Hardware attacks and software induced HW attacks and the need for separated trust anchors!

Georg Sigl

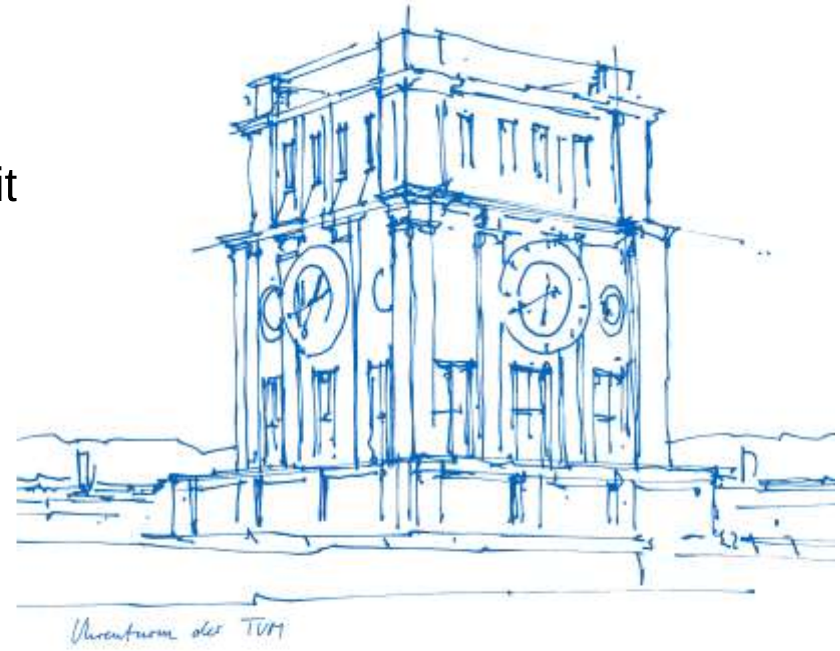
Technical University of Munich

Department for Electrical and Computer Engineering

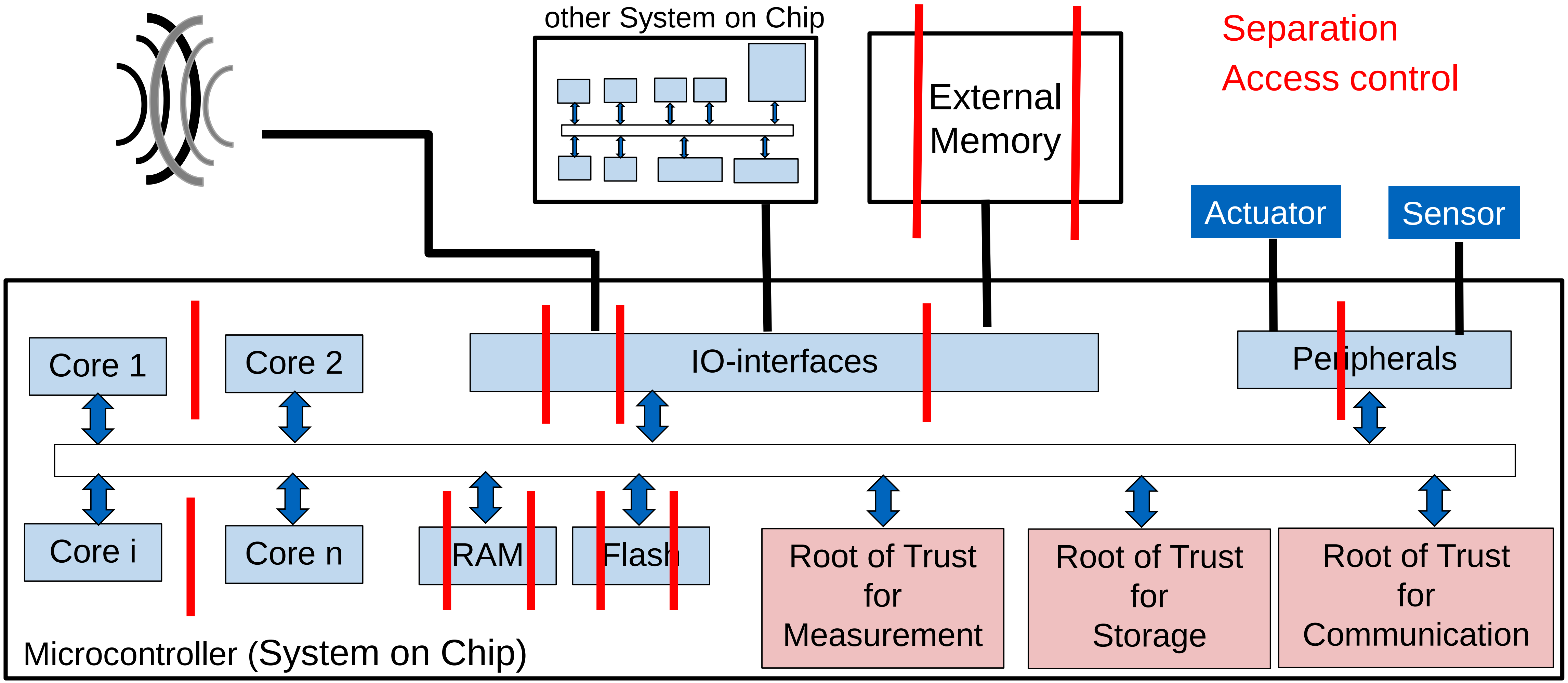
Fraunhofer Institute for Applied and Integrated Securit

