Side-Channel Analysis Intro: Acquisition (with ChipWhisperer)

PA192

Łukasz Chmielewski

CRoCS,
Masaryk University,
chmiel@fi.muni.cz

November 2025

CROCS
Centre for Research on Cryptography and Security

Outline

CROCS
Centre for Research on Cryptography and Security

Plan for Today

1. Introduction

1. ChipWhisperer Installation
2. Setups
3. Analysis of some captured by you traces
4. Even if we have enough devices: please work in pairs! Discuss you solutions.

Disclaimers

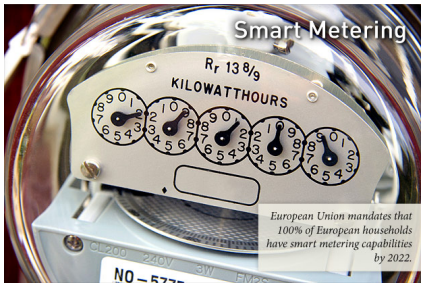
- Frist some super-brief introduction to SCA
- The the main goal is to show you how simple power analysis work and
  - building a setup for SCA looks like...
- This seminar is for you and there is no homework. We can look at what you want, so please let me know when you have questions...
- Since there are many technical components, things might get shaky...

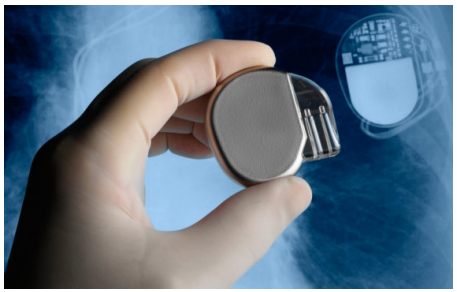
CROCS
Centre for Research on Cryptography and Security

Side-Channel Analysis Introduction

Side-Channel Analysis Introduction

Known challenge: embedded crypto devices





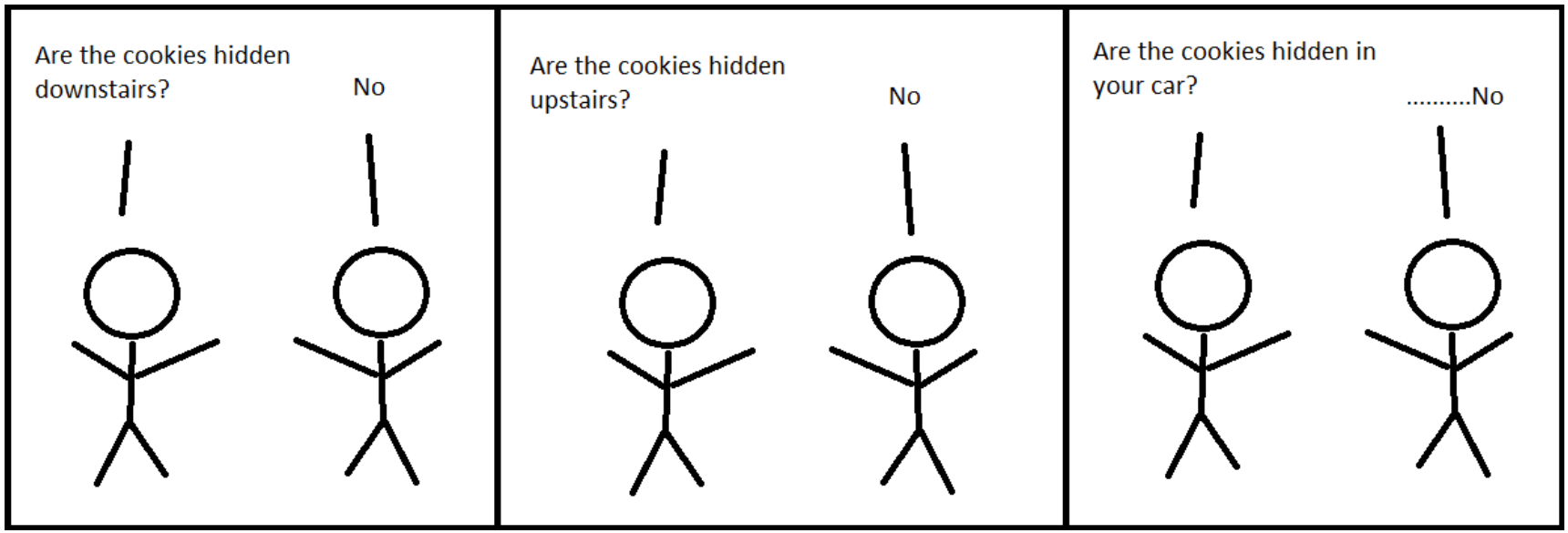
CROCS
Centre for Research on Cryptography and Security

Snow Example: what do you think it is?

Snow Example: what do you think it is? answer.

https://www.independent.co.uk/news/world/europe/melting-snow-being-used-by-police-to-find-cannabis-farms-in-the-netherlands-10036057.html

