Side Channel Attacks

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Acknowledgments

- The presentation includes material from
  - Giorgio DI NATALE
  - Nicolò MAUNERO
  - Gianluca ROASCIO

  whose valuable contribution is here acknowledged and highly appreciated.

Prerequisites

- Lectures:
  - *HS_1.1 – The role of Hardware in Security*
  - *HS_1.2 - Hardware Vulnerabilities*

Goal

- Presenting the basic concepts behind the Side Channels effects and the related possible attacks:

Outline

- Introduction
- Timing Attacks
- Power Attacks
- Electromagnetic Attacks
- Acoustic Attacks
- Optical Attacks

Hardware Attacks Modalities

modality

non-invasive

passive

- Timing Attacks
- Power Attacks
- Electromagnetic Attacks
- Acoustic Attacks
- Optical Attacks

active

- Fault Attacks
- Test-Infrastructure-based Attacks

invasive

- Microprobing
- Reverse Engineering
- Data Remanence Attacks

Rationale

- The vulnerability stems from the hardware device *physicality.*
- Computer and communications devices emit numerous forms of energy or release clues, as unintended *side effects of normal operations*.

Unintentionally released clues

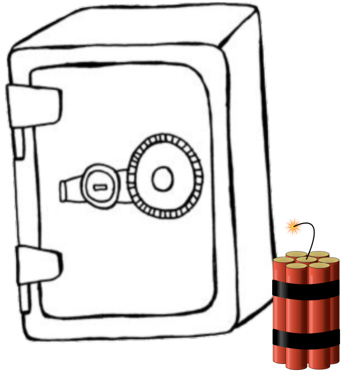
- Emitted energy in various forms:
  - Electromagnetic radiation
  - Noise
  - Light
  - …
- Additional info:
  - Spent time
  - Spent energy
  - Interferences of emitted electromagnetic radiation with nearby receivers
  - …

Non-invasive Passive Attacks (aka *Side-Channel Attacks*)

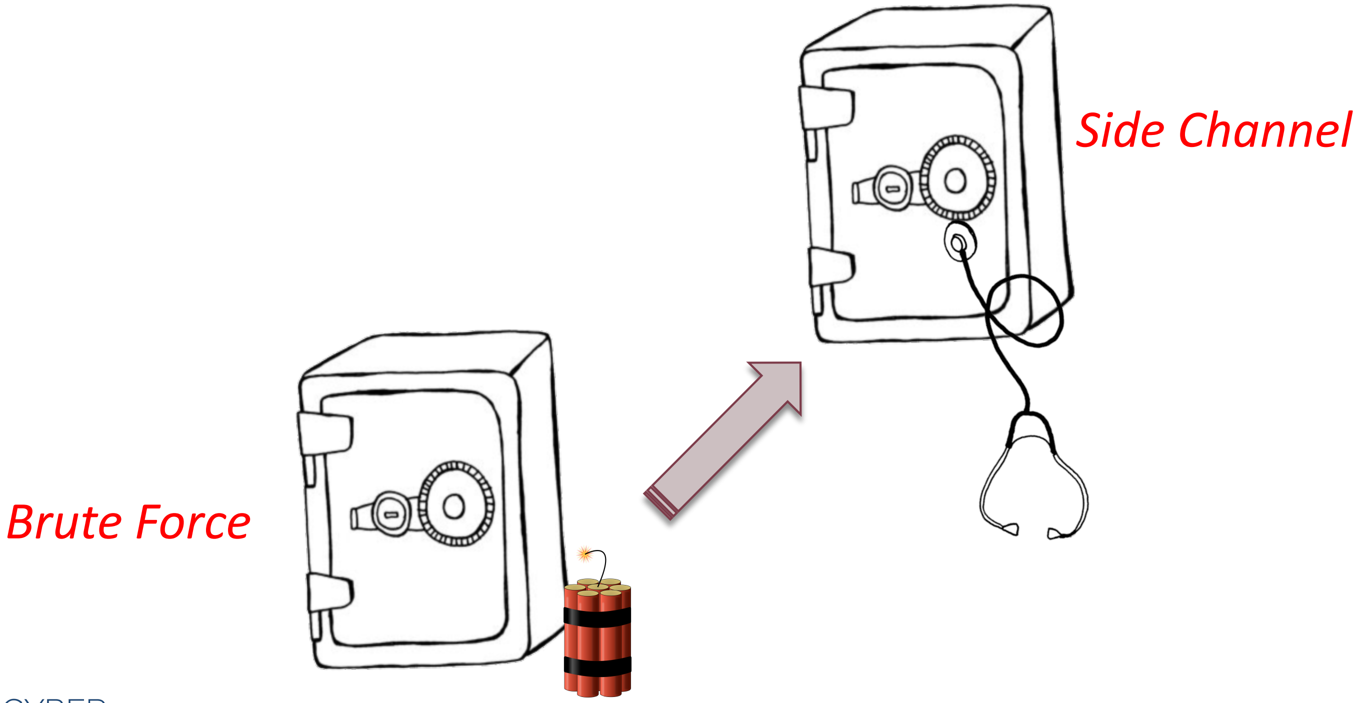
- The unintentionally emitted energy and/or clues carry information about processed data.
- Under good conditions, a sophisticated and well-equipped eavesdropper can intercept and analyse such compromising emanations to steal data by exploiting information gathered via “side-channel” interfaces.

Brute Force vs. Side-Channel

Brute Force



Brute Force vs. Side-Channel



Countermeasures against Side Channel Attacks

- Side Channel Attacks are so significant that since the late 1950s US army started a secret research project to study “*compromising emissions*”.
- TEMPEST was the initial US military codeword

Compromising emissions

- Are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed (*side-channel attack*), may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.

TEMPEST

- Later TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) became a U.S. NSA (National Security Agency) specification and a NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations

Hardware Attacks Modalities

modality

- ***non-invasive***
  - *passive*
    - Timing Attacks
    - Power Attacks
    - Electromagnetic Attacks
    - Acoustic Attacks
    - Optical Attacks
  - *active*
    - Fault Attacks
    - Test-Infrastructure-based Attacks
- ***invasive***
  - Microprobing
  - Reverse Engineering
  - Data Remanence Attacks

Timing Attacks

- A timing side-channel attack tries to recover sensible data by measuring computation time in a hardware device
- In particular, it looks at how long it takes a system to do something and uses *statistical analysis* to find the target data.

Timing Attacks

- Variabilities include, among the other:
  - performance optimizations
  - branching and conditional statements
  - processor instructions
  - RAM and cache hits.

Timing analysis on RSA

Input: $X, N, K=(k_{j-1}, \ldots, k_1, k_0)_2$

Output: $Z = X^K \bmod N$

```
Z = 1;
for i=j-1 downto 0 {
    Z = Z * Z mod N //Square
    if (k_i==1) {
            Z = Z * X mod N //Multiply
    }
}
```

Hardware Attacks Modalities

modality

non-invasive

passive

- Timing Attacks
- Power Attacks
- Electromagnetic Attacks
- Acoustic Attacks
- Optical Attacks

active

- Fault Attacks
- Test-Infrastructure-based Attacks

invasive

- Microprobing
- Reverse Engineering
- Data Remanence Attacks

Power attacks

- They rely on *Power Analysis*: a low-cost and effective way to extract the contents of a device without physically de-processing the part.
- With power analysis, the variation in power consumption of a device is used to determine its contents.

Power analysis

- Two main approaches:
  - *Simple Power Analysis*
  - *Differential Power Analysis*

Simple Power Analysis

- A method of side-channel attack that examines a chip's current consumption over a period of time.
- Since different operations will exhibit different power profiles, one can determine what type of function is being performed at a given time.

SPA examples

- One can distinguish a multiplication function from an addition function, since multiplication consumes more current than addition.
- When reading data from a memory, the ratio of 1's vs. 0's will be reflected in the power profile.