October 2018

Fraunhofer
AISEC



Security in Embedded Systems



Roots of Trust

- Root of Trust for Measurement
  - Program to measure code which runs on system in order to ensure system integrity
  - Program must not be changed by any attack and execution must be in a secure/isolated environment

- Root of Trust for Storage
  - Secret key which can be used to encrypt and authenticate externally stored information
  - Key should never leave SoC
  - Key must not leak to any other party

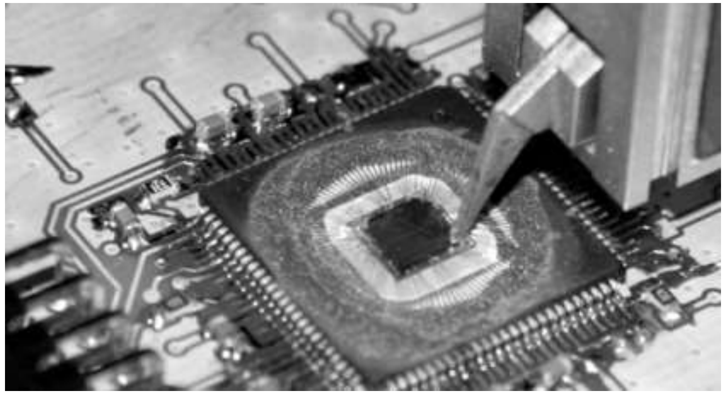
- Root of Trust for Communication
  - Asymmetric key pair for internet communication
  - Secret part of key pair must not leave SoC
  - Trusted public key of a certification authority

Attack types

- Hardware Attacks
  - Invasive
    - Reverse Engineering
    - Probing/Forcing (FIB)
  - Semi- and Non-Invasive
    - Fault Injection
    - Side Channel
- SW induced HW Attacks
  - Cache Attacks
    - Meltdown/ Spectre
    - Side Channel
  - Fault Attacks
    - Rowhammer
    - Clockskrew
- Software Attacks
  - Modification
    - Control Flow
    - Data
  - Information Extraction
    - Memory dump
    - Access control bypass

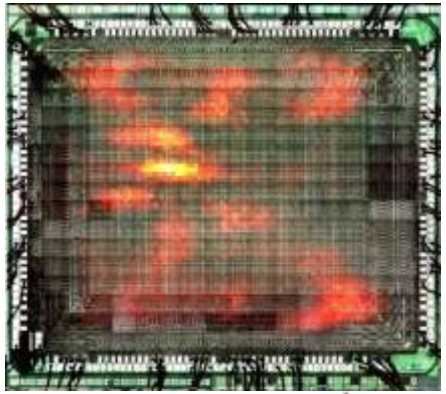
High-Resolution Magnetic Field Side-Channels