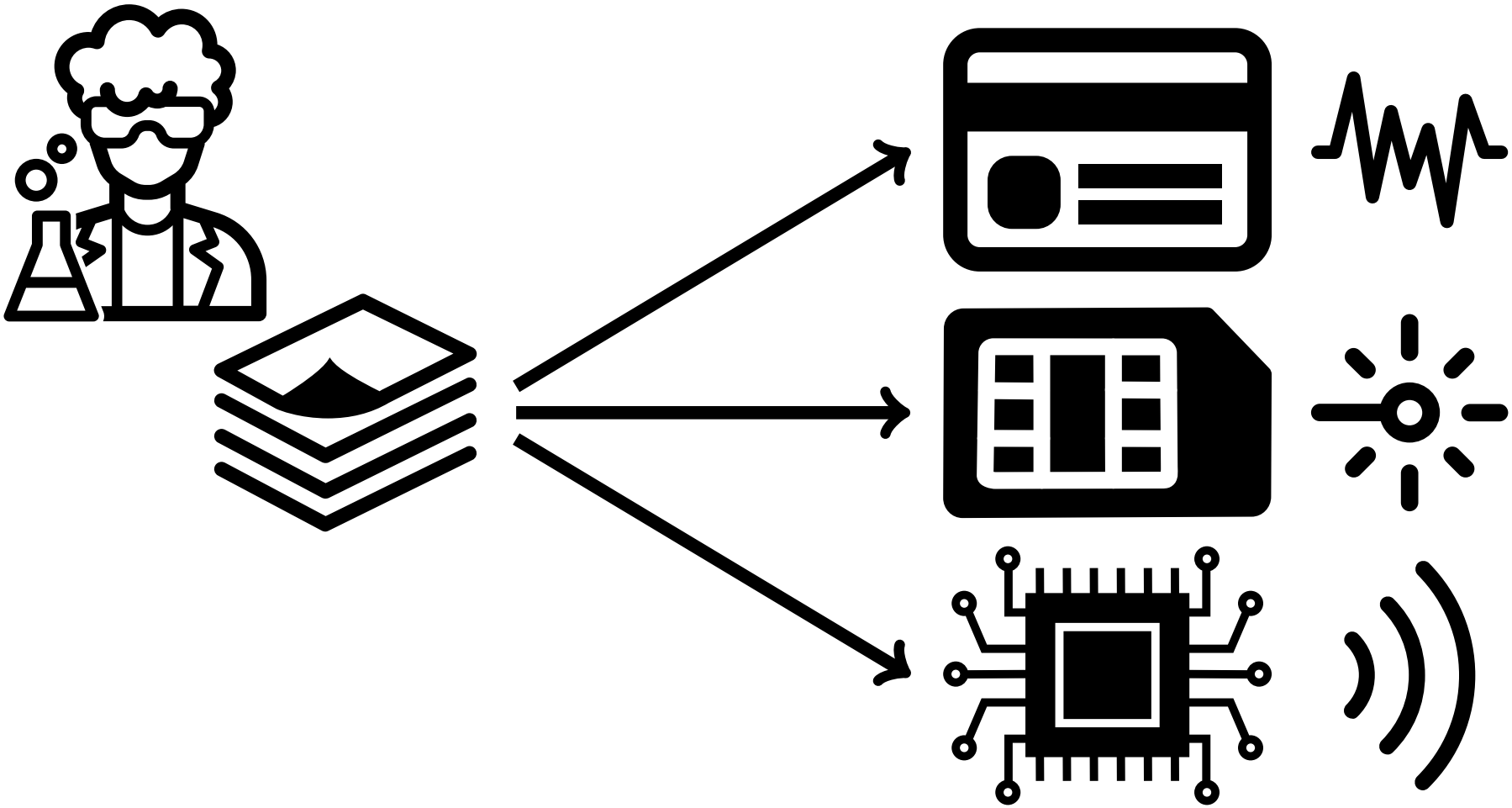
Cookies Example



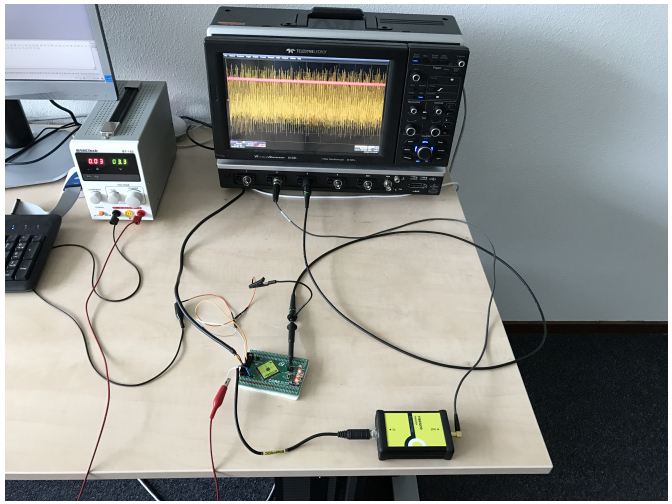
https://www.simplethread.com/great-scott-timing-attack-demo/

CROCS
Centre for Research on Cryptography and Security

Types of Side Channels



Implementation attacks



CROCS
Centre for Research on Cryptography and Security

Relevance

TPM-FAIL, November 13, 2019

LadderLeak, May 28, 2020

SCA Titan: January 7, 2021

Minerva, October 3, 2019

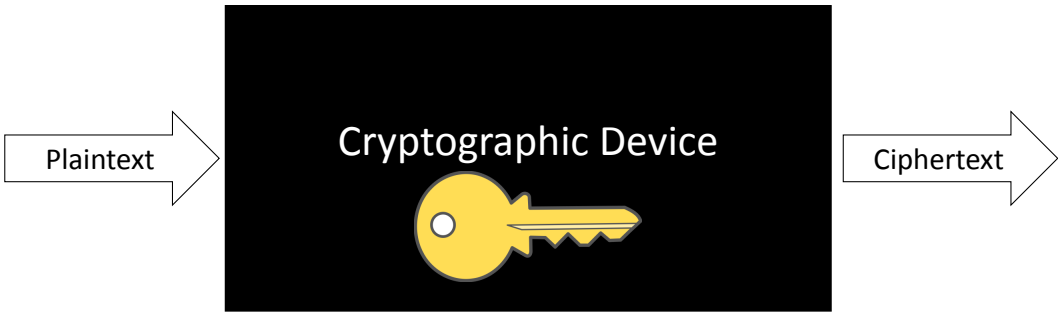
TPMScan, March 12, 2024

EUCLEAK, August 30, 2025

A bit older **ROCA** for RSA (2017): `https://crocs.fi.muni.cz/public/papers/rsa_ccs17`

