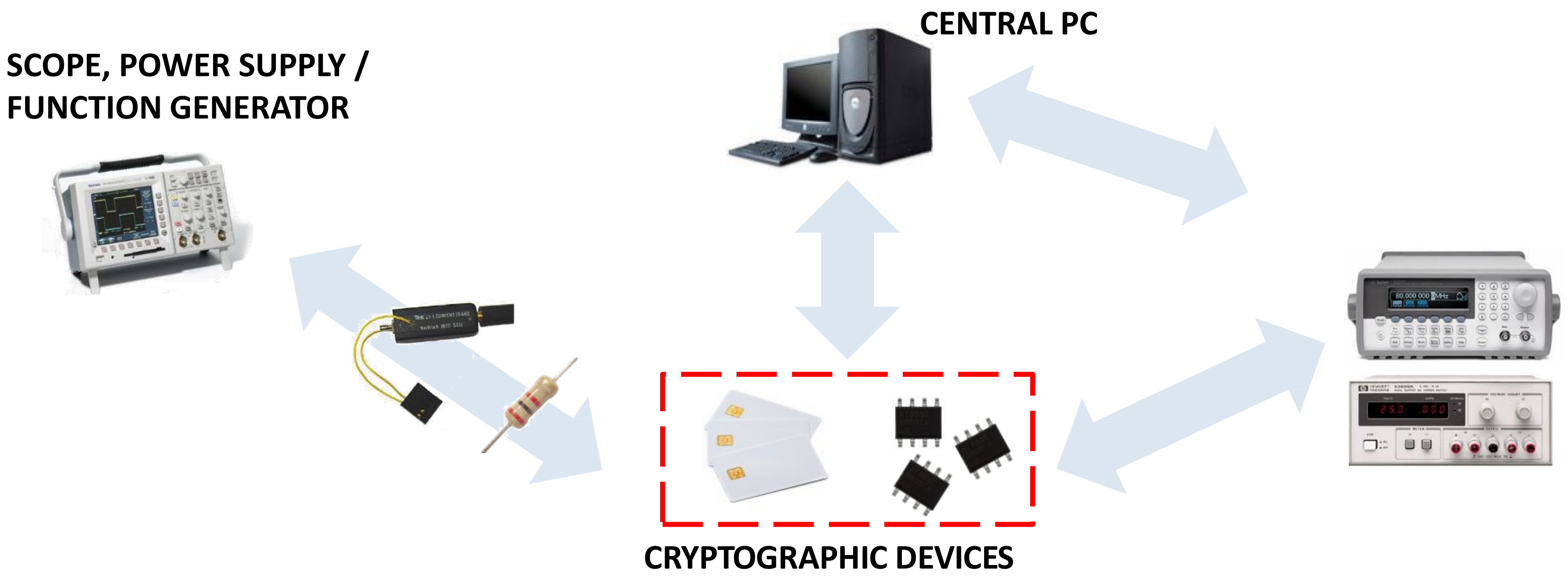
Measuring Power Consumption

- **Not average power over time, not peak power**
- Instantaneous power over time
  - Trace or curve, many samples



