International Symposium on the Physical and Failure Analysis of Integrated Circuits 2018

IPFA 2018

Is Hardware Security prepared for unexpected discoveries?

Dr Sergei Skorobogatov

University of Cambridge, UK

Dept of Computer Science and Technology

UNIVERSITY OF CAMBRIDGE

Purpose

- Remind about the importance of Hardware Security
  - Growing number of devices being used in critical and sensitive applications
  - Have we learned from history of attacks?
- Highlight that mitigation is not developed in time to defeat attacks
- Present some new attacks
- Discuss predictability of attacks

Outline

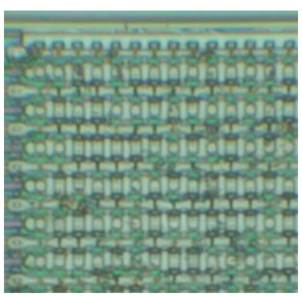
- Introduction
- History of attack technologies
- New attacks
- Discussions
- Challenges and Future work
- Conclusion

Introduction

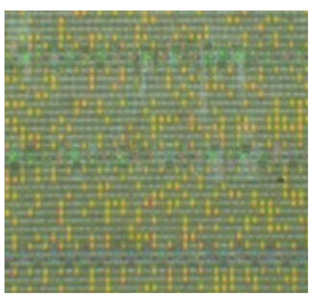
- History of disturbing physical attacks
  - Mask ROM visibility
  - Power analysis
  - Optical fault injection
  - Data remanence in Flash/EEPROM
  - Combined attacks
  - Optical emission analysis
  - Flash/EEPROM imaging under SEM
  - CPU speculative execution bug

History of disturbing physical attacks

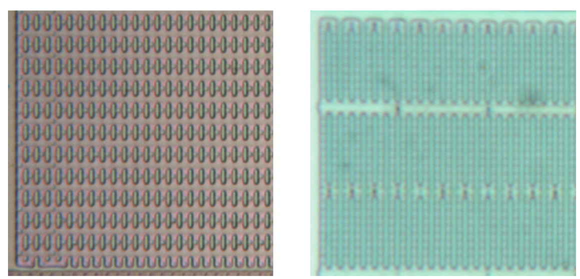
- Mask ROM “invisibility” in 1990s
  - Information is encoded with doping level
  - Impossible to see under optical microscope
  - Failure Analysis helps with defects etching
  - Countermeasures at silicon level



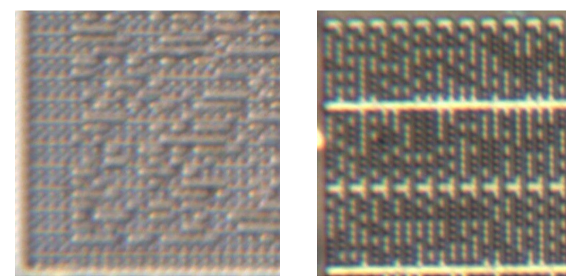
encoding by presence of transistors



encoding by shorts in metal layer



encoding by doping concentration

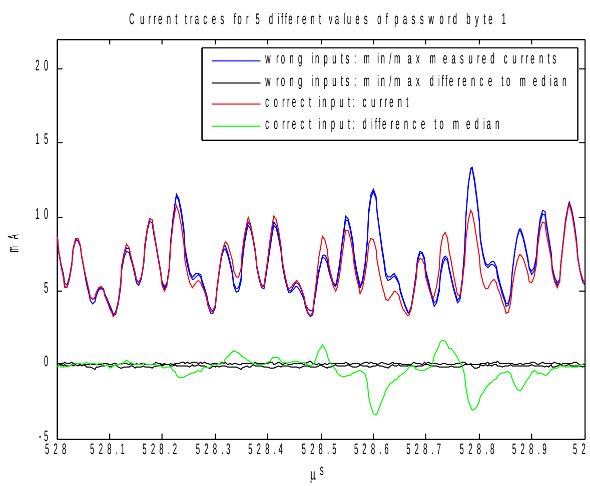


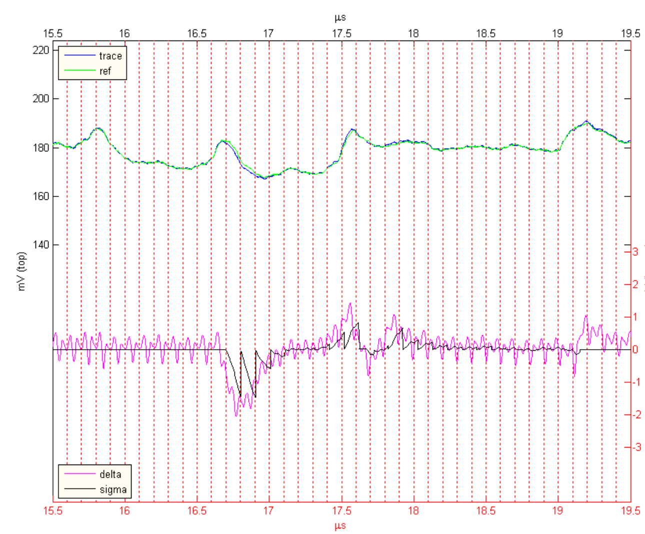
after selective dash etching

O. Kömmerling, M. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. USENIX 1999

History of disturbing physical attacks

- Power analysis reveals deep secrets
  - Leakage from switching CMOS transistors is correlated with processed data
  - Can break passwords and crypto keys
  - Countermeasures are very sophisticated