CROCS
Centre for Research on Cryptography and Security

Blackbox scenario



- Cryptographic function is a black box, parameterized with key, that maps plaintext into ciphertext
- Analyzing the security in the blackbox scenario relates to classical cryptanalysis
- Adversary's goal: secret key or plaintext recovery by observing plaintext/ciphertext pairs

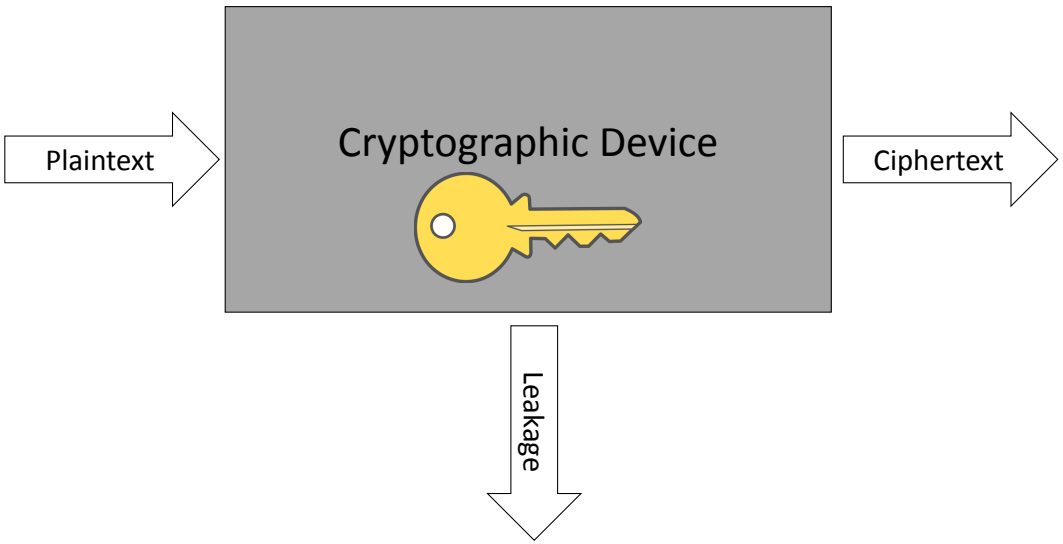
CROCS
Centre for Research on Cryptography and Security

Greybox scenario

- Crypto is **implemented on a real device** such as a microcontroller, FPGA, ASIC etc.
- We can measure and process certain *physical quantities* in the device's vicinity
- Adversary's goal: secret key or plaintext recovery by observing plaintext/ciphertext pairs **and a side channel**
- *Side channel* is any unintentional signal that can offer us a blurry view of the algorithm's internal computations
- Examples: execution/reaction time, power consumption, electromagnetic emission, sound

CROCS
Centre for Research on Cryptography and Security

Greybox scenario



- Assuming limited access to the internal computations through this side channel window → greybox scenario
- Security in the blackbox scenario does not imply security under the greybox scenario

Timing side-channel

CROCS
Centre for Research on Cryptography and Security

Timing side-channel: PIN verification

- Software for PIN code verification

```
Input: 4-digit PIN code
Output: PIN verified or rejected
Process CheckPIN (pin[4])
int pin_ok=0;
if (pin[0]==5)
   if (pin[1]==9)
      if (pin[2]==0)
         if (pin[3]==2)
            pin_ok=1;
         end
      end
   end
end
return pin_ok;
EndProcess
```

We will look at power consumption of a similar function :-)

- What are the execution times of the process for PIN inputs `[0,1,2,3]`, `[5,3,0,2]`, `[5,9,0,0]`
- The execution time increases as we get closer to `[5,9,0,2]`

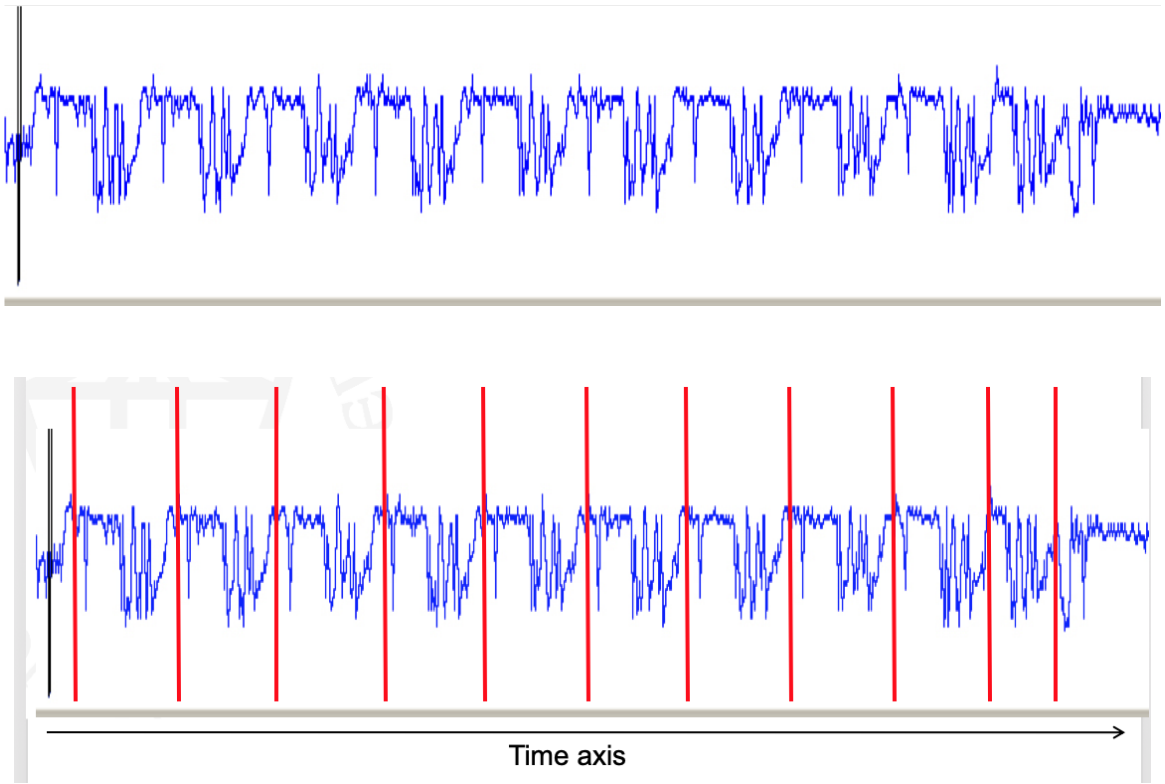
CROCS
Centre for Research on Cryptography and Security