SPA on RSA

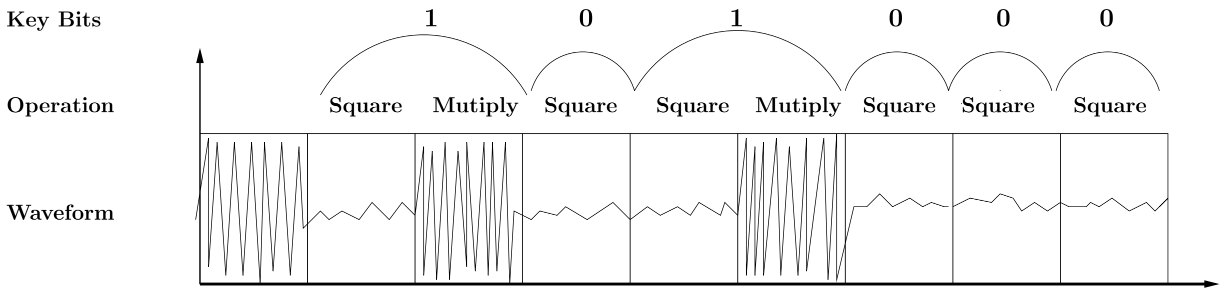
```
Input:    X, N, K=(k_{j-1}, …, k_1, k_0)_2
Output:   Z = X^K mod N

    Z = 1;
    for i=j-1 downto 0 {
        Z = Z * Z mod N //Square
        if (k_i==1) {
                Z = Z * X mod N //Multiply
        }
    }
```

Simple Power Analysis on RSA

Input: $X, N, K=(k_{j-1}, \ldots, k_1, k_0)_2$
Output: $Z = X^K \bmod N$

```
Z = 1;
for i=j-1 downto 0 {
      Z = Z * Z mod N //Square
      if (k_i==1) {
            Z = Z * X mod N //Multiply
      }
}
```



Simple Power Analysis limitations

- Is useful when data-dependent features in the power traces are apparent.
- May not be practical in presence of
  - Noise
  - Interrupts
  - Multi-core architectures
  - Peripherals
  - …

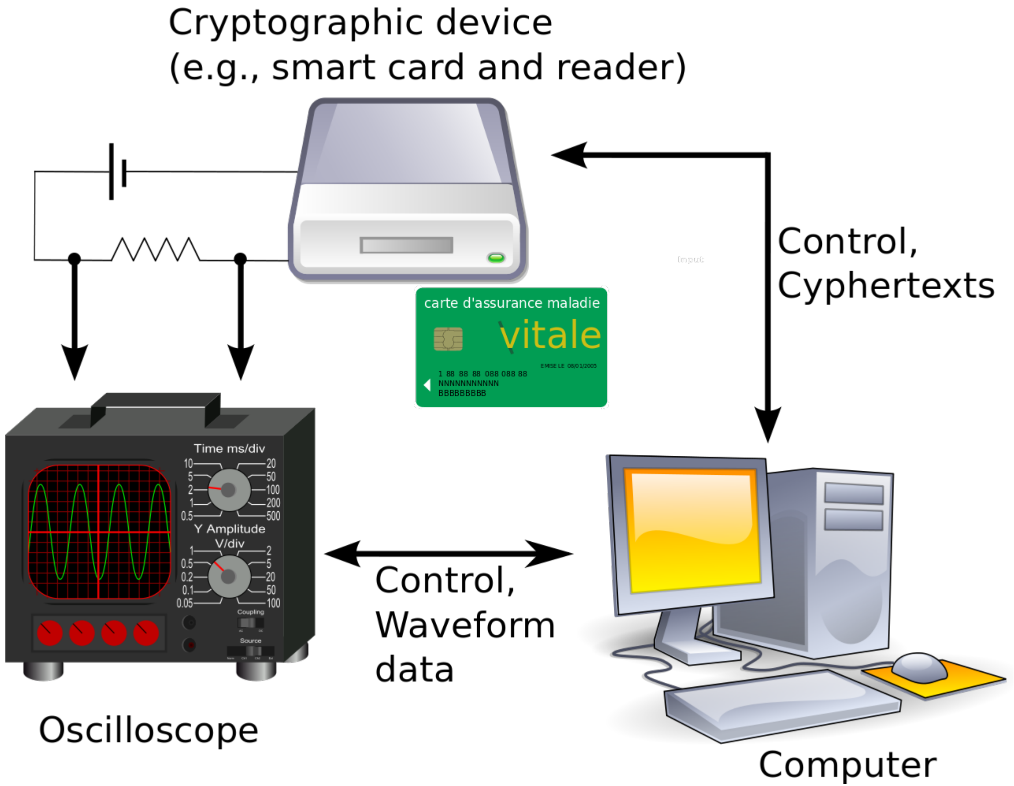
Differential Power Analysis

- Is a statistical method for analyzing power consumption to identify data-dependent correlations.

Differential Power Analysis

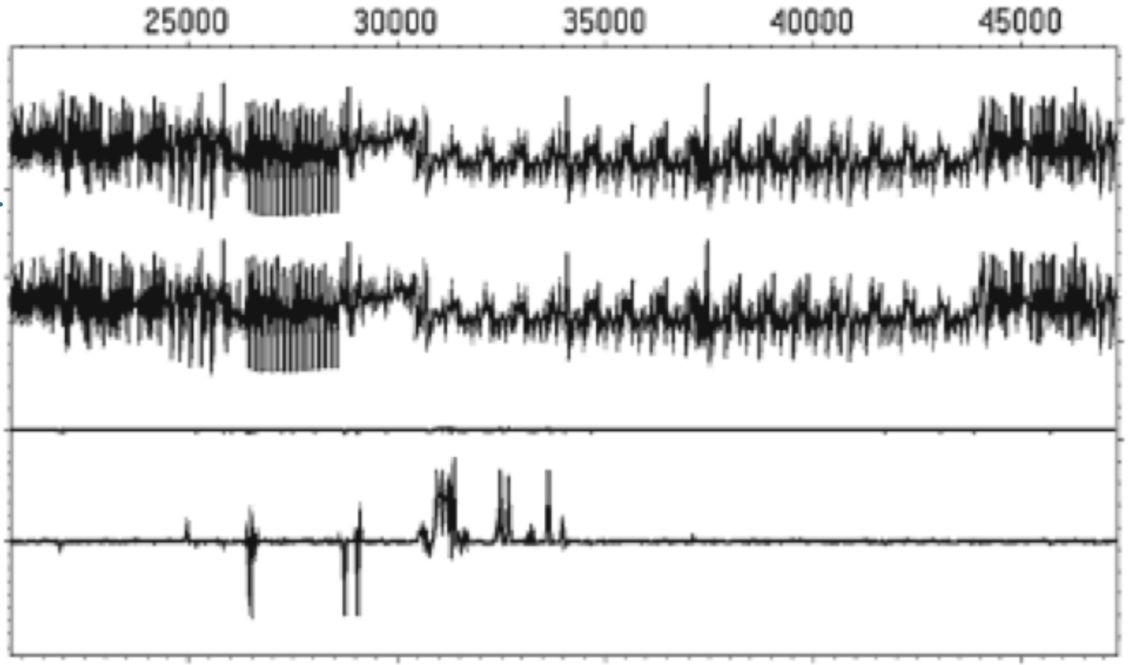
- It takes multiple traces of two sets of data, then computes the difference of the average of these traces.
  - If the difference is close to zero, then the two sets are not correlated.
  - If the sets are correlated, then the difference will be a non-zero number.
- Given enough traces, even tiny correlations can be seen, regardless of how much noise is in the system, since the noise will effectively cancel out during the averaging.