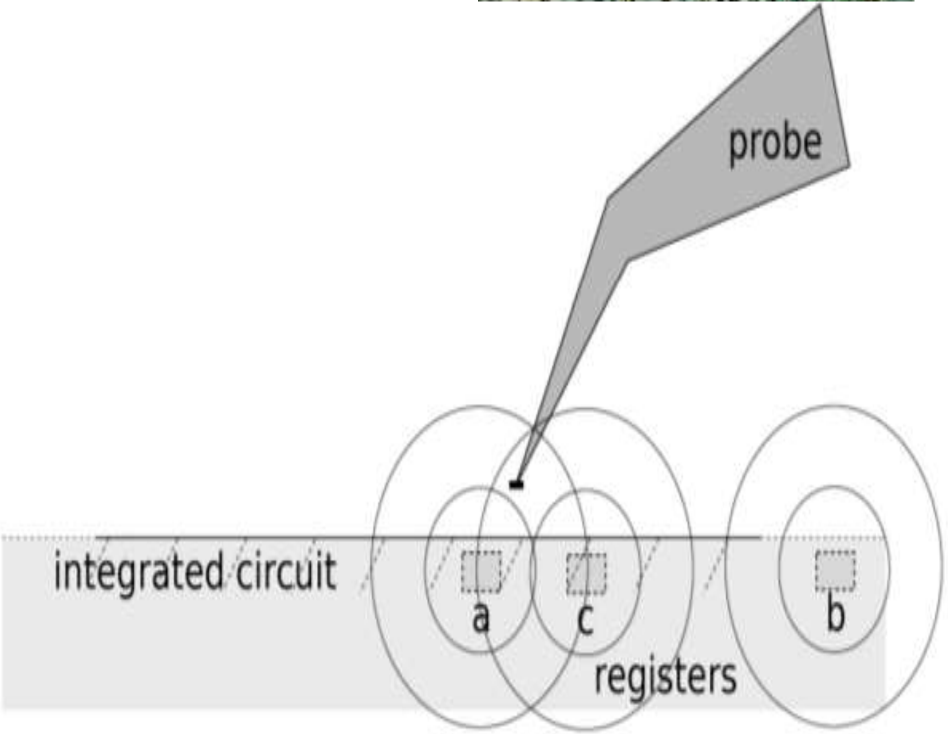
Localized EM against Asymmetric Crypto



Input: Secret $d = d_D d_{D-1} \ldots d_2 d_1$ with $d_i \in \{0, 1\}$

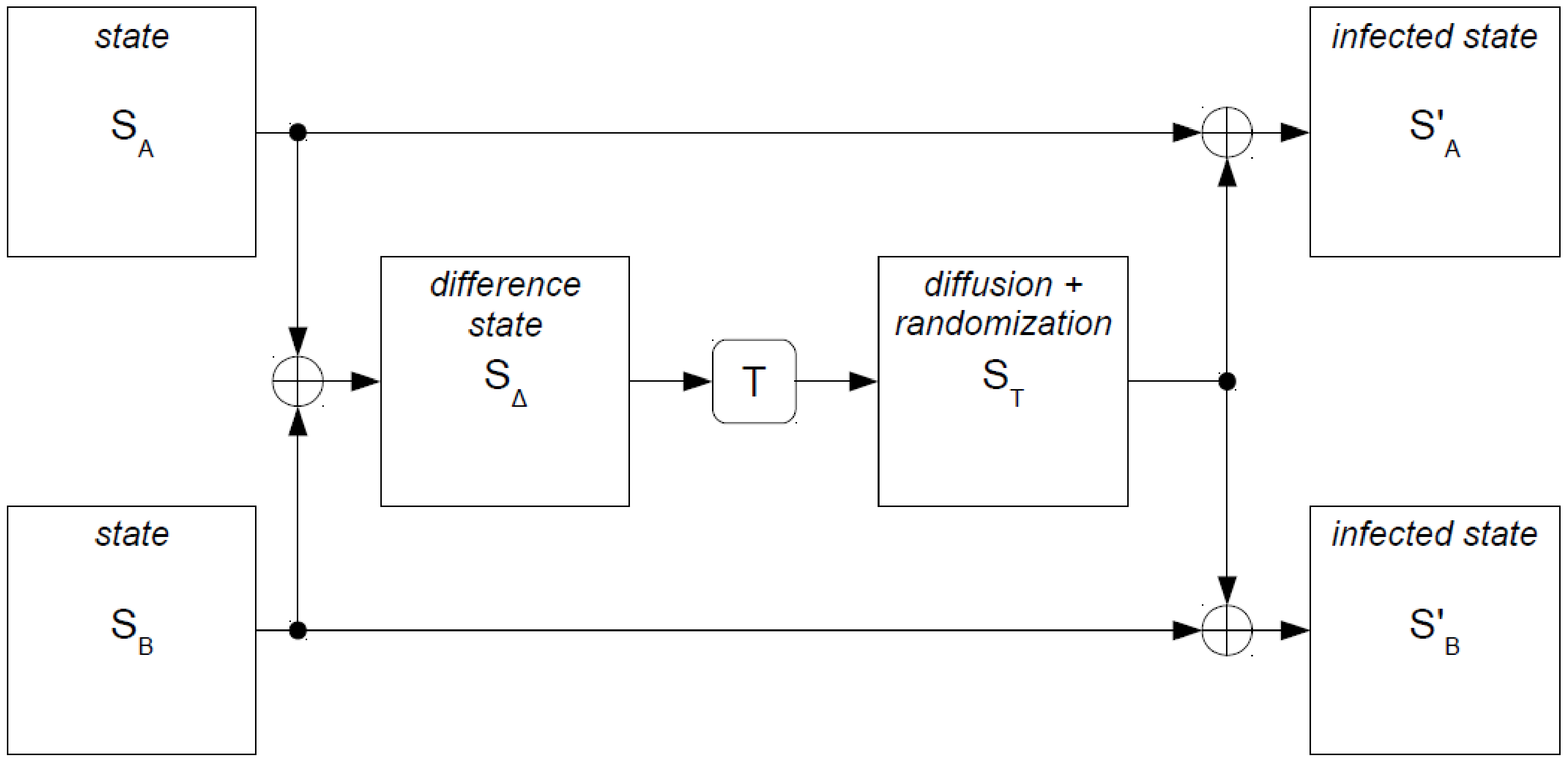
1: **for** $i = D$ downto 1 **do**
2:     **if** $d_i = 1$ **then**
3:         $c \leftarrow c^2 + a$
4:         $a \leftarrow c$
5:     **else**
6:         $c \leftarrow c^2 + b$
7:         $b \leftarrow c$
8:     **end if**
9: **end for**