Simple Power Analysis (SPA)

- Based on one or a few measurements
- Mostly discovery of data-(in)dependent but instruction-dependent properties e.g.
  - Symmetric:
    - Number of rounds (resp. key length)
    - Memory accesses (usually higher power consumption)
  - Asymmetric:
    - The key (if badly implemented, e.g. RSA / ECC)
    - Key length
    - Implementation details: for example RSA w/wo CRT

CROCS
Centre for Research on Cryptography and Security

SPA example 1



SPA on RSA (Square-and-Multiply)

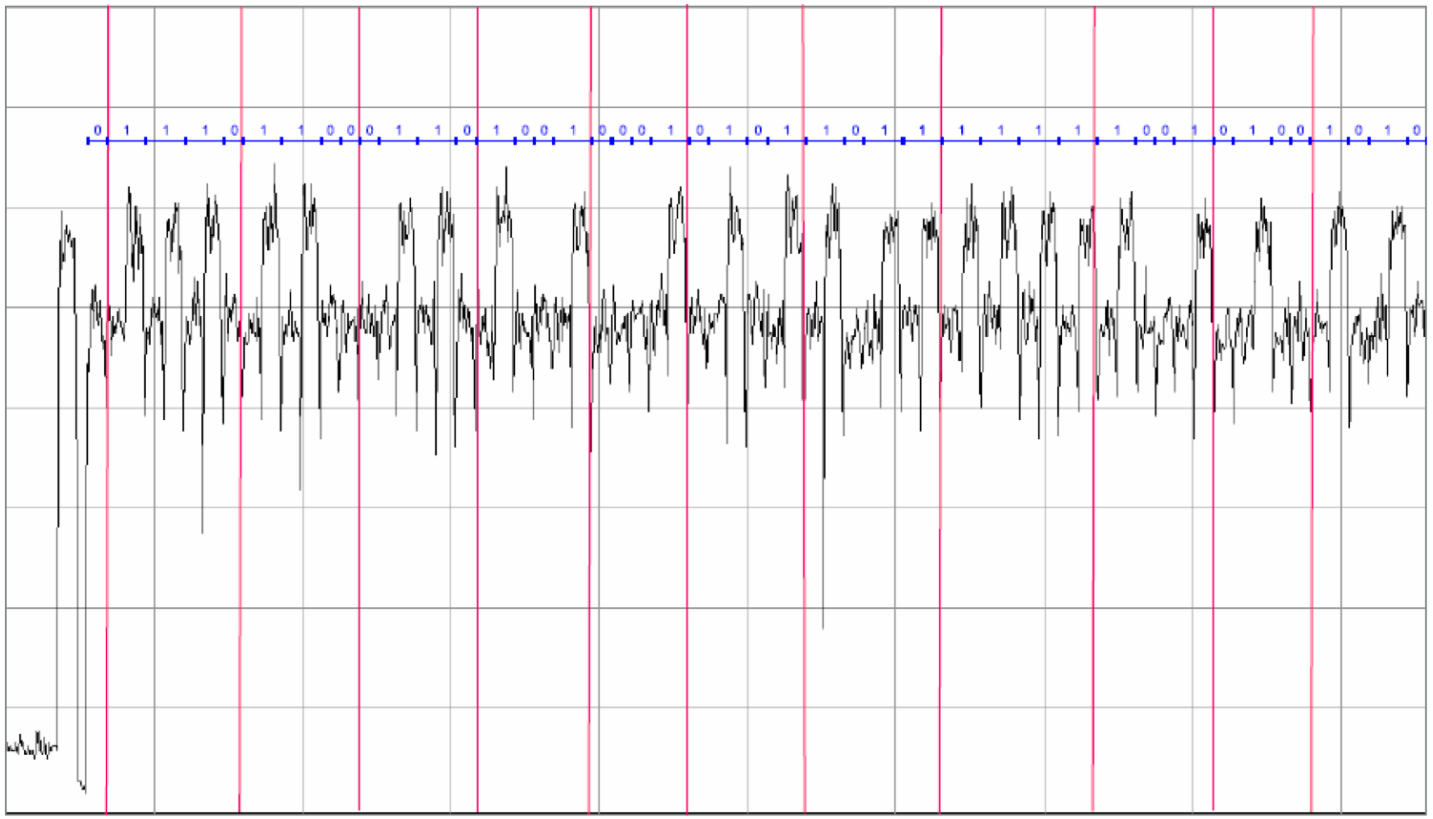
- RSA modular exponentiation

```
Input: integers x, e, n, length l of e
Output: x^e mod n

Process ModularExponentiation(x, e, n, l)

r=1;
for j=l-1 down to 0
   r=r^2 mod n //square
   if (bit j of e) == 1
      r= r*x mod n //multiply
end
return r;
EndProcess
```

- Do you already see a timing attack?
- The exponent-dependent branch is causing it!
- Do you see another side-channel attack?