Differential Power Analysis



DPA example

2 sets of traces

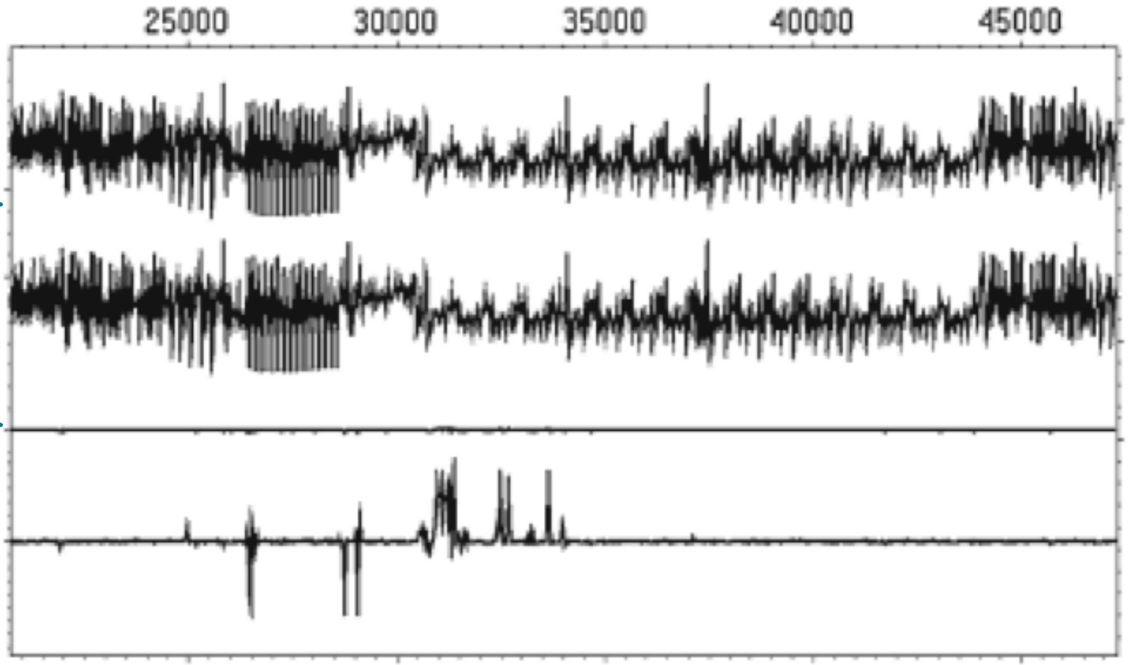


[Paul Kocher, Joshua Jaffe, Benjamin Jun, Pankaj Rohatgi: “Introduction to Differential Power Analysis”, Journal of Cryptographic Engineering, April 2011, Volume 1, Issue 1]

DPA example

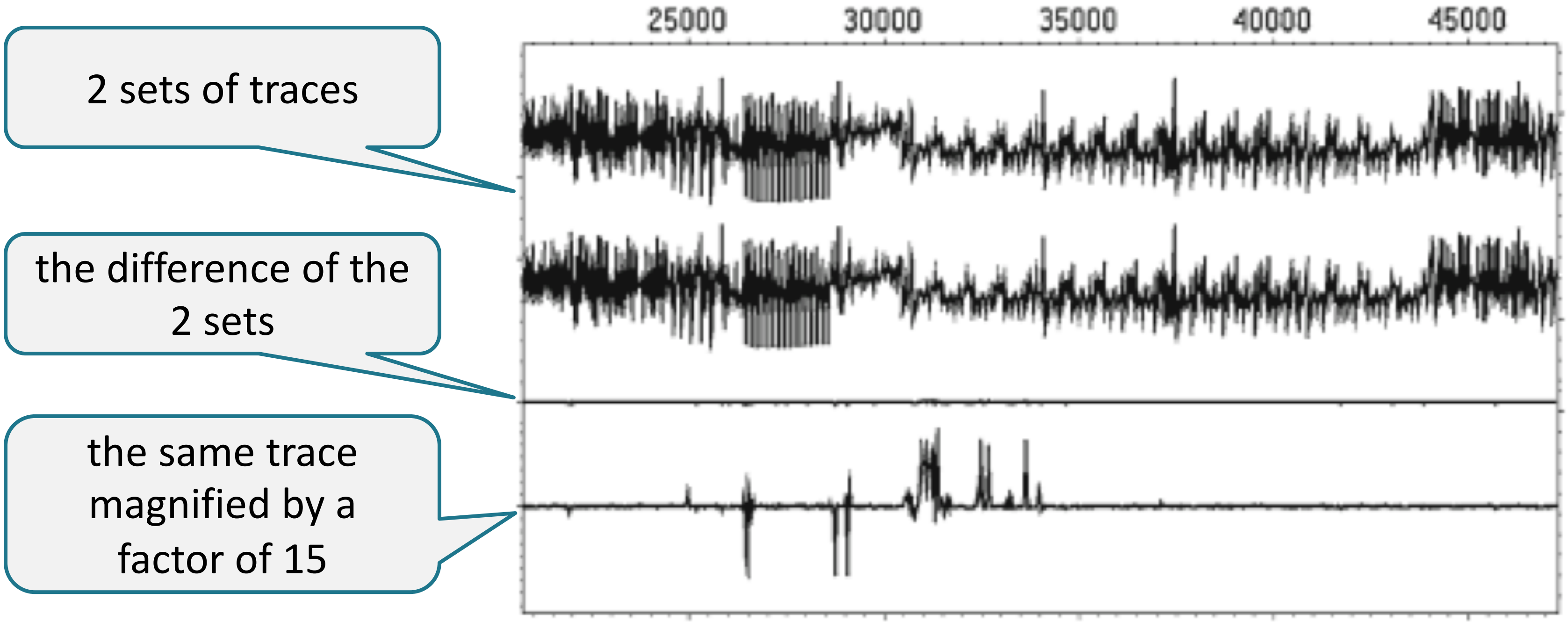
2 sets of traces

the difference of the 2 sets



[Paul Kocher, Joshua Jaffe, Benjamin Jun, Pankaj Rohatgi: “Introduction to Differential Power Analysis”, Journal of Cryptographic Engineering, April 2011, Volume 1, Issue 1]

DPA example



[Paul Kocher, Joshua Jaffe, Benjamin Jun, Pankaj Rohatgi: "Introduction to Differential Power Analysis", Journal of Cryptographic Engineering, April 2011, Volume 1, Issue 1]

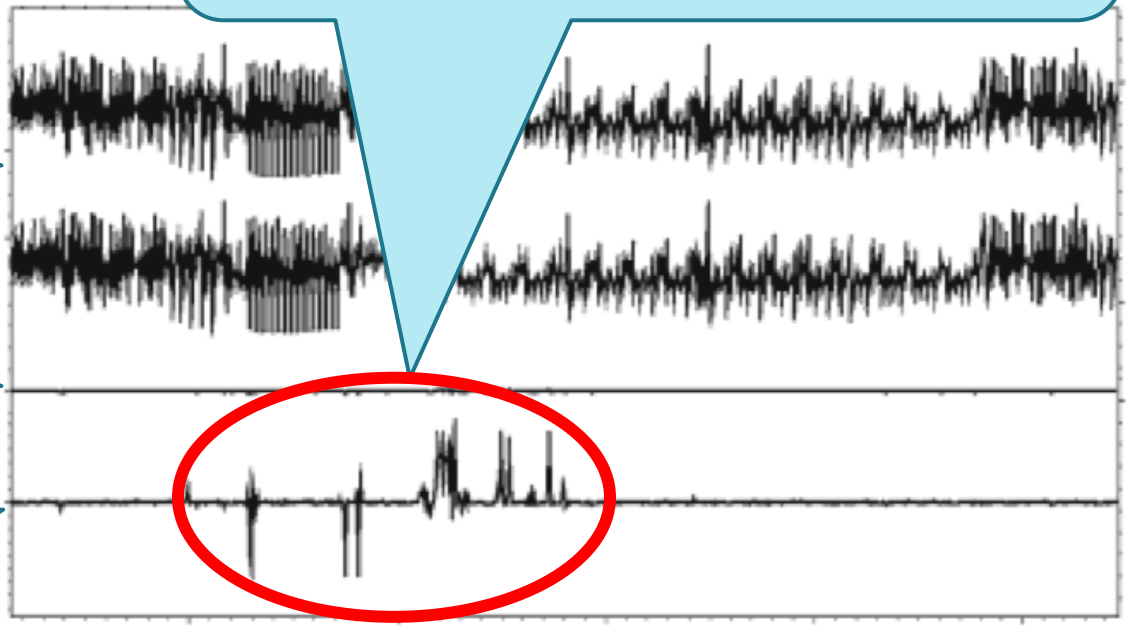
DPA example

This shows that there is statistical correlation between the two sets.
If there were no correlation, the difference would be zero, or close to zero