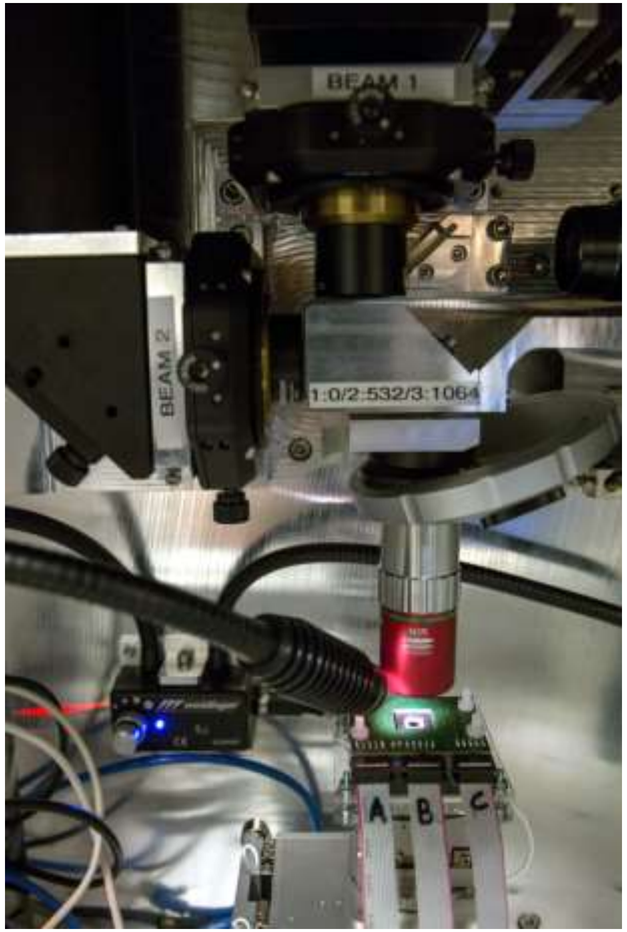




Heyszl, Johann; Mangard, Stefan; Heinz, Benedikt; Stumpf, Frederic; Sigl, Georg:
Localized Electromagnetic Analysis of Cryptographic Implementations. CT-RSA, 2012

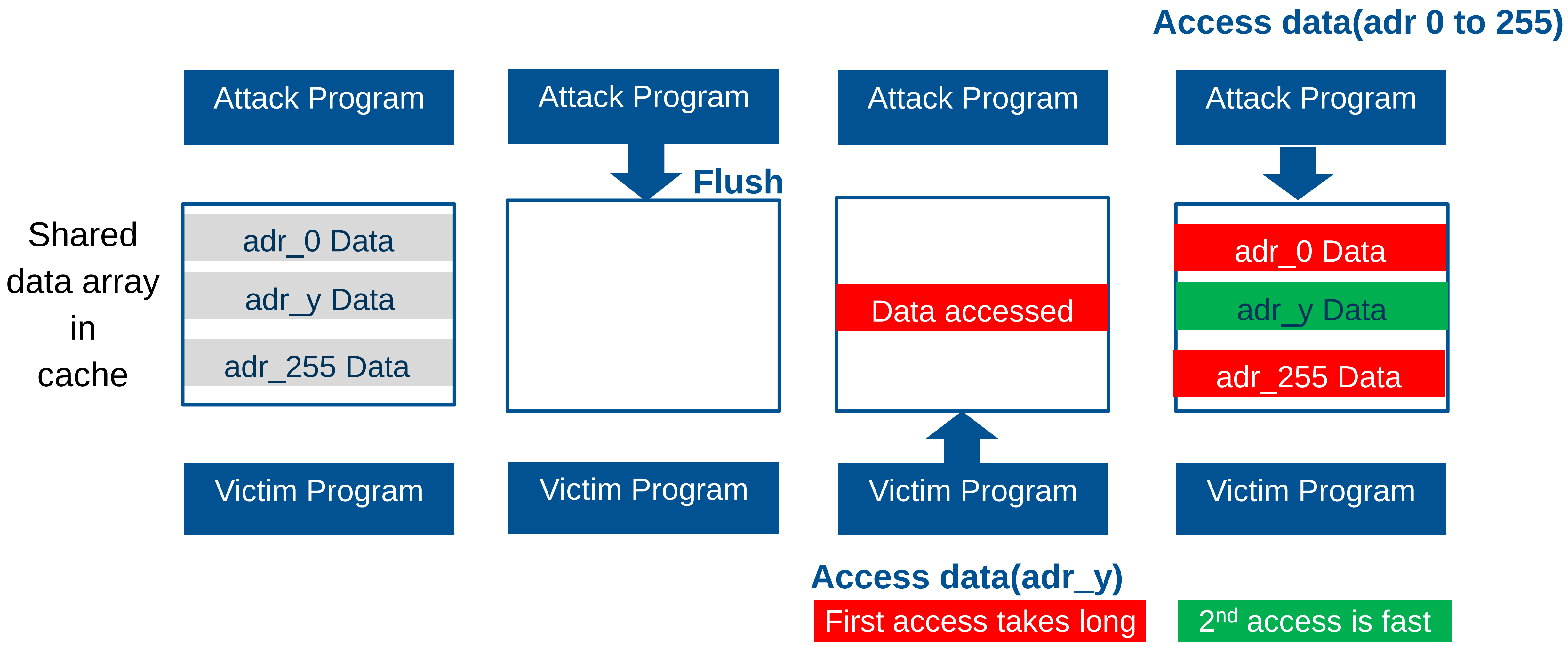
Fault Attack on an AES with a simple countermeasure



