



This work is distributed
under the CC BY-SA license,
unless stated otherwise.

Hardware Security

8. Physical side-channel attacks 1 (passive)

Ján Jančár

Summer 2026

Today

- Overview
- Semi-invasive and Invasive attacks
- Non-invasive passive attacks (SCA)

Physical side-channel attacks

What we will spend the rest of the course on

Next few weeks

- Physical side-channel attacks 1 (passive)
- Physical side-channel attack defences (passive)
- Physical side-channel attacks 2 (passive)

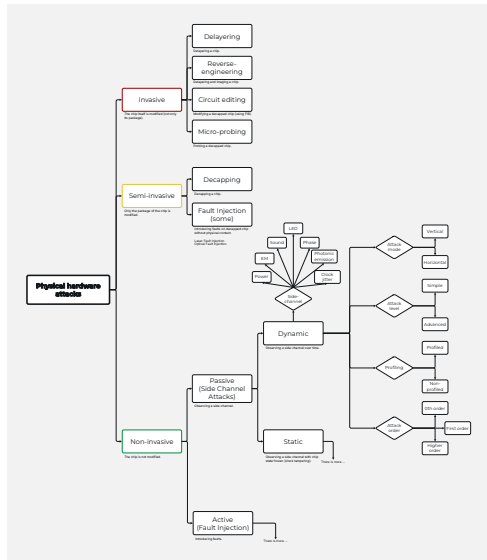
- Physical side-channel attacks 3 (active)
- Physical side-channel attack defences (active)

- Guest lecture: **Thomas Roche**
- Guest lecture: **Łukasz Chmielewski**
- Certifications & Recap

Physical side-channel attacks

Overview

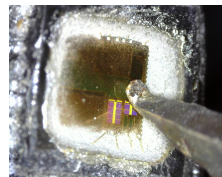
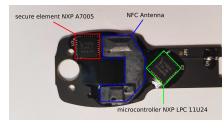
- Non-invasive
 - Target is not modified/damaged
 - Passive
 - ▶ Side-channel analysis (**SCA**)
 - ▶ Attacker observes
 - Active
 - ▶ Fault injection (induction, **FI**)
 - ▶ Attacker tampers/injects faults
- Semi-invasive
 - Target is modified, but only its package
 - **Decapping**
 - Fault injection (some)
- Invasive
 - Target is modified/damaged
 - Delaying
 - Reverse-engineering
 - **Micro-probing**
 - **Circuit editing**



Semi-invasive attacks

Decapping

- Decapsulation
 - Removing the chip cover
 - Revealing the raw die
- Techniques
 - Chemical (100€ – 1 000€)
 - Laser (10 000€ – 40 000€)
 - Mechanical (200€ – 20 000€)
- Necessary for some other attacks/steps
 - Reverse-engineering
 - Micro-probing
 - Fault injection
 - EM analysis
 - Circuit editing

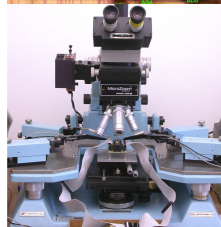
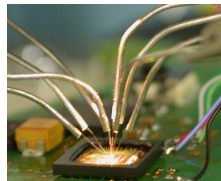


Side Journey to Titan

Invasive attacks

Micro-probing

- Decap
- Remove some layers of the chip
 - Laser cutting
 - Etching
 - Focused Ion Beam
- Micro-probe (5 000€ – 300 000€)
- Capture or inject signals into internal components



Invasive attacks

Circuit editing

- Focused Ion Beam (80 000€ – 1 000 000€)
 - Shoots a beam of Gallium ions
 - Can remove or deposit material
- Requires decapping
- Also used **constructively**
 - To edit a chip after manufacture

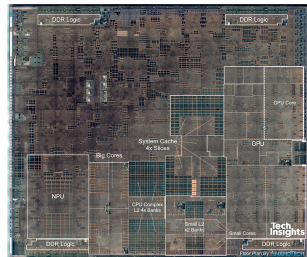


commons.wikimedia.org/wiki/File:Fib.jpg

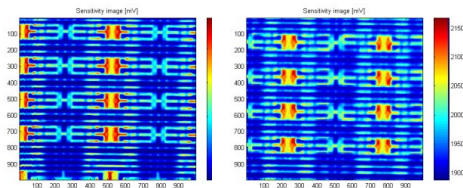
Invasive attacks

Reverse-engineering

- Attacks usually require knowledge of the target
 - The more you know, the easier it gets
- Targets
 - Data/code in ROM/RAM/Flash
 - Chip hardware itself
- Techniques
 - Decap + image
 - ▶ Offered as a commercial service
 - ▶ [texplained.com](https://www.texplained.com)
 - ▶ [techinsights.com](https://www.techinsights.com)
 - ▶ [chiprebel.com](https://www.chiprebel.com)
 - Lasers + EM
- Talk by Christopher Tarnovsky
- Silicon Prawn
- Constructive use case
 - How do you know you have a genuine/unmodified device?
 - Supply chain attack/hardware trojan detection