2 sets of traces

the difference of the 2 sets

the same trace magnified by a factor of 15

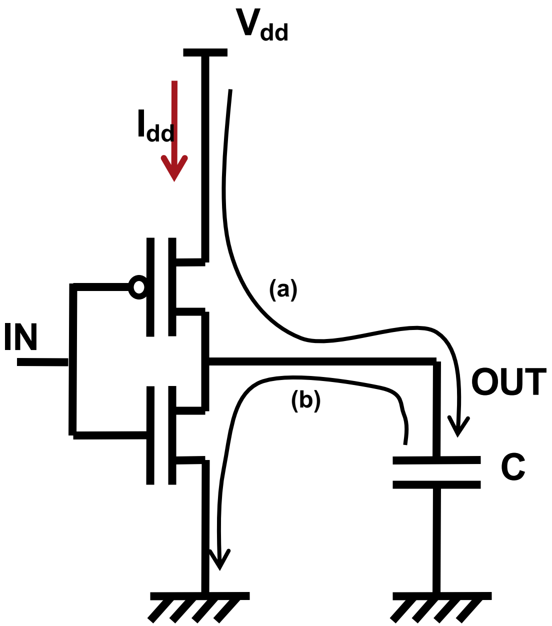


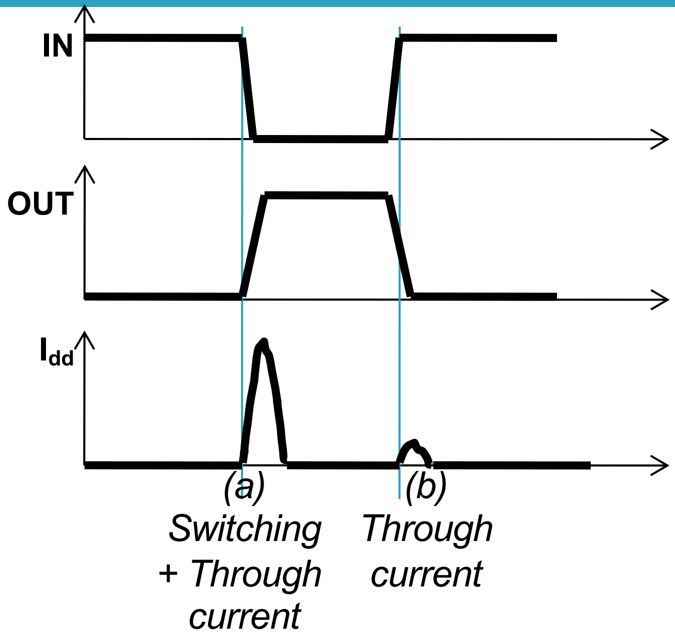
[Paul Kocher, Joshua Jaffe, Benjamin Jun, Pankaj Rohatgi: "Introduction to Differential Power Analysis", Journal of Cryptographic Engineering, April 2011, Volume 1, Issue 1]

DPA attacks

- Require the knowledge of the algorithm but not its physical implementation
- Are cheap and easy to perform
- The basic idea is to correlate the power consumed by the device and the encryption data including the key

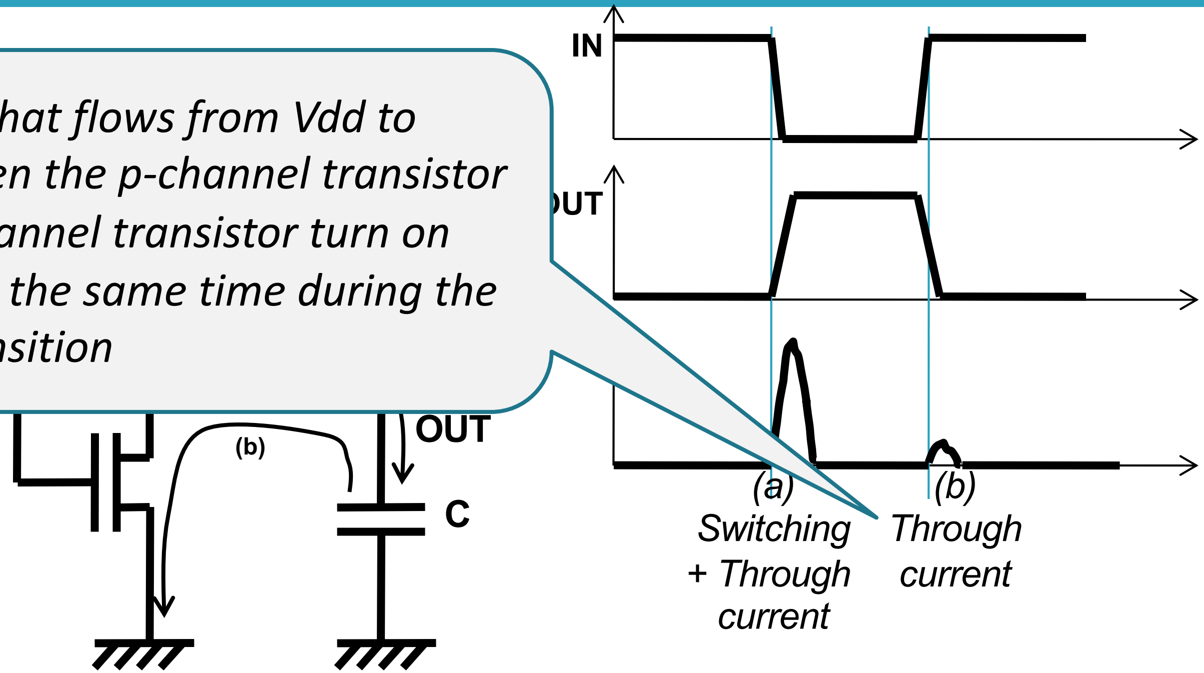
Power Consumption of CMOS



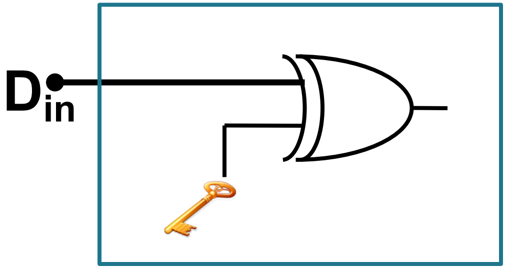


Power Consumption of CMOS

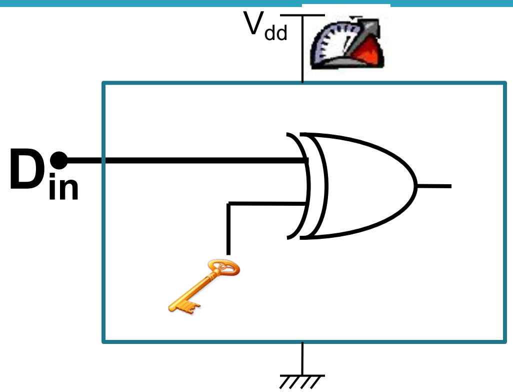
Current that flows from Vdd to GND when the p-channel transistor and n-channel transistor turn on briefly at the same time during the logic transition