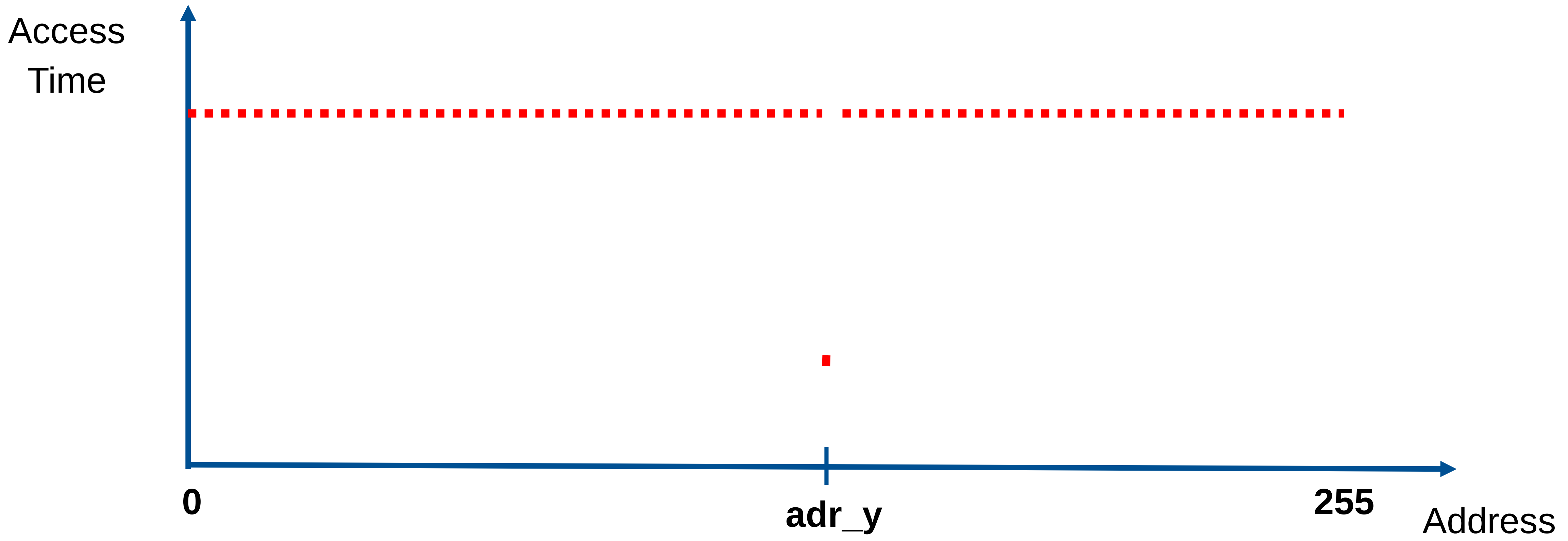


Selmke, Bodo and Heyszl, Johann and Sigl, Georg: Attack on a DFA protected AES by Simultaneous Laser Fault Injections. FDTC 2016 Fault Diagnosis and Tolerance in Cryptography, 2016