anandtech.com:AppleA12dieshot

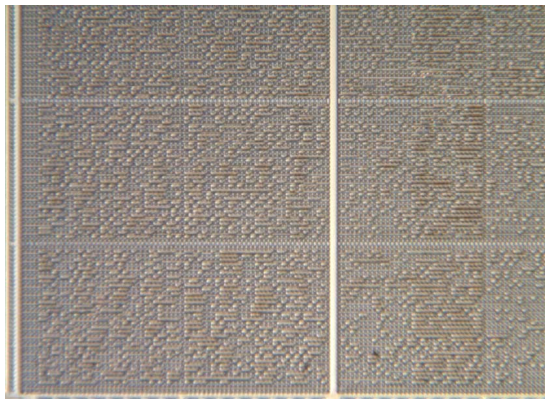


<https://www.cl.cam.ac.uk/archive/rja14/Papers/SISW02.pdf>

Invasive attacks

Reverse-engineering (ROM)

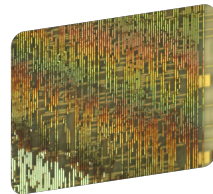
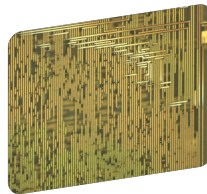
- Decap
- Etch selectively
- Image
- Read out ROM data/code



cl.cam.ac.uk/~sps32/ahsa2017_prob.pdf

Invasive attacks

Reverse-engineering (Mifare)



media.ccc.de/v/24c3-2378-en-mifare_security

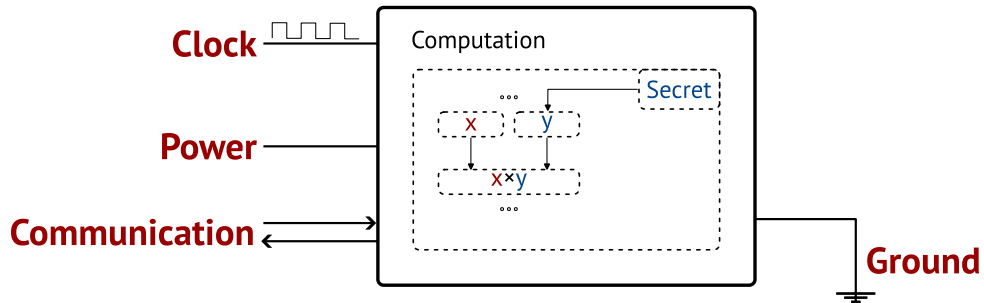
- Used computer vision techniques (2007)
- Mapped the whole logic circuit
- Recovered the Crypto1 cipher + logic



Non-invasive passive attacks

Observing the leakage

Target



Non-invasive passive attacks

Cryptographic implementations

What are we attacking?

⚙️ Hardware

- Actual circuit for computing the cryptographic function
 - AES Encrypt/Decrypt, RSA Sign, ...
- “*cryptographic accelerator*”
- Verilog

</> Software

- Cryptographic function implemented in code
 - ECDH, ECDSA, ...
- Generic ISA
- C, Assembly

⚙️ Software + Hardware

- Certain operations done in hardware
- Crypto-specific instructions
 - Modular arithmetic
 - Elliptic curve point addition
 - Elliptic curve scalar multiplication
- C, Assembly

❓ Why do we care?

➡ Different leakage behavior

- Hardware: May be parallel
- Software: Usually serial
- Hardware: Circuit
- Software: Instruction execution

Non-invasive passive attacks

Attack type

Dynamic

- 90%
- Target is running
- State is observed somehow
 - Power
 - EM radiation also via Bluetooth/WiFi
 - Sound
 - Light (LEDs)
 - Photonic emission
 - Clock jitter
 - Phase
- Attacker gets a **trace**: measurement of leakage over time
- Our focus

Static

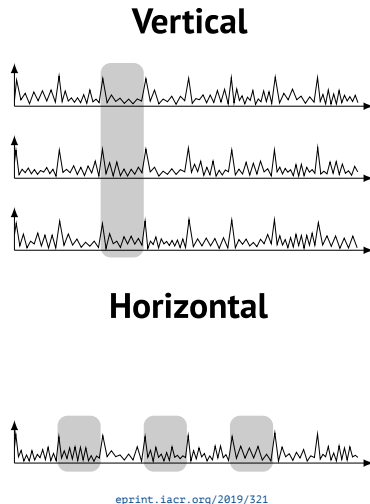
- 10%
- Target is stopped (via clock manipulation)
- State is measured somehow
 - Power
 - Impedance Analysis
 - Laser Logic State Imaging



Non-invasive passive attacks

Attack mode

- Vertical
 - Analyze the same area in many traces
 - SPA, DPA, CPA, ...
- Horizontal
 - Analyze different areas in the same trace
 - Big Mac attack, Horizontal correlation analysis, ...