CROCS
Centre for Research on Cryptography and Security

SPA example 2: RSA exponentiation



- Differential Power Analysis (DPA)

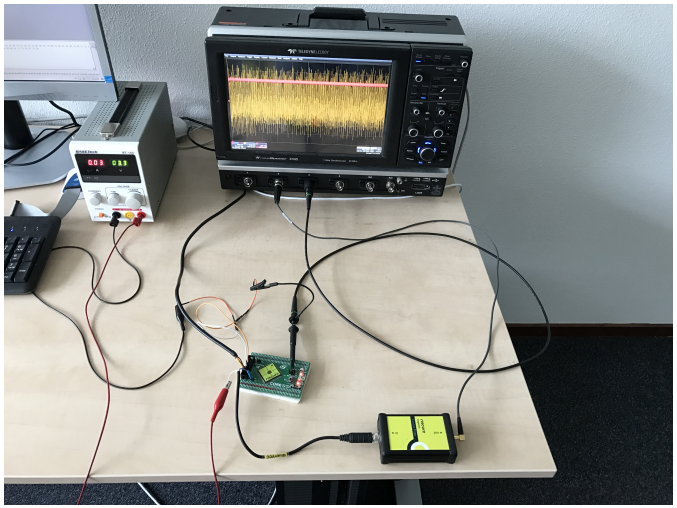
ChipWhisperer

ChipWhisperer

What is chipwhisperer?

To perform a side channel attack, two things is needed,

1. A capture hardware:
   oscilloscope: captures small signals with a precisely synchronized clock.
2. A target board:
   processor: is programmed to perform secure operation.



Setting up the hardware for side channel attacks is not easy!
CW1101 ChipWhisperer-Nano resolves difficulties, but hard to be customized!

CW1101 ChipWhisperer-Nano:

- comes with the capture hardware and the target together on a single board.
- has ARM Cortex-M0 processor.
- we have 20 of them in the lab (and 2 CW1173 ChipWhisperer-Lite based on ARM Cortex-M4F)

CROCS Centre for Research on Cryptography and Security

CW1101 ChipWhisperer Nano

The ChipWhisperer Nano comes with two main parts:

1. a multi-purpose power analysis capture hardware, and
2. a microcontroller (target board) which you can implement algorithms onto.

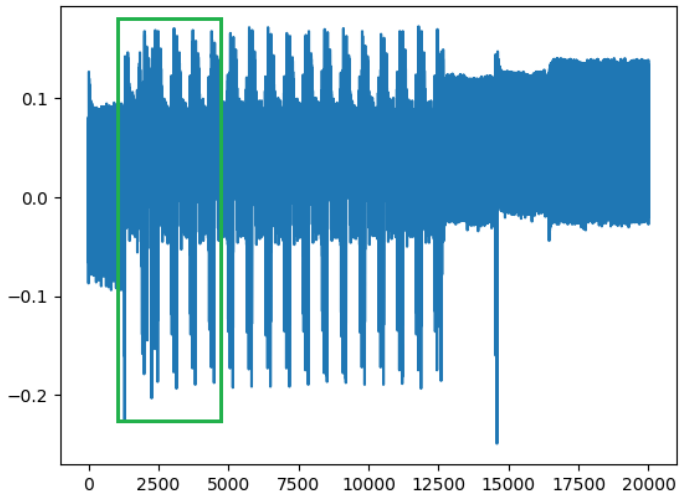


Figure: Figure from: https://myrelabs.com/breaking-rsa-with-chipwhisperer/

Documentation can be found at:

- https://www.newae.com/products/NAE-CW1101
- https://chipwhisperer.readthedocs.io/en/latest/
- https://wiki.newae.com/Main_Page.

CROCS
Centre for Research on Cryptography and Security

CW1101 ChipWhisperer Nano (Cont'd)

Open-source toolchain for hardware security research and education

Hardware: The ChipWhisperer uses a capture hardware and a target board.

- Schematics and PCB layouts for capture hardware & target board

Firmware: Three separate pieces of firmware are used on the hardware.

- The capture hardware:
  a USB controller (in C) & an FPGA for high-speed captures (in Verilog)
  In "hardware/capture" of the ChipWhisperer Github Repo.
- The target device has its own firmware (mostly in C)
  In "hardware/victims/firmware" of the ChipWhisperer Github Repo.

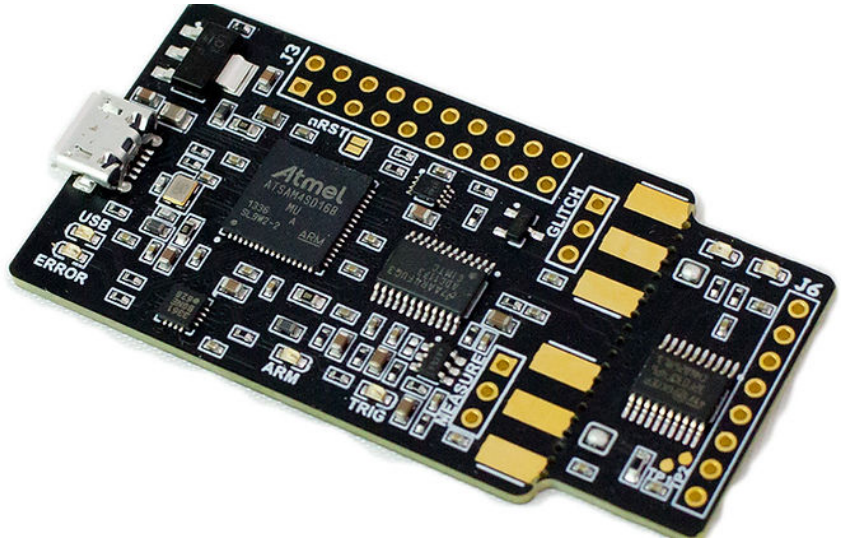
Software: The ChipWhisperer software includes

- a Python API for talking to hardware (Capture), and
- a Python API for processing power traces from hardware (Analyzer).