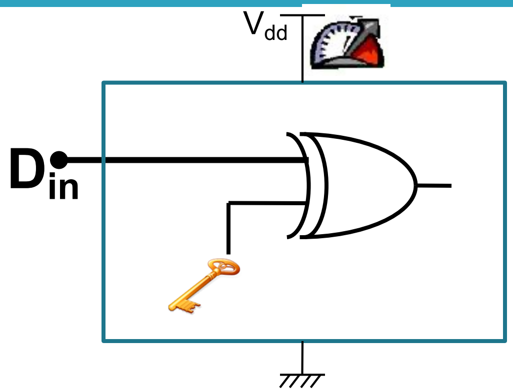
Power attack on XOR gate

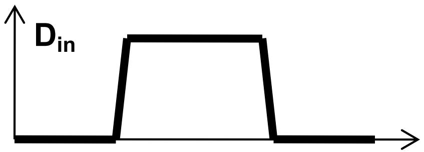


Power attack on XOR gate

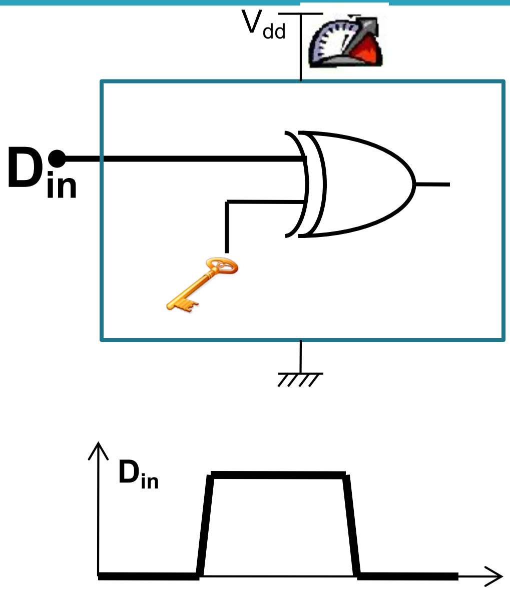


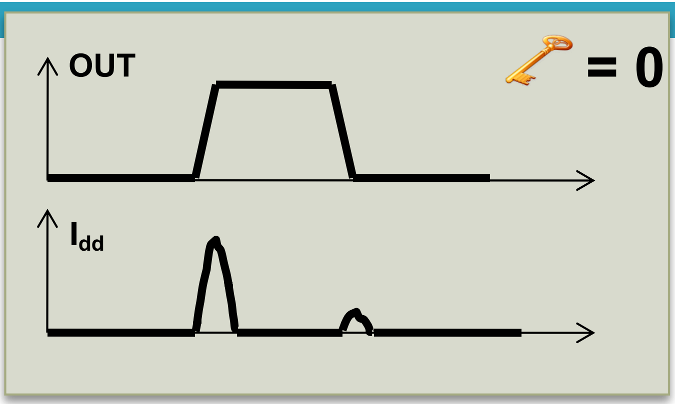
Power attack on XOR gate



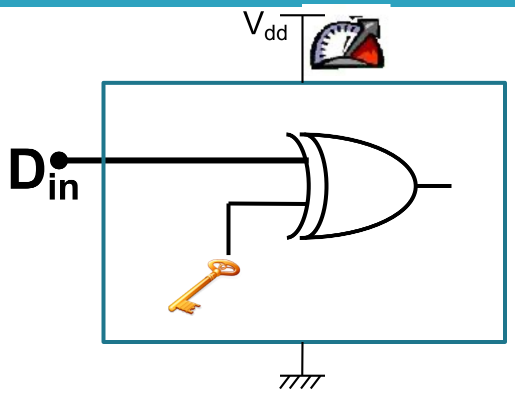


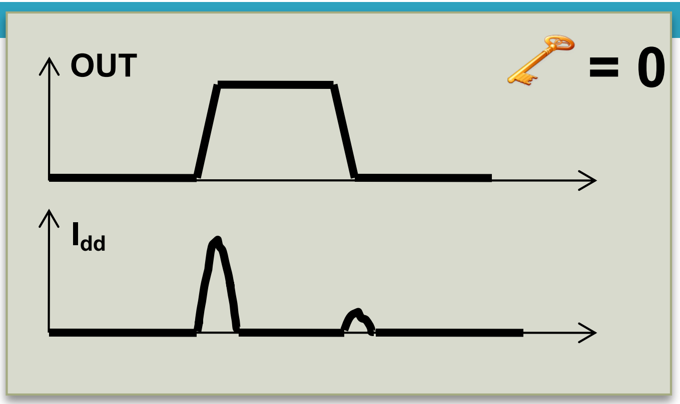
Power attack on XOR gate

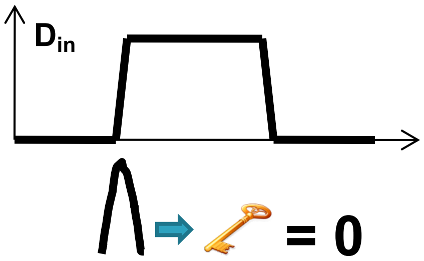




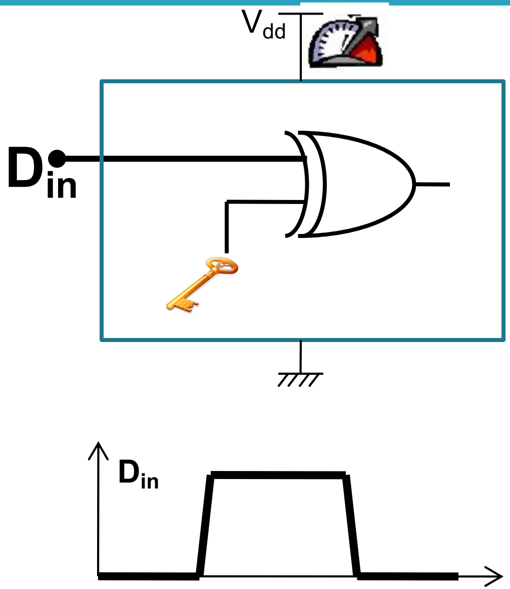
Power attack on XOR gate

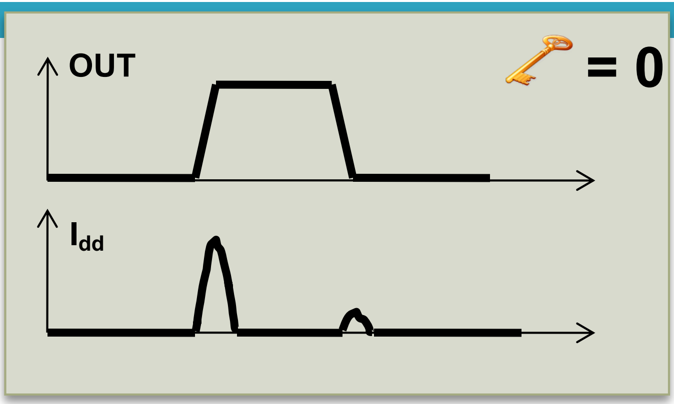


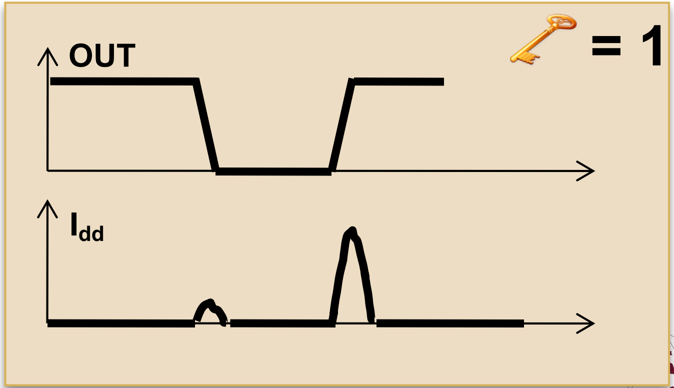




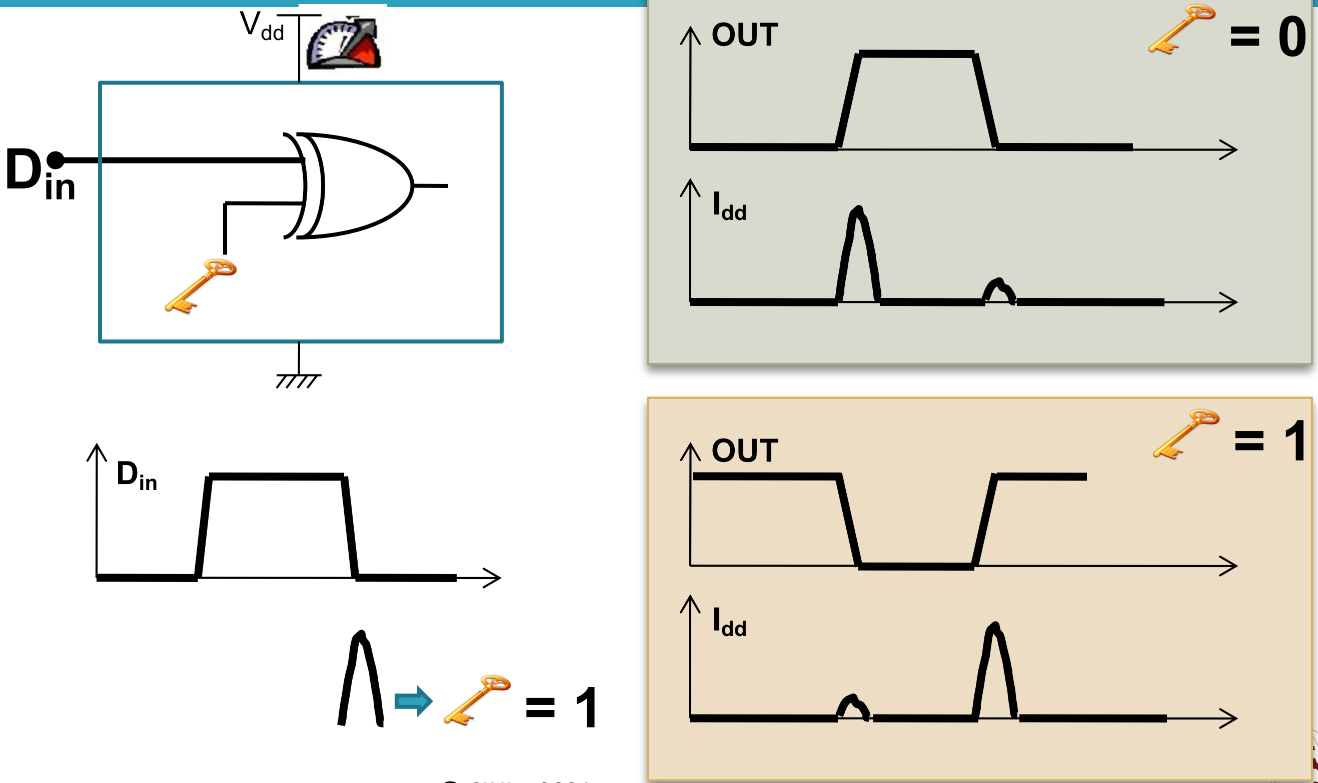
Power attack on XOR gate







Power attack on XOR gate



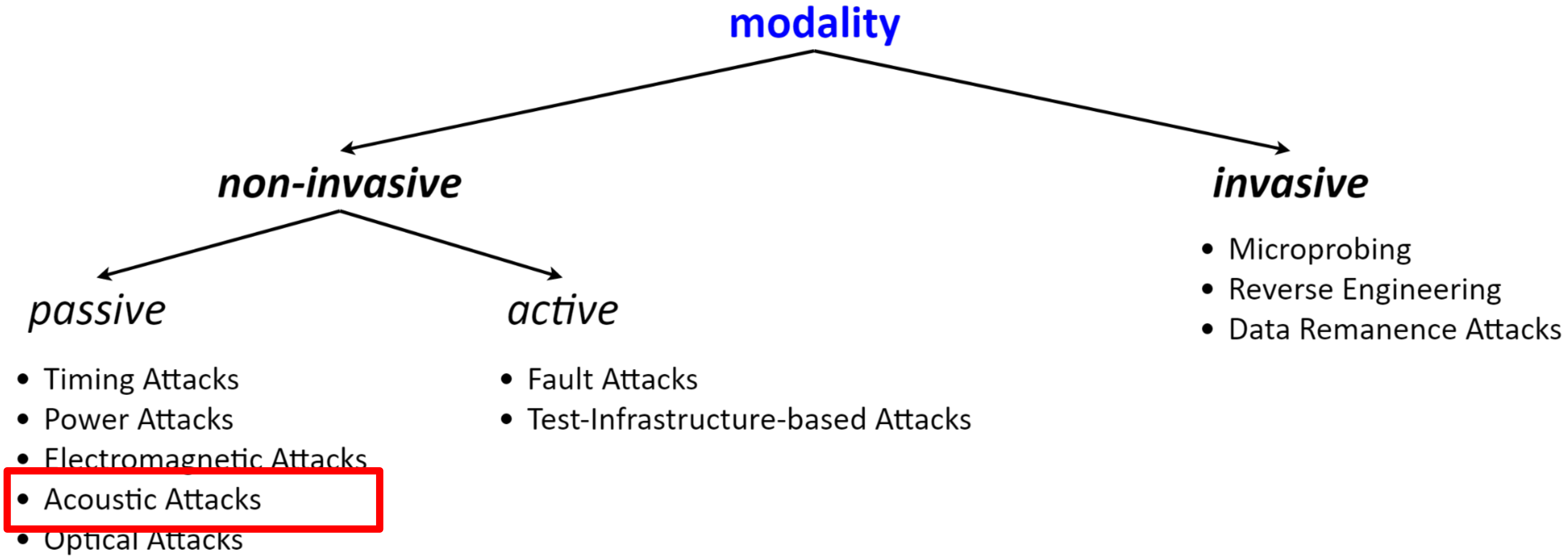
Countermeasures against DPA

- One of the most common is the introduction of random process interrupts.
- Instead of executing all the operations sequentially, the CPU interleaves the code’s execution with that of dummy instructions so that corresponding operation cycles do not match because of time shifts.

Incoherent averaging

- The introduction of dummy instructions has the effect of smearing the peaks across the differential trace due to a desyncronisation effect, known in digital signal processing as *incoherent averaging*

Hardware Attacks Modalities