Non-invasive passive attacks

Attack level

- Simple
 - One or a few traces
 - SPA
- Advanced
 - Many traces, statistical techniques, **distinguisher**, **leakage model**
 - DPA, CPA, MIA, ...

Non-invasive passive attacks

Profiling

- Profiled
 - Attacker has access to the same model of target device
 - ▶ They control the device, can set their own secrets
 - Attacker **profiles** the leakage with known secrets
 - TA, DL, ...
- Non-profiled
 - Attacker does not profile the leakage
 - SPA, DPA, CPA, ...

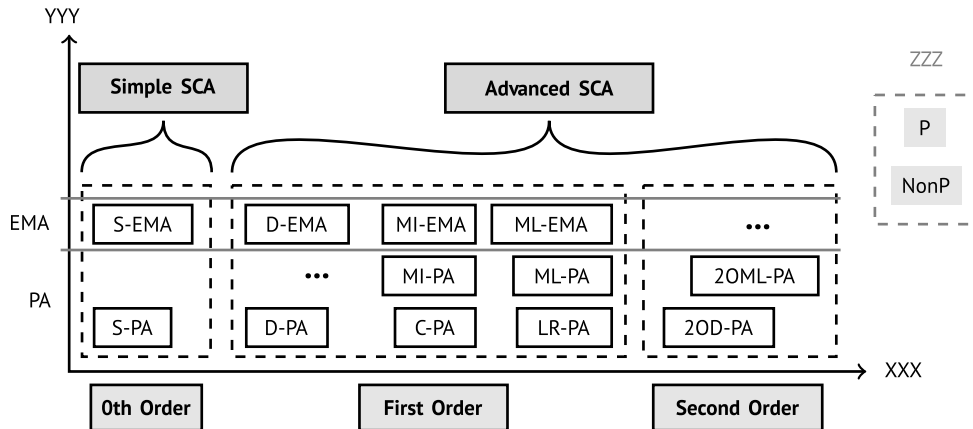
Non-invasive passive attacks

Attack order

- 0th order
 - Secret leaks directly
 - Execution(s) with fixed public input
 - SPA
- First-order (univariate)
 - Secret leaks from statistical observation of a **single** intermediate value
 - Execution(s) with varying public input
 - DPA (1st order), CPA (1st order), ...
- Higher-order (multivariate: 2nd, 3rd, ...)
 - Secret leaks from statistical observation of **multiple** intermediate values
 - Execution(s) with varying public input
 - DPA ($\geq$ 2nd order), CPA ($\geq$ 2nd order)

Non-invasive passive attacks

Attack overview



eprint.iacr.org/2019/321

Side-channels

- Timing
- Power
- EM radiation also via Bluetooth/WiFi
- Sound
- Light (LEDs)
- Photonic emission
- Clock jitter
- Phase

Power

- Sum of power consumption of all logic cells
- Why does power consumption of a chip vary?
 - ⊕ Transistor switching
- Each cell
 - P_{stat} : Static power consumption
 - ▶ Leakage current through transistors
 - P_{dyn} : Dynamic power consumption
 - ▶ Occurs when (part of) a logic cell switches
- Total
 - $0 \rightarrow 0, 1 \rightarrow 1$: Only P_{stat}
 - $0 \rightarrow 1, 1 \rightarrow 0$: Also P_{dyn}
 - Thus, P_{total} is **data-dependent!**

Side-channels

Electro-magnetic (EM) radiation

- EM emissions: Localized fields radiated by voltages and currents
 - Electric field (E)
 - Magnetic field (H)
- Each wire/cell
 - Static fields
 - ▶ E_{stat} : From static logic states (e.g., wire held at VDD)
 - ▶ H_{stat} : From static leakage currents
 - Dynamic fields
 - ▶ E_{dyn} : From changing voltages
 - ▶ H_{dyn} : From transient current spikes
- Static field is **invisible** to a probe
 - H-field probes: **Changing** H-field induces current in probe
 - E-field probes: **Changing** E-field capacitively influences the probe
- Fields are distributed around components radiating them
- Thus, EM radiation is **data-dependent** and **localized**!