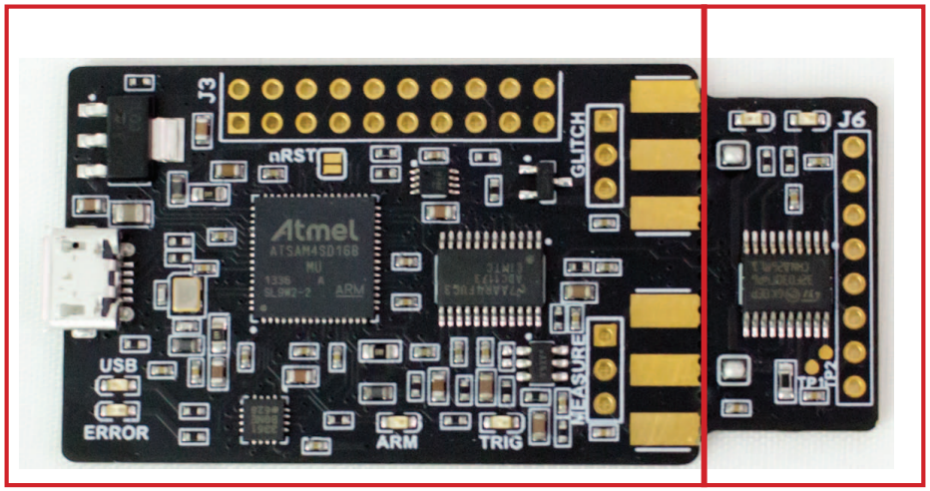
CROCS
Centre for Research on Cryptography and Security

Hardware Specification

- Hardware documentation can be found at: https://rtfm.newae.com
- More specifically look to: https://media.newae.com/datasheets/NAE-CW1101_datasheet.pdf



Hardware Specification



Feature	Notes/Range
ADC Specifications	8-bit ADC, 20 MS/s maximum sample rate.
ADC Sample Clock Source	Selectable between internal generator or external input.
Analog Input	AC-Coupled, fixed gain.
GPIO Types	Serial, clock, logic line (i.e., for reset pin). Fixed pin functions.
GPIO Voltage	3.3V.
Clock Options	3.75 MHz, 7.5 MHz, 15 MHz, 30 MHz , 60 MHz
Clock Output Type	Generated by microcontroller, clock only (no clock glitching support).
Trigger Type (ADC + Glitch)	Rising edge only.
Glitch Width (min)	~20nS (depends on cabling used for routing glitch output).
Glitch Offset	~200nS jitter, adjustable in 10nS increments.
Voltage glitch type	Low-power crowbar circuitry.
Crowbar pulse current	4A.
USB Interface	Custom USB firmware (full-speed USB 2.0 device).
Sample Buffer Size	50 000.
Target Device	STM32F030F4P6 or STM32F070
Programming Protocols	STM32Fx Bootloader

Figure: from https://media.newae.com/datasheets/NAE-CW1101_datasheet.pdf

- **REMARK:** there are different versions of ChipWhisperer, see https://rtfm.newae.com/Capture/