Cache Side Channel Attack: Flush & Reload



Cache Side Channel Attack: Flush & Reload



Cache Attack: Meltdown

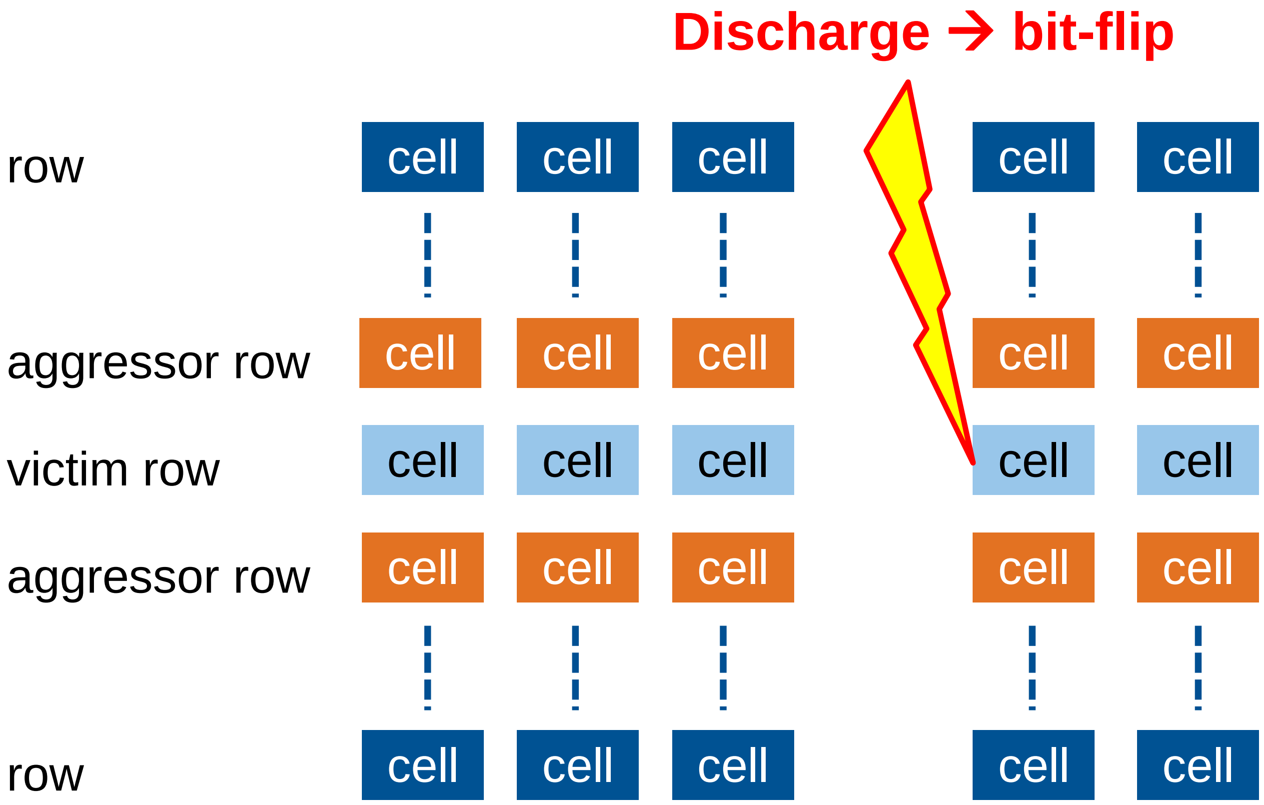
Security: MMU (Memory Management Unit) prevents data access for an attacker to the OS kernel
How to circumvent?

- Attacker trains the prefetcher with a dedicated program, e.g. a loop
- Attack program suddenly
  - accesses a byte at a memory address in kernel space
    → CPU prefetcher fetches one byte of data stored at this address in kernel space into cache
  - accesses an **array** with this byte value as index
- Then CPU detects that the branch prediction (with the access right violation) was wrong and reverts most actions, but **cache data are not deleted**
- Now the attacker accesses the complete **array** and measures access time
- The access with the shortest access time corresponds to the read byte value

Root Cause: Wrong assumption during CPU design that speculation can be undone

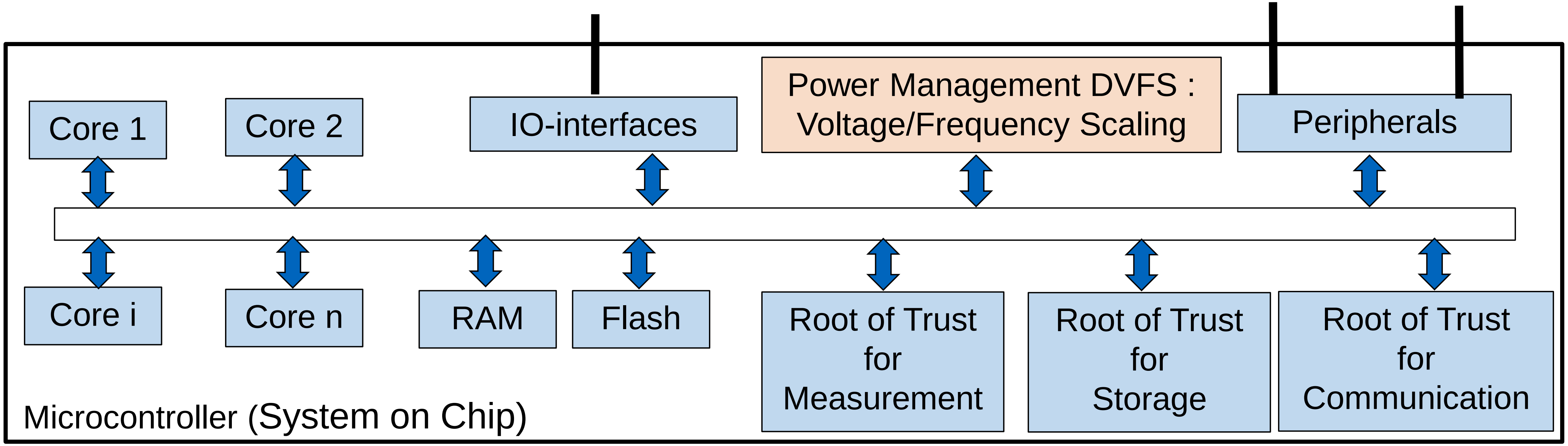
Software based fault attack: Rowhammer

- Reading frequently aggressor rows changes contents in victim
- Attacks
  - Change access rights
  - Escape sand boxes (from browser)
  - …
- Root Cause
  - DRAM considers average usage only not an attack
  - No error correction implemented (too expensive, performance?)



Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. Y. Kim, R. Daly, J. Kim, C.Fallin, J. Lee, D. Lee, C. Wilkerson, K.Lai, O. Mutlu; 2014 ACM/IEEE 41st International Symposium on Computer Architecture (ISCA)

Software based fault attack: CLKskrew



“CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management”. A.Tang, S. Sethumadhavan, and S. Stolfo, Columbia University, 26th USENIX Security Symposium, 2017

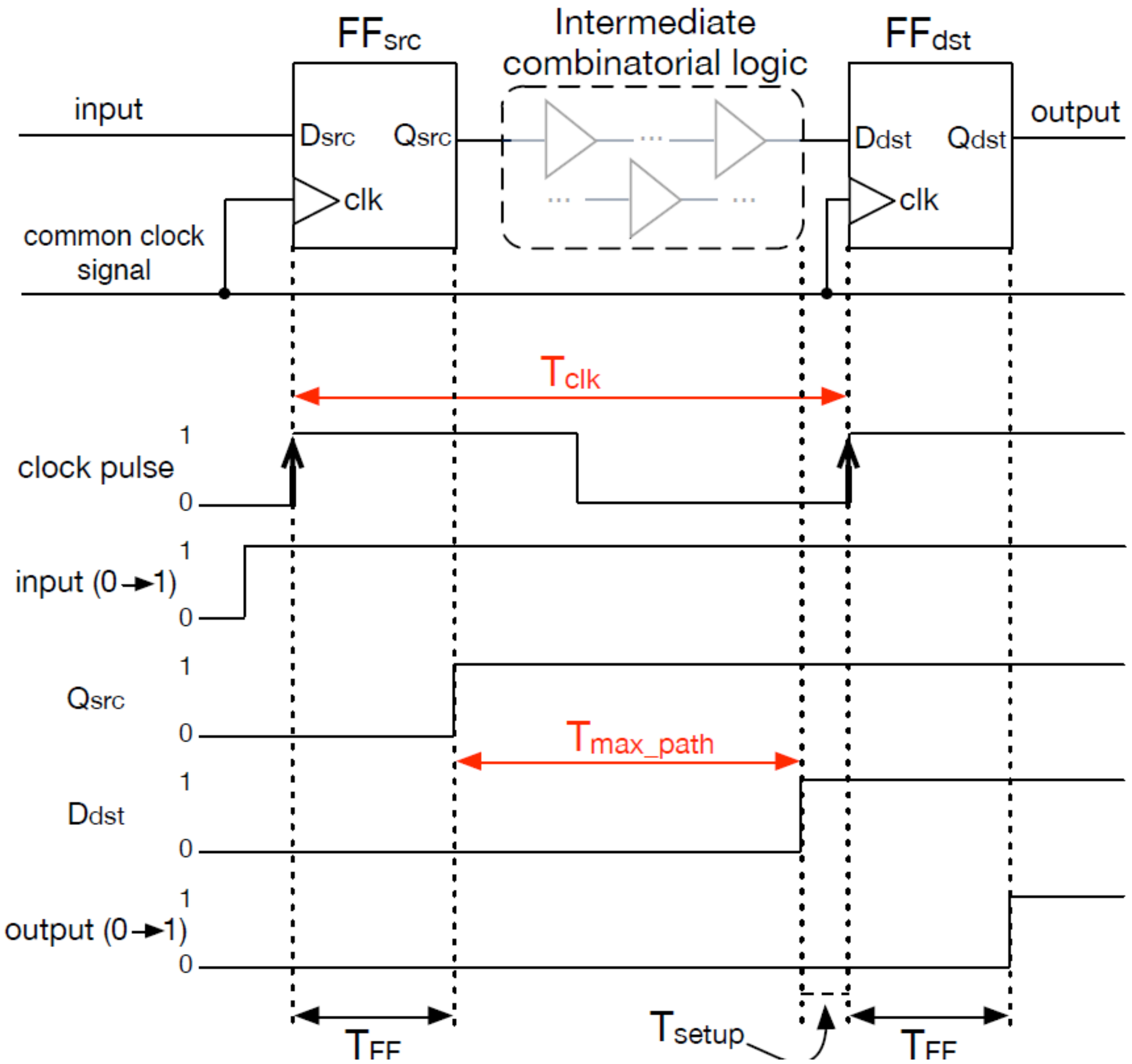
- Compromised OS kernel driver used to operate circuit beyond DVFS limits
- Faults are injected which reveal cryptographic keys and perform untrusted software download
- Attack demonstrated on ARM Trustzone in a Nexus mobile phone