Leakage models

- How does the leakage (power consumption) relate to the data/state that is being computed?
- Power consumption is **additive**
 - $P_{\text{total}} = P_{\text{stat}} + P_{\text{dyn}} = \sum_i P_{\text{stat}_i} + P_{\text{dyn}_i}$ (across cells)
- Operation leakage vs data leakage (model)
 - $P_{\text{total}} = P_{\text{op}} + P_{\text{data}} + P_{\text{el. noise}} + P_{\text{const}}$
- **Experiments**
 - Exp. 1: Execute fixed operation with fixed data
 - Exp. 2: Execute fixed operation with varying data
 - Exp. 3: Execute varying operation with fixed data

Side-channels

Leakage models (Exp. 1)

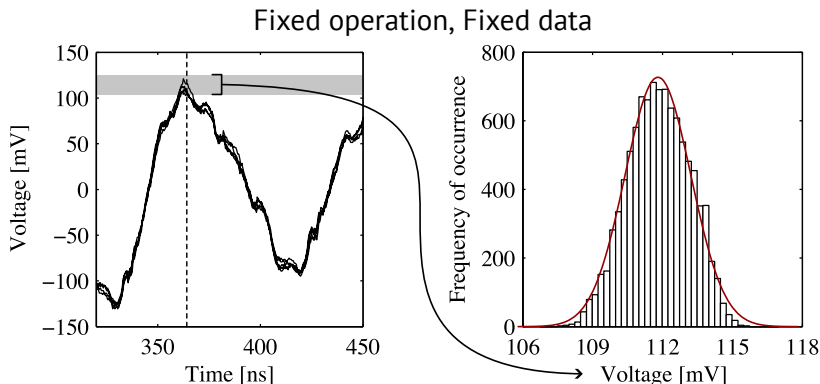


Figure 4.1. Power traces look very similar if the same data is processed.

Figure 4.2. Histogram of the power consumption at 362 ns of Figure 4.1.

Power analysis attacks

Thus $P_{\text{el. noise}}$ is approximately normally distributed $N(0, \sigma)$

Side-channels

Leakage models (Exp. 2)

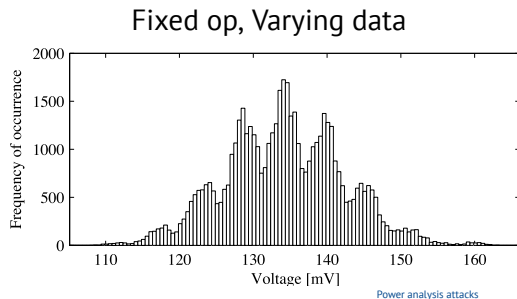


Figure 4.4. Histogram of the power consumption at 362 ns if different data values are transferred from the internal memory to a register.

- There are 9 peaks, why?
 - This is an 8-bit microcontroller
 - The power consumption depends on the Hamming weight (number of set bits)
- Thus P_{data} is (inversely) proportional to the Hamming weight of data
- Why?
 - Count the transistors that need to switch from an all-1 state

Side-channels

Leakage models (Exp. 2)

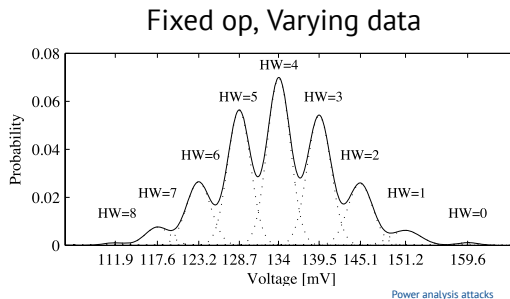


Figure 4.5. The distribution of the power consumption when the microcontroller transfers different data from the internal memory to a register.

- There are 9 peaks, why?
 - This is an 8-bit microcontroller
 - The power consumption depends on the Hamming weight (number of set bits)
- Thus P_{data} is (inversely) proportional to the Hamming weight of data
- Why?
 - Count the transistors that need to switch from an all-1 state