Hardware set up

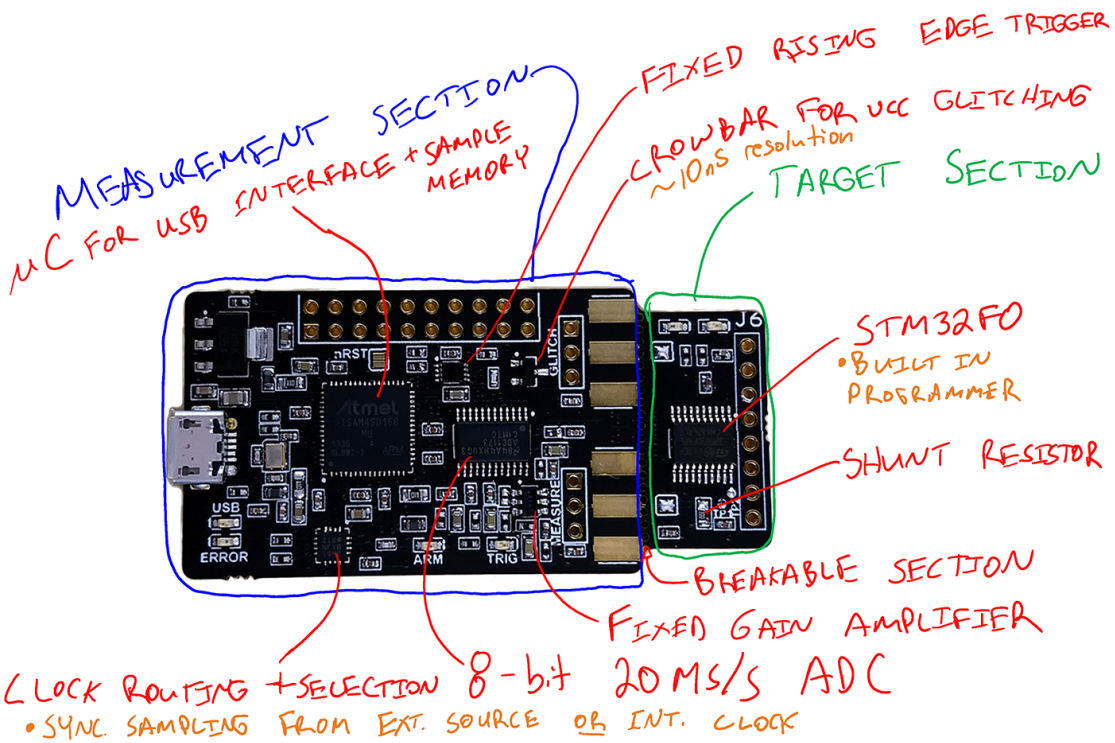


Figure: from https://rtfm.newae.com/Capture/ChipWhisperer-Nano/

Use a micro USB cable to connect the ChipWhisperer to a computer
Done? Then,

follow software guide at https://chipwhisperer.readthedocs.io/en/latest/

CROCS
Centre for Research on Cryptography and Security

Software installation

Chipwhisperer has an open-source Python library for

controlling the capture hardware and
communicating with the target.

There are two modes (basic & advanced) for chipwhisperer installation.

There are two ways for basic installation

- Windows Installer
- Virtual Machine (VirtualBox)

There are different choices for advanced installation and prerequisites

- GNU/Linux (preferred)
- Windows
- Mac OS X
- Virtual machine (Virtual Box)

Detailed documentation can be found at:
https://chipwhisperer.readthedocs.io/en/latest/index.html.

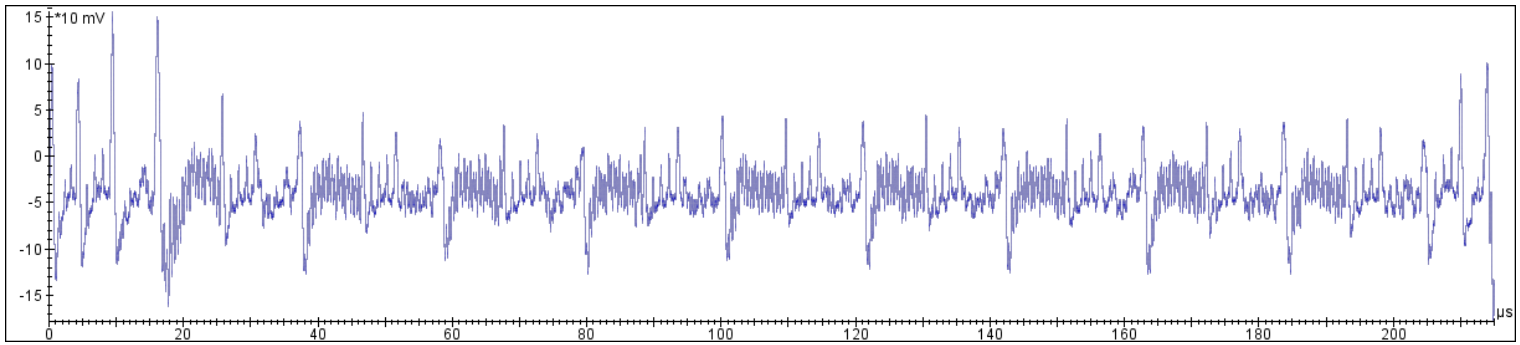
In this seminar we use the Virtual Box method:
https://chipwhisperer.readthedocs.io/en/latest/virtual-box-inst.html.

CROCS
Centre for Research on Cryptography and Security

Practical Side-channel Analysis

Practical Side-channel Analysis:
Acquisition of traces and SPA

Side-channel Traces

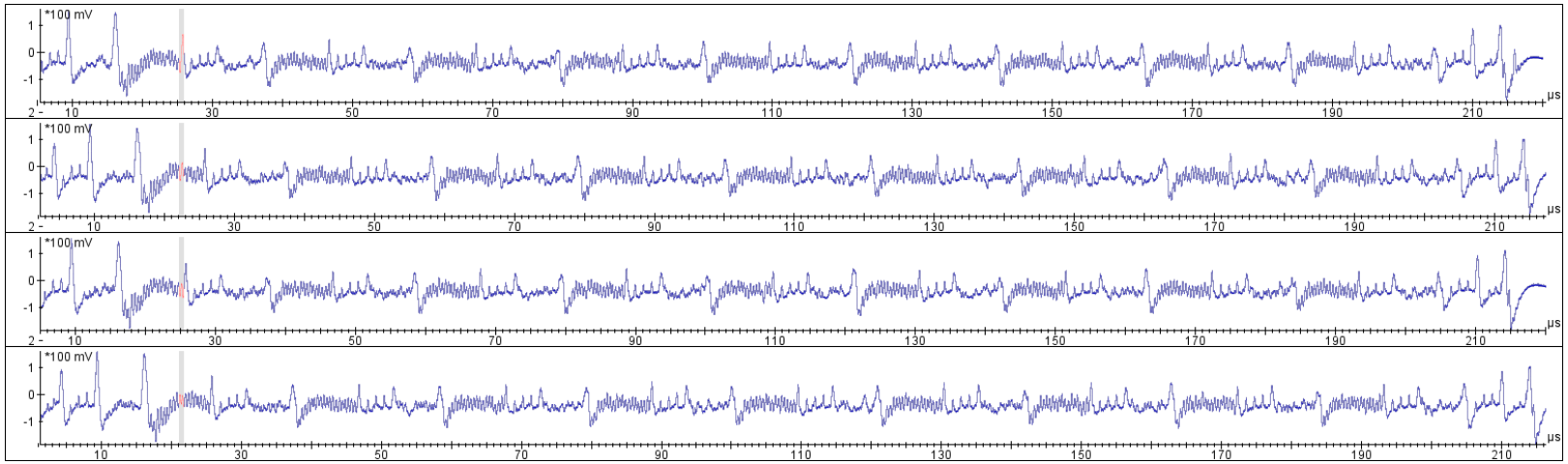


- What it is? AES
- What are typical side-channels? power, EM, time, sound, temeperature, light...
- smartcards vs. embedded devices
- What to do first? Build the setup :-)