Acoustic Attacks

- Several reported attacks. Among the others:
  - *Acoustic Triangulation Attacks*
  - *Ultrasonic noise*
  - *Surfing Attacks*

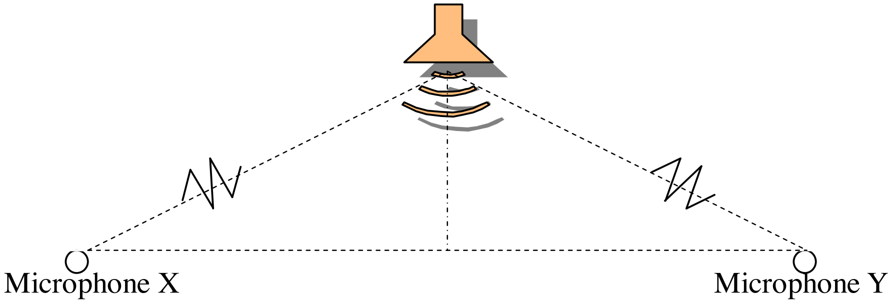
Acoustic Attacks

- Several reported attacks. Among the others:
  - *Acoustic Triangulation Attacks*
  - *Ultrasonic noise*
  - *Surfing Attacks*

Acoustic Triangulation Attacks

- Computer keyboards and keypads used on telephones and automated teller machines (ATMs) are vulnerable to attacks based on the sounds produced by different keys.

Acoustic Triangulation Attack



Acoustic Attacks

- Several reported attacks. Among the others:
  - *Acoustic Triangulation Attacks*
  - *Ultrasonic noise*
  - *Surfing Attacks*

Ultrasonic noise

- It may be possible to conduct timing attacks against a CPU performing cryptographic operations by analyzing variations in acoustic emissions.
- Analyzed emissions were ultrasonic noise emanating from capacitors and inductors on computer motherboards, using either a mobile phone located close to the laptop, or a laboratory-grade microphone located up to 4 m away

Acoustic Attacks

- Several reported attacks. Among the others:
  - *Acoustic Triangulation Attacks*
  - *Ultrasonic noise*
  - *Surfing Attacks*