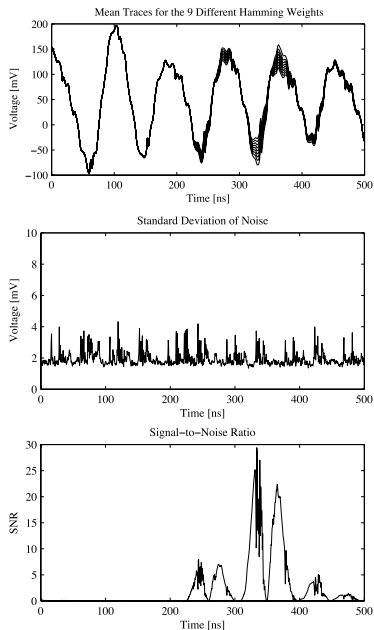
Leakage models

- Hamming weight
 - Leakage is (inversely) proportional to the **Hamming weight** of the intermediate value
 - $L(x) = HW(x)$
- Hamming distance
 - Leakage is (inversely) proportional to the **Hamming distance** between subsequent intermediate values
 - $L(x, x') = HD(x, x')$
- Which model to choose?
 - Depends on the target
 - It is a model anyway

Side-channels

Leakage models

Power analysis attacks



Hardware (Power / EM)

■ Digital sampling oscilloscope (DSO)

- Sampling rate (100 MS/s – 5 GS/s)
 - ▶ How fast can it sample?
- Bandwidth (5 MHz – 10 GHz)
 - ▶ How high-frequency can it get?
- Sample memory (10k – 2G samples)
 - ▶ How much can it store?
- Resolution (8 – 12 bits)
 - ▶ How precise is each sample?
- Trigger
 - ▶ How can you trigger the measurement?
- Interface (USB, Ethernet)
 - ▶ Can it stream?