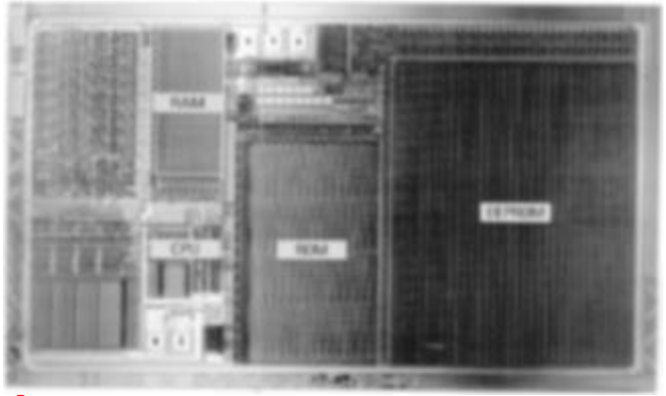
Measuring Power Consumption

Typical (automated) measurement setup



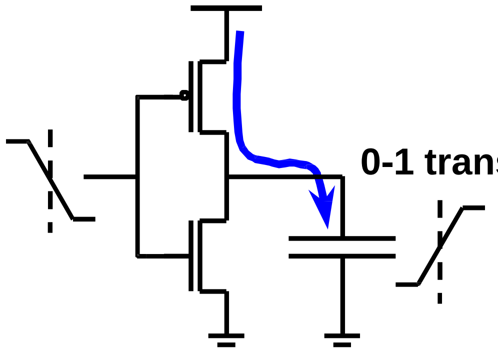
Measuring Power Consumption

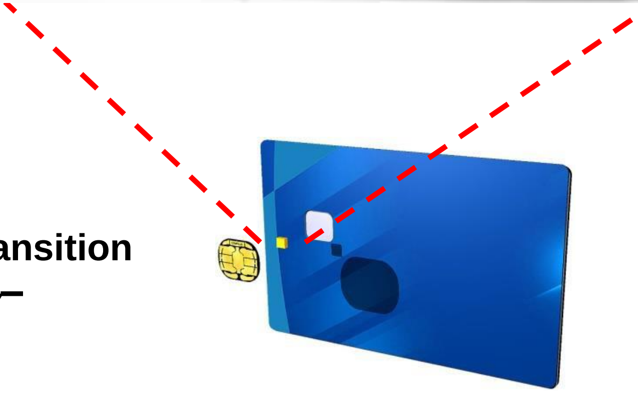
- **Logic**: constant supply voltage, supply current varies
- **Predominant technology**: CMOS
  - Low static power consumption
  - Relatively high dynamic power consumption
  - Power consumption depends on input



- **CMOS inverter**:

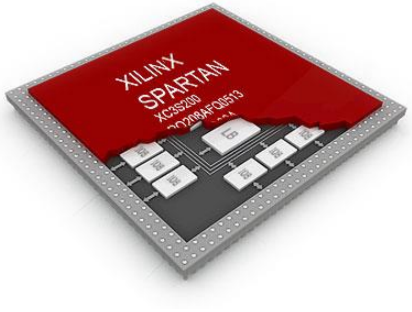
Input	Output	Current
0 → 0	1 → 1	Low
0 → 1	1 → 0	Discharge
1 → 0	0 → 1	Charge
1 → 1	0 → 0	Low



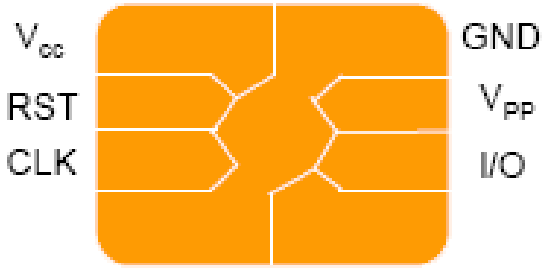


Hardware Targets

- Two common victims of hardware cryptanalysis are **smart cards** and **FPGAs**
  - Attacks on smart cards are applicable to any general purpose processor with a fixed bus architecture.
  - Attacks on FPGAs are also reported. FPGAs represent application specific devices with parallel computing opportunities.



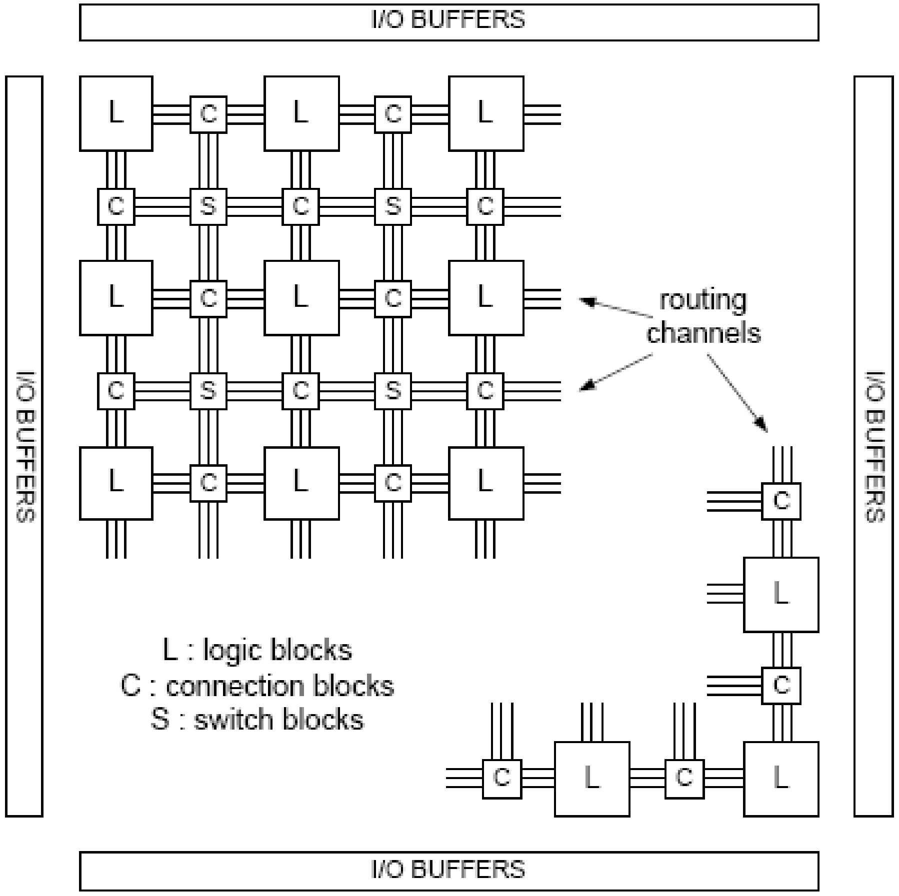
Smart Cards



- Smart cards have a small processor (8bit in general) with ROM, EEPROM and a small RAM
- **Eight wires** connect the processor to the outside world
- **Power supply**: There is no internal battery
- **Clock**: There is no internal clock
- Typically equipped with a **shield** that destroys the chip if a tampering happens