The concept of voltage and frequency scaling

- Voltage reduction saves power, but
- Voltage reduction reduces performance
- → Operating frequency must be reduced

- If operating frequency is too high for a given voltage, faults occur

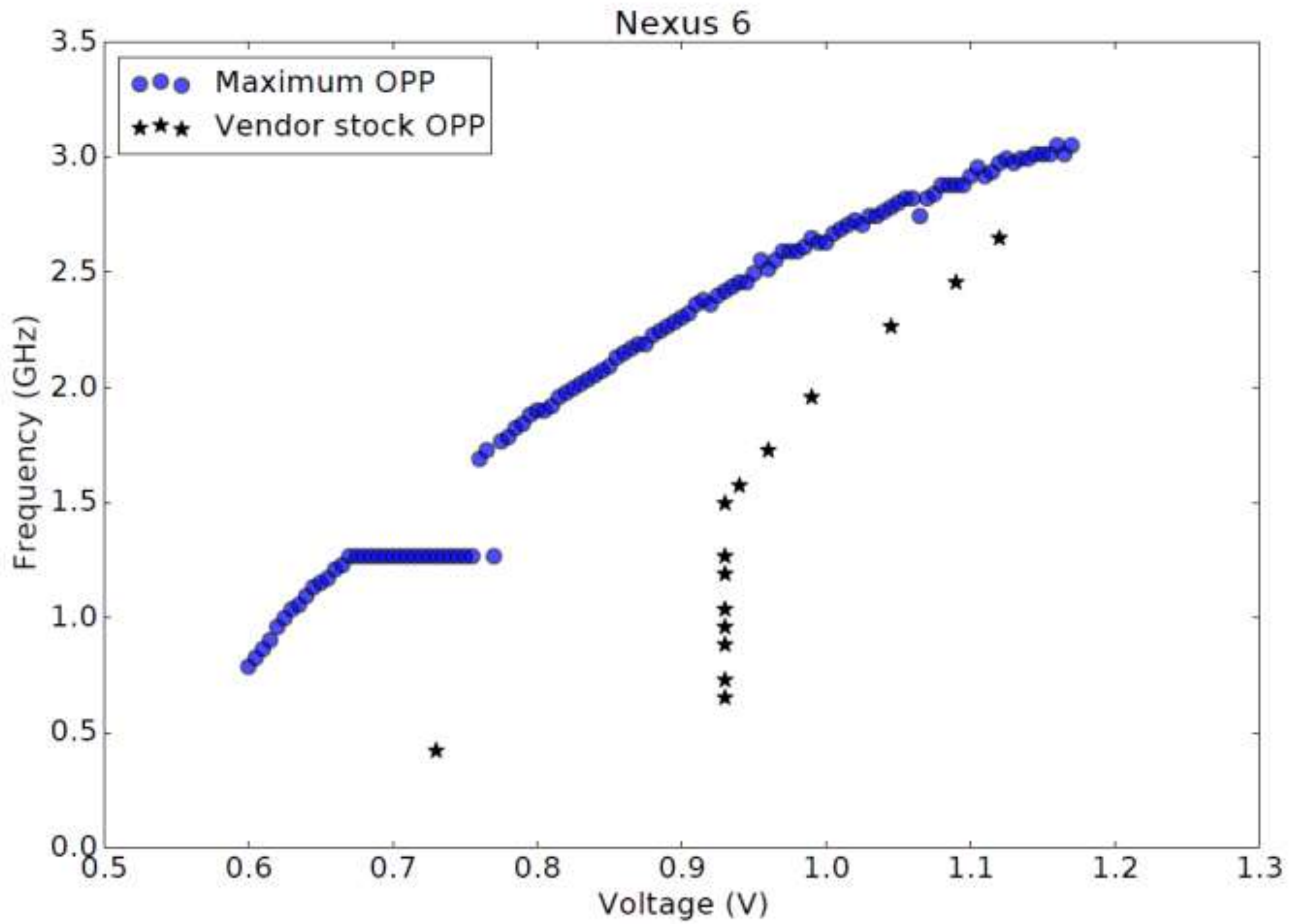
- Registers configure voltage and frequency
- In the attacked implementation voltage is configured for the complete system, but
- Clocks can be configured for each core individually



Example attacks performed with CLKskrew

- ARM TrustZone is supposed to provide an isolated trusted execution environment
- The OS kernel is able to change the clock and voltage values even when TZ code is running

- Two sample attacks have been performed:
  - Attacking AES keys of decryptions executed in TrustZone
  - Signature verification of software downloads



Intermediate conclusion

The risk is increasing!

- Increasing number of
  - Software controlled hardware features
  - Hardware functions at the reliability border
- Every software controlled hardware feature is a target for remote fault and side channel attacks
- Through side channels almost everything is observable