■ Power supply

- Low noise

■ Probe

- Power
 - ▶ Ordinary
 - ▶ Differential
 - ▶ Current
- EM
 - ▶ H-field/E-field

■ Filters

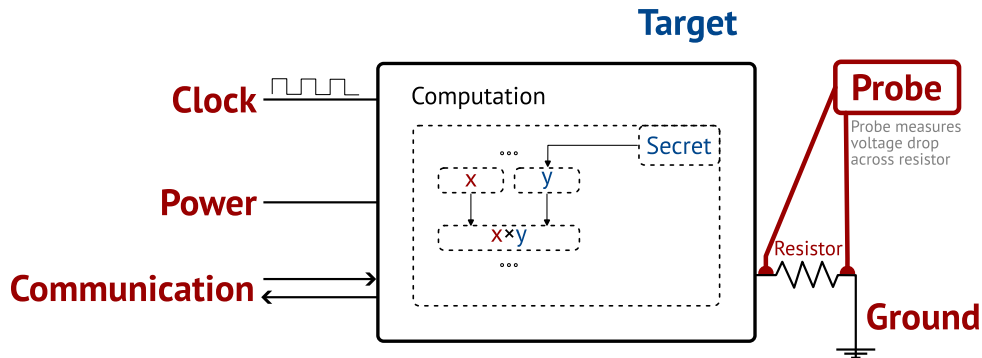
- Low-pass/Band-pass/High-pass

■ Amplifiers

- Low noise

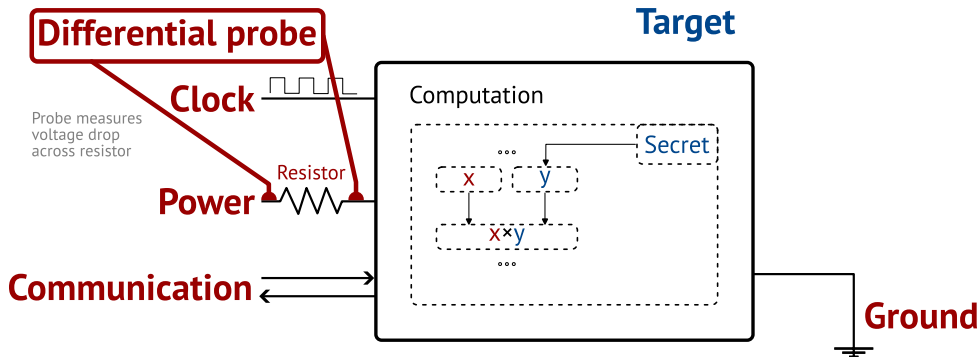
Practical setup

Power measurement



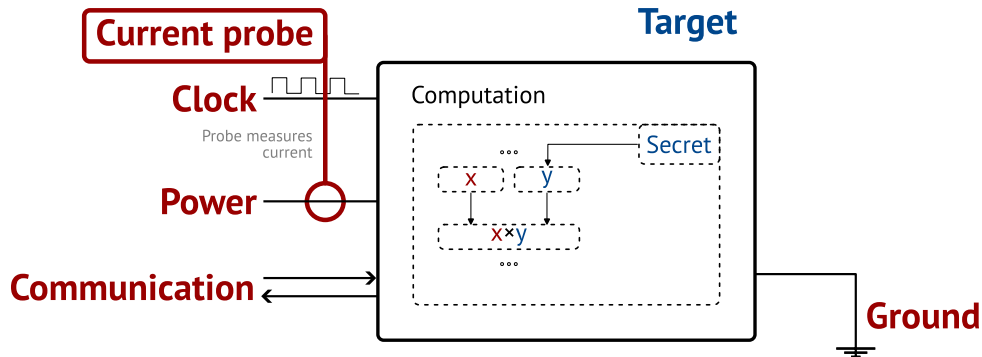
Practical setup

Power measurement



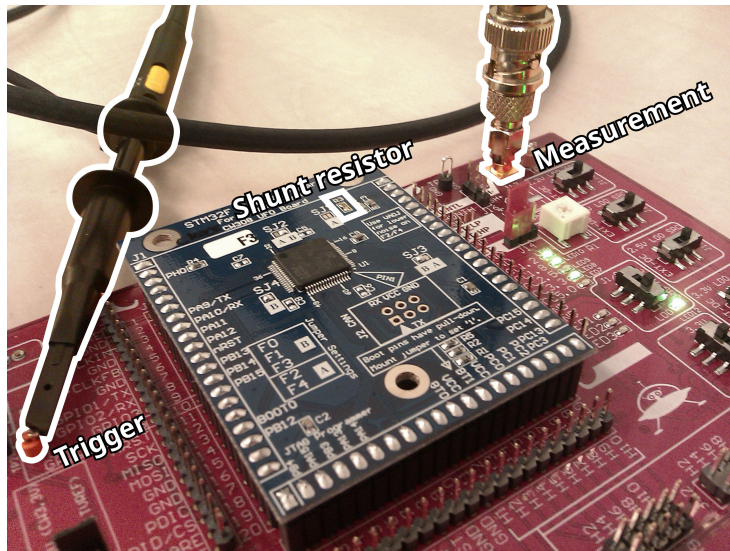
Practical setup

Power measurement



Practical setup

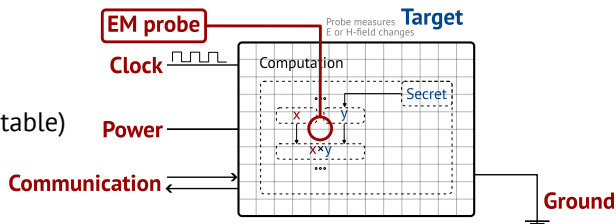
Power measurement



Practical setup

EM measurement

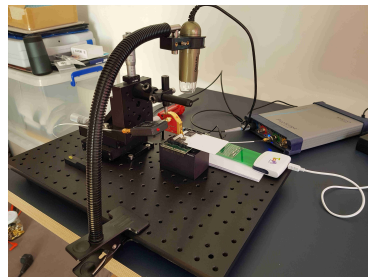
- EM radiation is localized
- Probe position matters
- Solution
 - Precise positioning system (XYZ table)
 - Grid search



Practical setup

EM measurement

- EM radiation is localized
- Probe position matters
- Solution
 - Precise positioning system (XYZ table)
 - Grid search

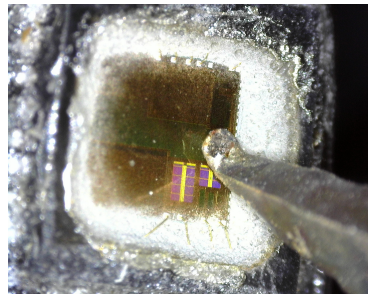


Side Journey to Titan

Practical setup

EM measurement

- EM radiation is localized
- Probe position matters
- Solution
 - Precise positioning system (XYZ table)
 - Grid search

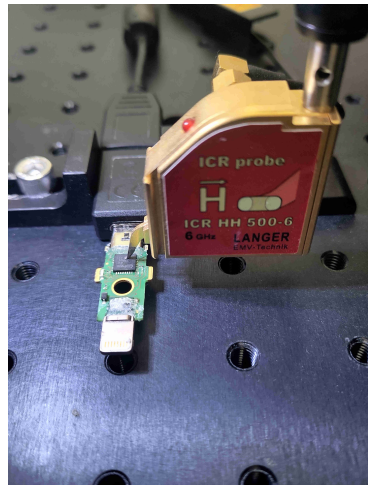


Side Journey to Titan

Practical setup

EM measurement

- EM radiation is localized
- Probe position matters
- Solution
 - Precise positioning system (XYZ table)
 - Grid search