Surfing Attacks

SurfingAttack – hacking phones via ultrasonic waves

March 2, 2020 By Pierluigi Paganini

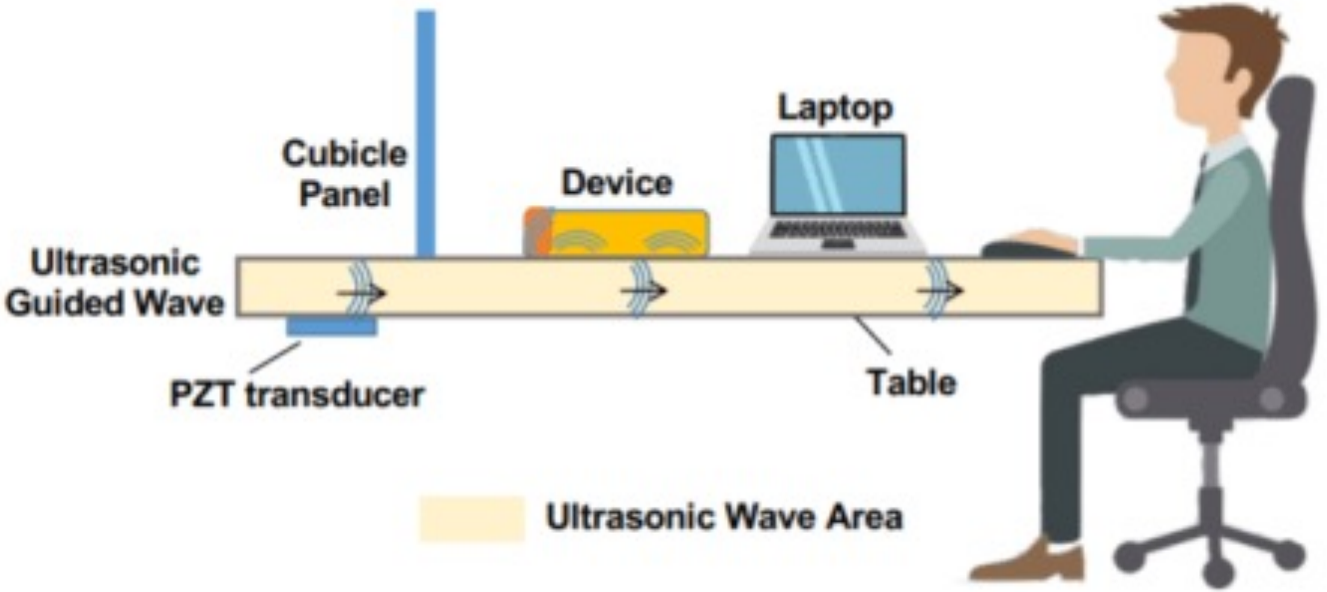
SurfingAttack is an attacking technique that allows to wake up mobile device and control them using voice commands encoded in ultrasonic waves.

SurfingAttack is a hacking technique that sees voice commands encoded in ultrasonic waves silently activate a mobile phone's digital assistant. The technique could be used to do several actions such as making phone calls or reading text messages.

Surfing Attacks

- The attack scenario sees a laptop located in a separate room from the victim's phone.
- The laptop connects to a waveform generator via Wi-Fi or Bluetooth, the generator device must be in proximity of the target's phone.

Surfing Attacks



Hardware Attacks Modalities

modality

non-invasive

passive

- Timing Attacks
- Power Attacks
- Electromagnetic Attacks
- Acoustic Attacks
- $\boxed{\text{Optical Attacks}}$

active

- Fault Attacks
- Test-Infrastructure-based Attacks

invasive

- Microprobing
- Reverse Engineering
- Data Remanence Attacks

Approaches

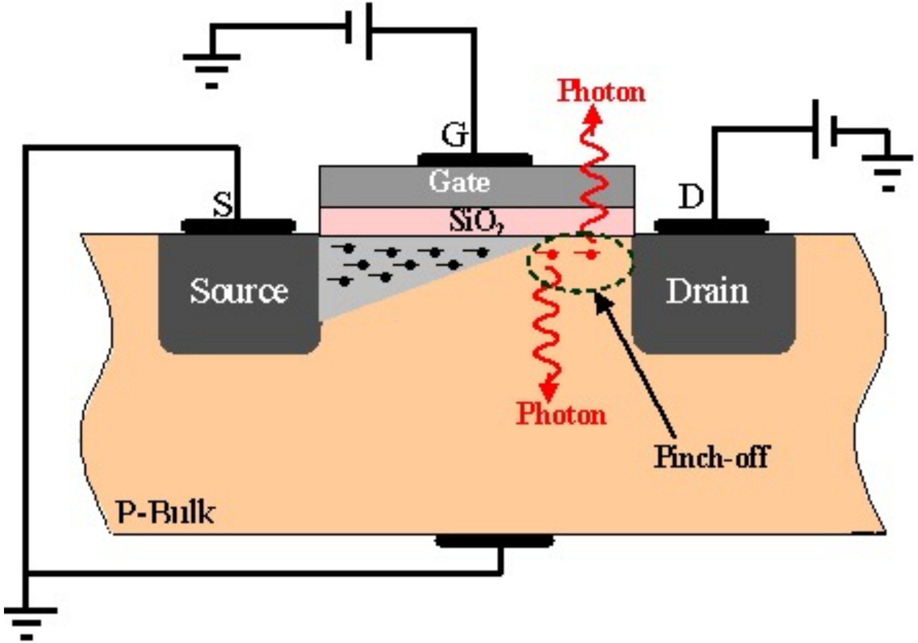
- Several approaches:
  - *Photoemission based*
  - *Optical Contactless Probing*
  - *Thermal imaging attack*

Approaches

- Several approaches:
  - *Photoemission based*
  - *Optical Contactless Probing*
  - *Thermal imaging attack*

Photoemission based

- Light emission from silicon has been observed by:
  - Newman in 1955 from reverse-biased PN junction
  - Solomon and Klein in 1976 from oxides



Photoemission based

- Photoemission mechanisms must be explained by quantum mechanical theory and is still not completely understood.
- In the simplistic model, when energetic carriers recombine in a semiconductor, they can lose energy though a photon (lattice vibration) or by emitting a photon of light.

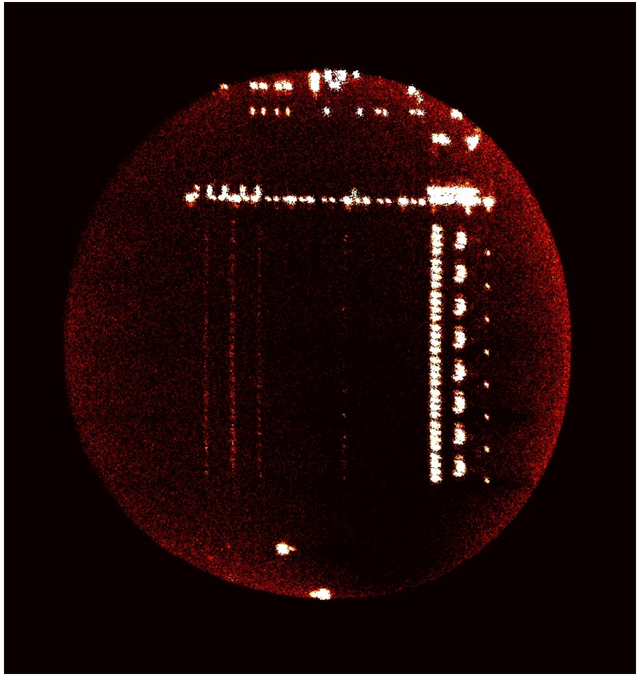
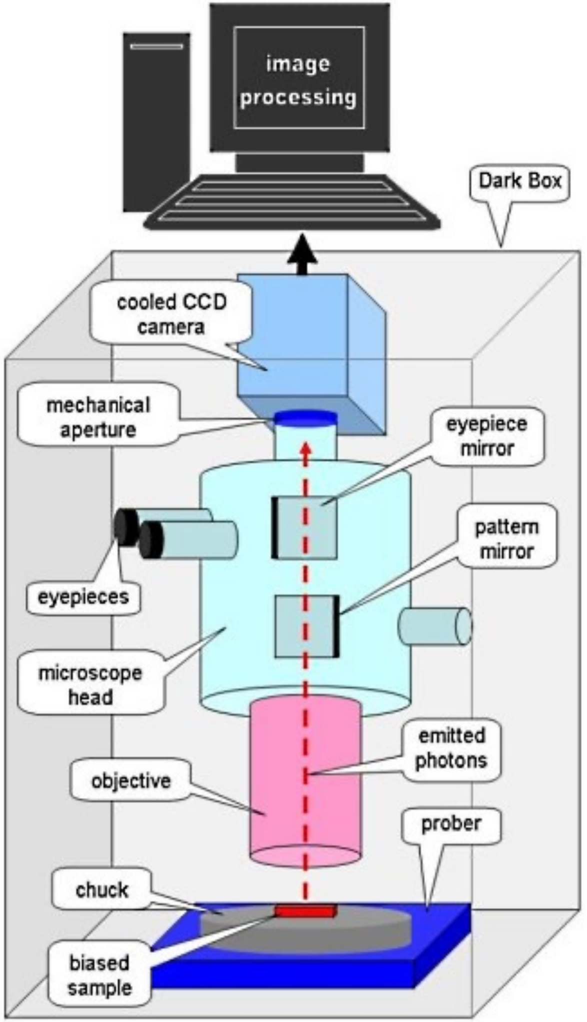


