Innovation Tour Point Zero Forum

Demonstration: Limits of Hardware Key Protection

01.07.2024 – Prof. Andreas Habegger

Berner Fachhochschule | Haute école spécialisée bernoise | Bern University of Applied Sciences

Live hacking – Key extraction using SCA

A cryptographic devices is attackable using side channel analysis

Target

Cryptographic devices:

- electronic devices
- implement a cryptographic algorithm
- store a secret (key)
- perform crypto operations

Channels

Side Channel Analysis (SCA)

- test points on PCB
- enabled interfaces (i.e. JTAG)
- power consumption
- electromagnetic radiation, temperature emission, etc.

Research

- ”Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, Paul Kocher
- ”Differential Power Analysis”, Paul Kocher et al.
- ”On the Importance of Eliminating Errors in Cryptographic Computations”, Dan Boneh et al.

Principles of power analysis (PA)

The power consumed in a device is composed of two types – dynamic, sometimes called switching power, and static, sometimes called leakage power.

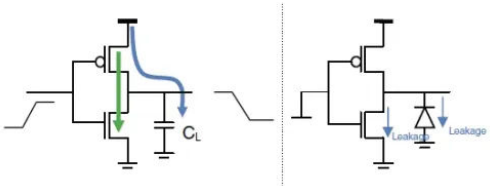


Figure: Total power is the sum of the dynamic (green) and leakage power (blue)

Source: https://semiengineering.com

- Total power is a function of switching activity, capacitance, voltage, and the transistor structure itself.
- Resulting power profile is related to work being done.

Principles of power analysis (PA)

The power consumed in a device is composed of two types – dynamic, sometimes called switching power, and static, sometimes called leakage power.

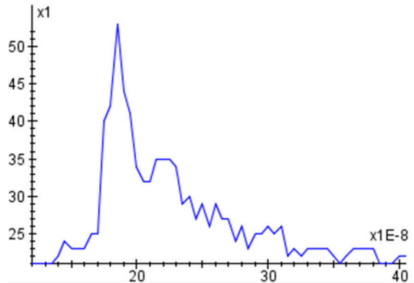


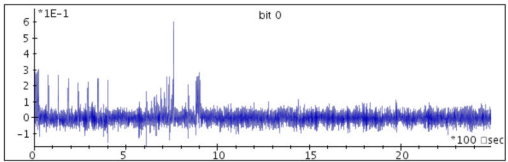
Figure: Power consumption profile during one clock cycle

Source: Riscure

- Simple Power Analysis (SPA) ⟷ time variation; pattern variation

Principles of power analysis (PA)

The power consumed in a device is composed of two types – dynamic, sometimes called switching power, and static, sometimes called leakage power.



- Differential Power Analysis (DPA) ⟷ amplitude variation; identification of data dependencies; Statistical models

- Deep understanding of cryptography, electronics, and mathematics
- High performance measurement equipment i.e. LeCroy, Keysight, R&S
- Highly specialized tooling i.e. Riscure


Live Demo

Thanks for your attention!

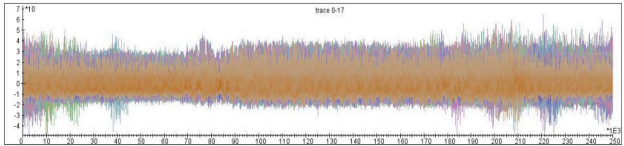


Figure: Overlaid trace set (raw data)

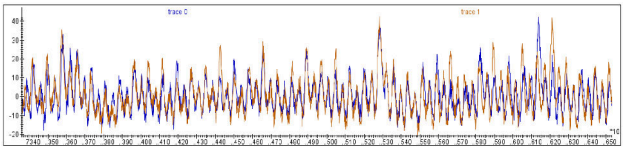


Figure: Overlaid trace set (filtered data)