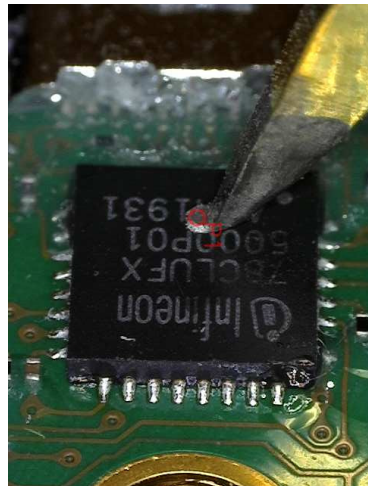


EUCLEAK

Practical setup

EM measurement

- EM radiation is localized
- Probe position matters
- Solution
 - Precise positioning system (XYZ table)
 - Grid search



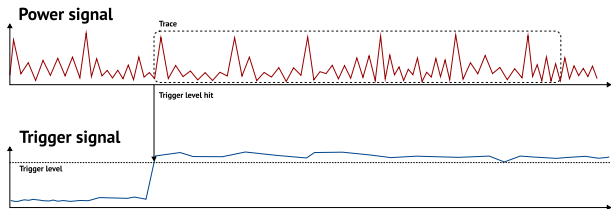
EUCLEAK

Practical setup

Acquisition

- 1 Setup target, scope, and trigger
 - Scope channels: Range, coupling, sampling rate, sample amount
 - Trigger: Level, Rise/Fall, Pattern
- 2 Arm scope
- 3 Execute operation
- 4 Get trace (or stream trace)

Repeat until enough traces



Non-invasive passive attacks

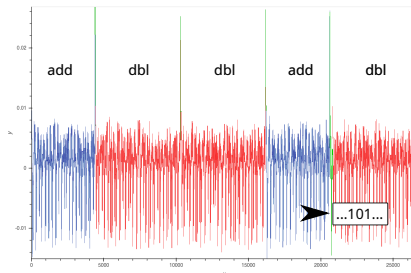
Finally, some attacks

Simple Power Analysis (SPA)

- Introduced in “*Differential Power Analysis*” by Kocher, Jaffe, Jun
- Simplest attack
 - Just **look** at the trace and read out the key
- Usually applied against operation leakage
- Double-and-add scalar multiplication

```
def scalarmult(P, k):  
    R = infy  
    for i in range(k.bit_length(), 0, -1):  
        R = dbl(R)  
        if k & (1 << i):  
            R = add(R, P)  
    return R
```

- ? Dynamic/Static? ➔ Dynamic
- ? Simple/Advanced? ➔ Simple
- ? Vertical/Horizontal? ➔ Theoretically horizontal, but no one would really call it that
- ? Order? ➔ 0th order, no actual data analysis necessary



Simple Power Analysis (SPA)

- But what if?
- Double-and-add always

```
def scalarmult(P, k):  
    R = infy  
    for i in range(k.bit_length(), 0, -1):  
        R = dbl(R)  
        if k & (1 << i):  
            R = add(R, P)  
        else:  
            dummy = add(R, P)  
    return R
```

- ❓ Any ideas?
 - ➡ We have to use data leakage
 - ➡ We have to get more traces
 - ▶ Increase the signal
 - ▶ Reduce the noise

Differential Power Analysis (DPA)

- Introduced in “*Differential Power Analysis*” by Kocher, Jaffe, Jun
- Conceptual basis of many attacks
- 1-bit DPA requires
 - Knowledge of the algorithm
 - Choosing an intermediate value
 - ▶ Needs to be computable given part of the key and public input
 - Choosing a bit of that intermediate value

Differential Power Analysis (DPA)