FPGAs

- FPGAs allow parallel computing
- Multiple programmable configuration bits



Attack Model / Assumptions

- Consider a device capable of implementing the cryptographic function
- The key is usually stored in the device and protected
- Modern cryptography is based on Kerckhoffs's assumption → all of the data required to operate a chip is entirely hidden in the key

- ***Attacker only needs to extract the key***

Attack Phases

- Such attacks are usually composed of two phases:
  - **Interaction phase**: interact with the hardware system under attack and obtain the physical characteristics of the device
  - **Analysis phase**: analyze the gathered information to recover the key

Principle of divide-and-conquer attack

- The divide-and-conquer (D&C) attack attempts at recovering the key by parts
- The idea is that an observed characteristic can be correlated with a partial key
  - The partial key should be small enough to enable exhaustive search
- Once a partial key is validated, the process is ***repeated*** for finding the remaining keys
- D&C attacks may be iterative or independent

Attack Classification

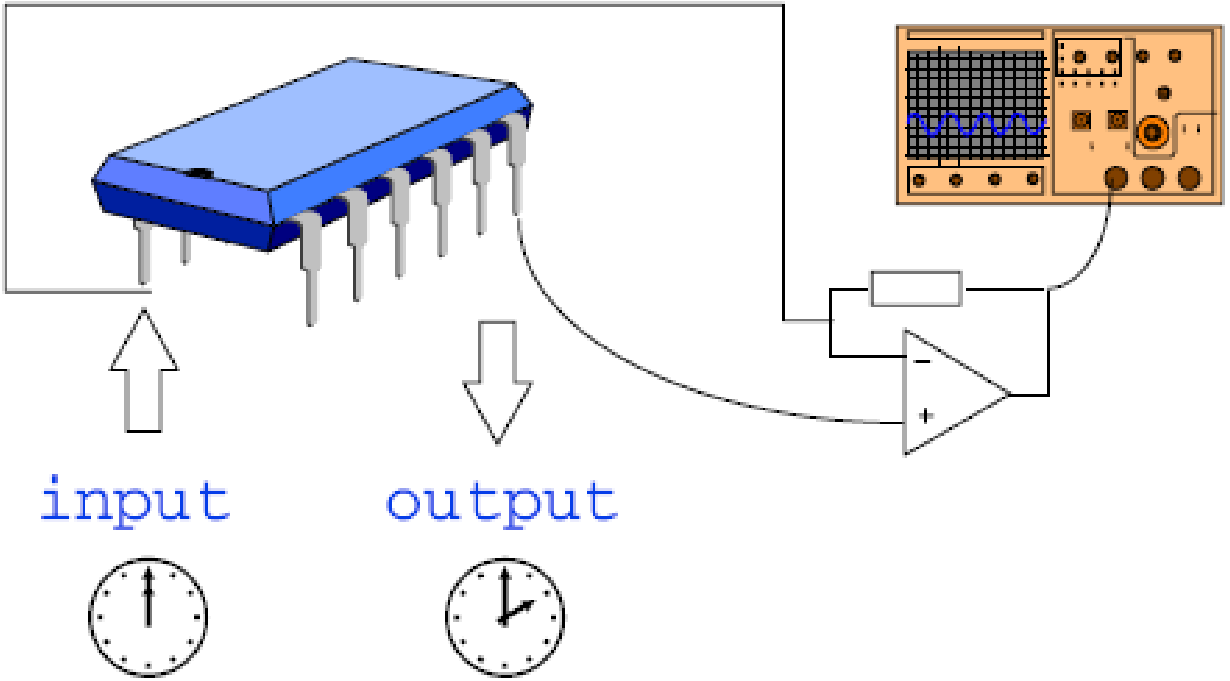
- **Invasive** vs. **noninvasive** attacks
- **Active** vs. **passive** attacks
  - Active attacks exploit side-channel inputs
  - Passive attacks exploit side-channel outputs

Attack Classification

- **Simple** vs. **differential** attacks
  - Simple side-channel attacks directly map the results from a small number of traces of the side-channel to the *operation* of device under attack
  - Differential side-channel attacks exploit the correlation between the *data values* being processed and the side-channel *leakage*

Power Attacks

- Measure the circuit's processing time and current consumption to infer what is going on inside it.



Measuring Phase

- The task is usually straightforward
  - Easy for smart cards: the energy is provided by the terminal and the current can be read
- Relatively inexpensive (<$1000) equipment can digitally sample voltage differences at high rates (1GHz++) with less than 1% error
- Device's power consumption depends on many things, including its structure and data being processed

Power Attacks