Photo Emission Microscope

- The first photon emission microscope (PEM) was developed in the early 1980s



http://www.vvku.eu/cv/efa/background.html

Approaches

- Several approaches:
  - *Photoemission based*
  - *Optical Contactless Probing*
  - *Thermal imaging attack*

Optical Contactless Probing (OCP)

- Optical techniques have been developed by chip manufacturers in the field of *failure analysis* to debug nanoscale ICs in a contactless way from the backside of the chip.
- They include, for instance:
  - *Electro-Optical Probing* (EOP)
  - *Electro-Optical Frequency Mapping* (EOFM)

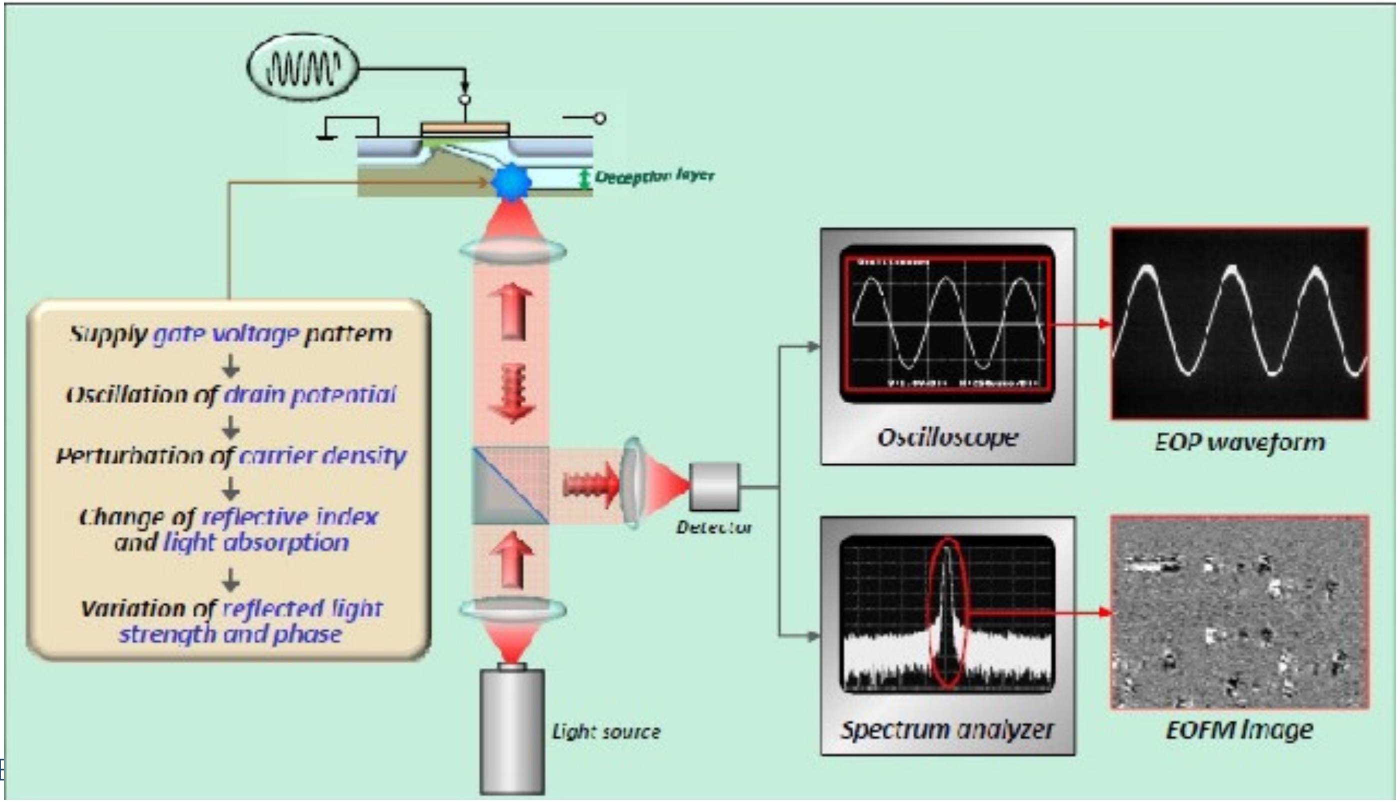
OCP rationale

- While the optical path from the transistors to the surface of the IC is obstructed by multiple interconnected layers, the analysis can be carried out from the IC backside through the silicon substrate.

EOP

- EOP are expensive equipment comprised of several elements:
  - an appropriate laser or laser diode
  - an electro-optic crystal (if using an external crystal for detection)
  - detectors for sensing the phase shift of the laser beam (typically photodiodes)
  - a variety of optical hardware, including polarizing beam splitters, magnifying lenses, a faraday rotator, and a half-wavelength waveplate
  - detection electronics.

EOP/EOFM mechanism



OCP side effects

- Unfortunately, OCP tools can be used by an attacker to probe volatile and on-die-only secret data from the backside of a chip without making any physical contact with transistors.

Approaches

- Several approaches:
  - *Photoemission based*
  - *Optical Contactless Probing*
  - *Thermal imaging attack*

Thermal imaging attack

- Attacks using a thermal imaging camera
- Example: capturing PIN numbers of customers using cash machines

Figure 1: A micro camera in a cash machine case
Source: http://krebsonsecurity.com/

Thermal imaging attack

- Attacks using a thermal imaging camera
- Example: capturing PIN numbers of customers using cash machines

Figure 1: A micro camera in a cash machine case
Source: http://krebsonsecurity.com/

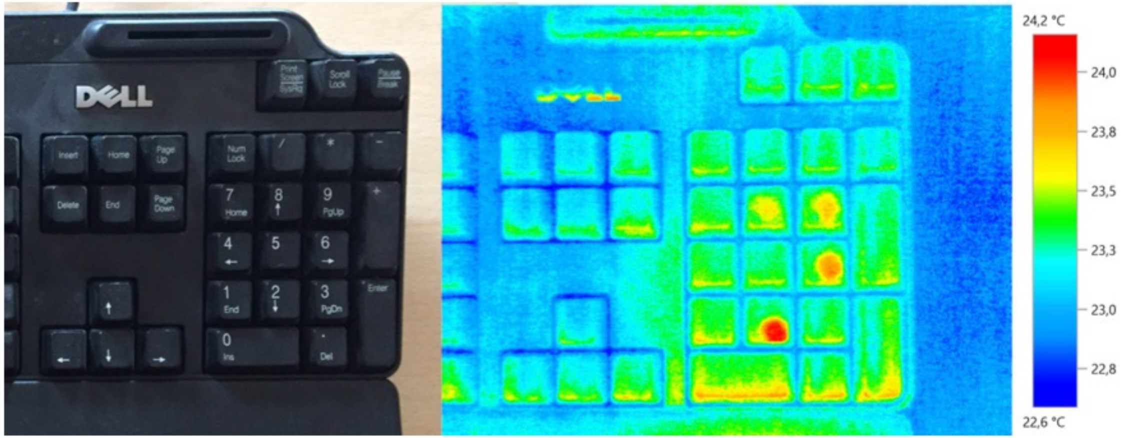


Figure 3: Attack on a computer keyboard, time: 5 seconds, PIN:8962

Paolo PRINETTO

Director
CINI Cybersecurity
National Laboratory

Paolo.Prinetto@polito.it

Mob. +39 335 227529

CYBER
CHALLENGE.IT

CYBERSECURITY
NATIONAL
LABORATORY

https://cybersecnatlab.it