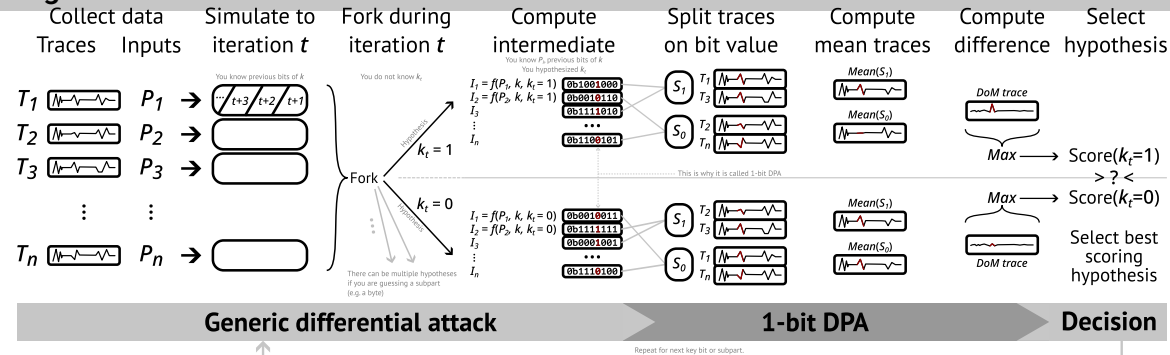
Process

- 1 Collect many traces with **random** public inputs and **fixed** secret
- 2 You know a key **subpart** k
- 3 Simulate execution
- 4 Fork based on (next) key bit or subpart k_t
 - Compute a hypothetical **intermediate value** $f(d, k, k_t)$
 - Split traces based on **chosen bit** of intermediate value
 - ▶ S_1, S_0
 - Compute the **mean traces** for set S_1 and S_0 : $Mean_1$ and $Mean_0$
 - Compute the **difference of means** (DoM) trace: $|Mean_1 - Mean_0|$
- 5 Correct guess will have a peak in the DoM trace where the intermediate value is computed
- 6 Incorrect key bit or subpart guess will have no peaks

Intuition: Correct guess $\rightarrow$ Correct split $\rightarrow S_1$ have bit value 1, S_0 have bit value 0 $\rightarrow$ Difference in leakage $\rightarrow$ Peak in DoM trace

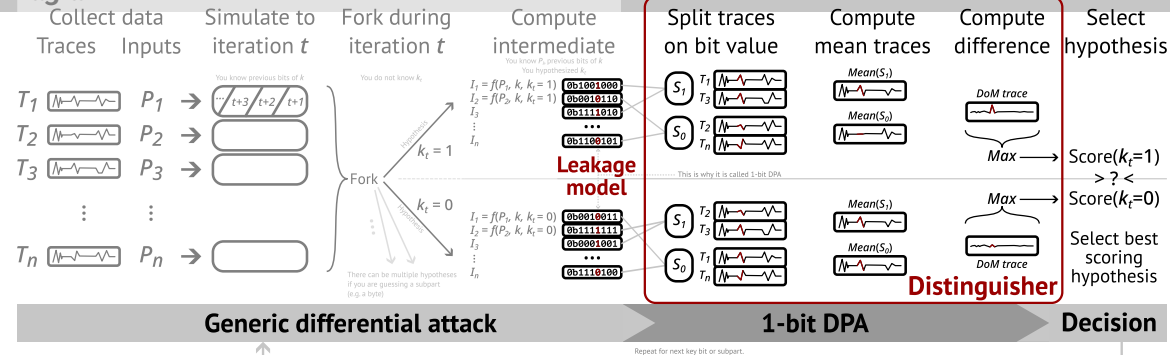
Differential Power Analysis (DPA)

Diagram



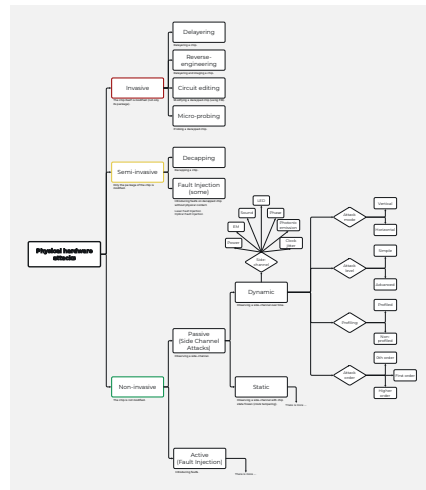
Differential Power Analysis (DPA)

Diagram



Physical side-channel attacks

- Invasive vs Semi-invasive vs Non-invasive
- Active vs Passive
- Dynamic vs Static
- Simple vs Advanced
- Vertical vs Horizontal
- Profiled vs Non-profiled
- 0th vs First order vs higher-order

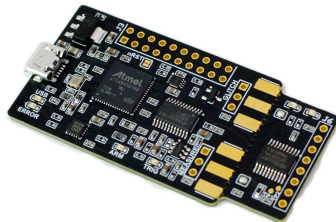


Takeaways

- What physical side-channel attacks are
- Why and how power/EM leaks data
- How SPA works
- How DPA works

Tutorial

- ChipWhisperer-Nano (x24)
- SPA/DPA on password check



Recommended reading

- For **this** lecture
 - Read [Differential Power Analysis](#)
 - ▶ The original SPA/DPA paper by Kocher, Jaffe, Jun
- For **next** lecture
 - Read Embedded Cryptography 1 – Chapter 7 – Countermeasures and Advanced Attacks
 - ▶ Focus on the countermeasures

References

- Differential Power Analysis
- EUCLEAK: Side-Channel Attack on the YubiKey 5 Series
- A Side Journey to Titan: Side-Channel Attack on the Google Titan Security Key
- Horizontal Collision Correlation Attack on Elliptic Curves
 - Nice taxonomy