CROCS
Centre for Research on Cryptography and Security

Problems with Side-channel Traces

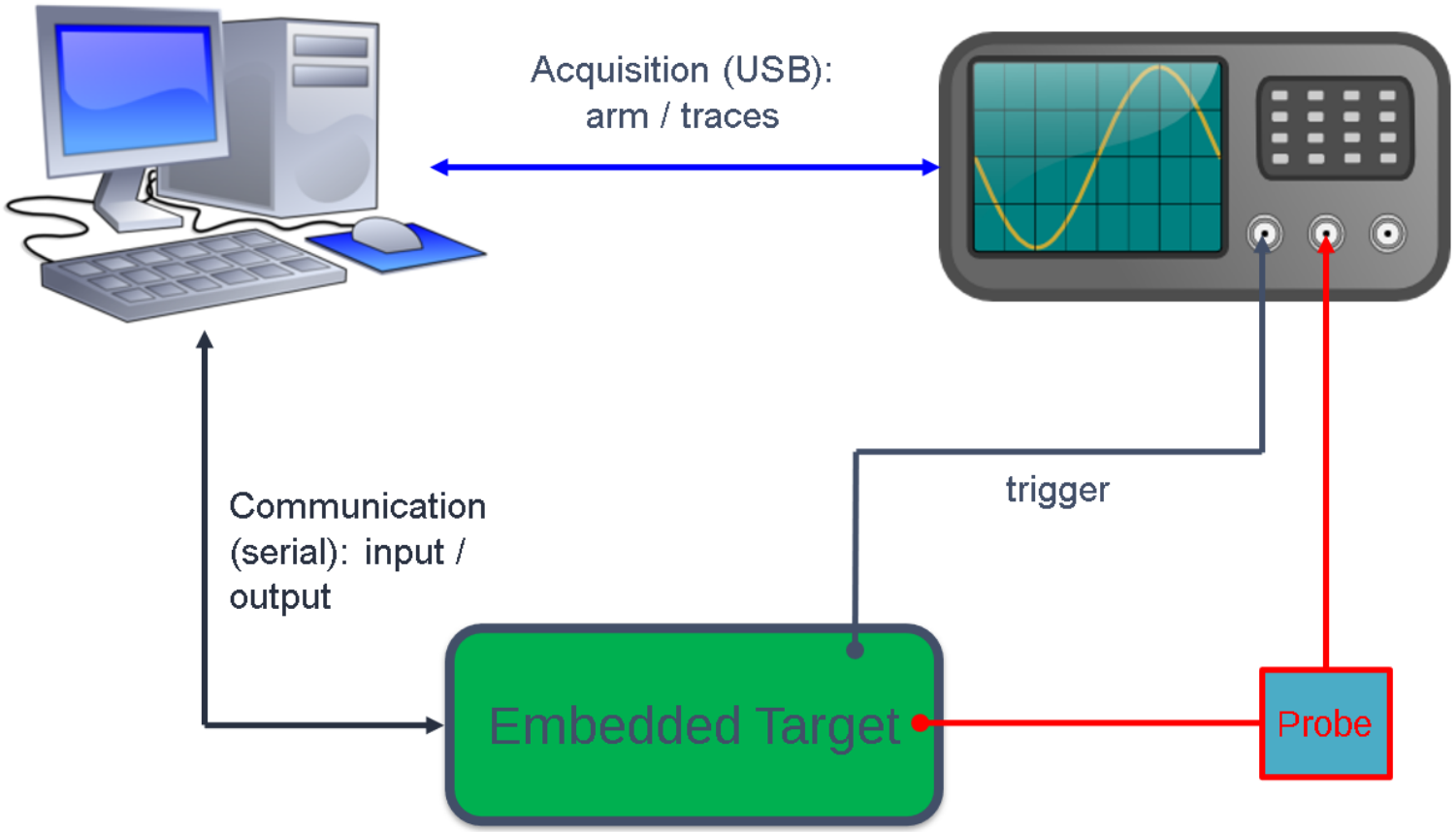
- Misalignment:



- Noise
- How to minimize these problems?
- (1) Build a good “enough” setup.
- (2) Do processing of the traces (e.g., alignment, compression, etc.).
- (3) Attack and profit.

CROCS
Centre for Research on Cryptography and Security

Typical Setup Components



Test Excersise: Capturing AES traces with ChipWhisperer

- Even if your setup works please work in pairs.
- If you installed everything then upload `Excercise_Acquisition_CPA.ipynb` in `http://localhost:8888/notebooks/jupyter/courses/sca101/` and run it.
- Try to capture a few traces and plot them. what do you see?
- What do you think is happening?

CROCS
Centre for Research on Cryptography and Security

Main Excersise: PIN

- Even if your setup works please work in pairs.
- If you installed everything then upload `Power Analysis for Password Bypass-SPA.ipynb` in `http://localhost:8888/notebooks/jupyter/courses/sca101/` and run it.
- Password-checking is implemented letter by letter.
- What do you see?
- What do you think is happening?

CROCS
Centre for Research on Cryptography and Security

Conclusions

- The main goal of this seminar is to introduce Side-Channel Analysis by experimenting with ChipWhisperer.
- Simple Power Analysis.
- Thank you for the attendance :-)

CROCS
Centre for Research on Cryptography and Security

Questions

?