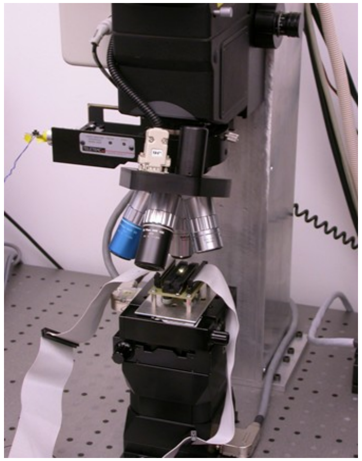


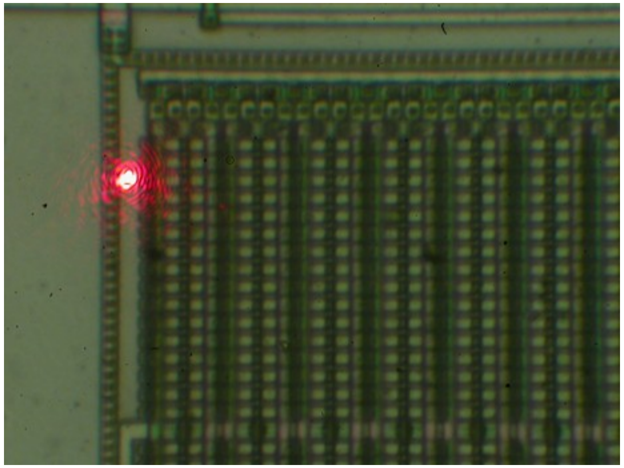


P. Kocher: Differential Power Analysis. Crypto 1999

History of disturbing physical attacks

- Optical fault injection
  - CMOS transistors and memory cells can be controlled with a laser beam
  - Confirmed down to 28nm devices
  - Countermeasures at silicon level

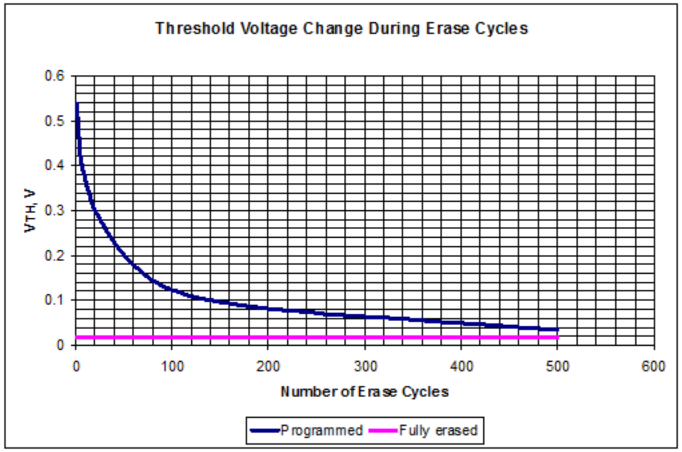


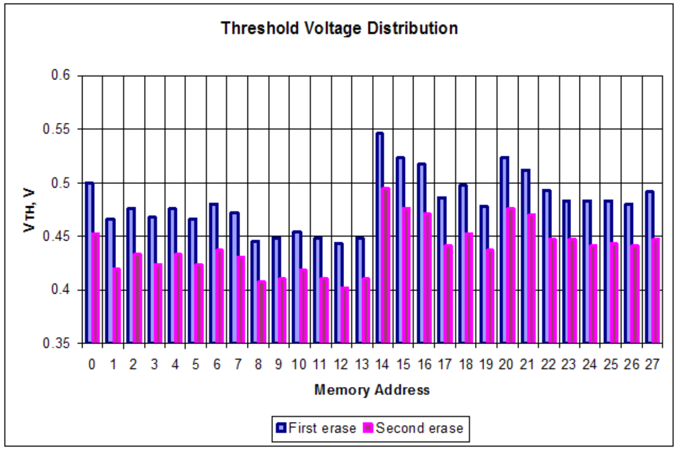


S. Skorobogatov, R. Anderson: Optical Fault Induction Attacks. CHES 2002

History of disturbing physical attacks

- Data remanence in Flash/EEPROM
  - Residual information present after Erase
  - Could lead to recovery of sensitive data
  - Once learned can be easily defeated

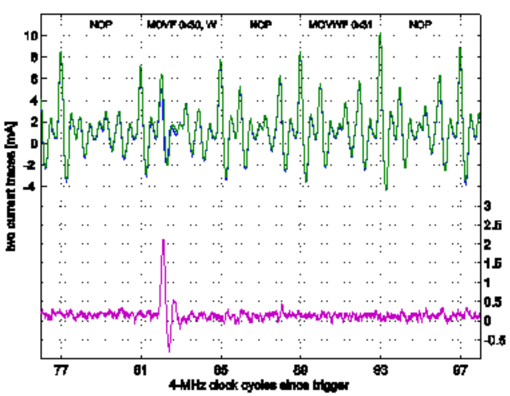




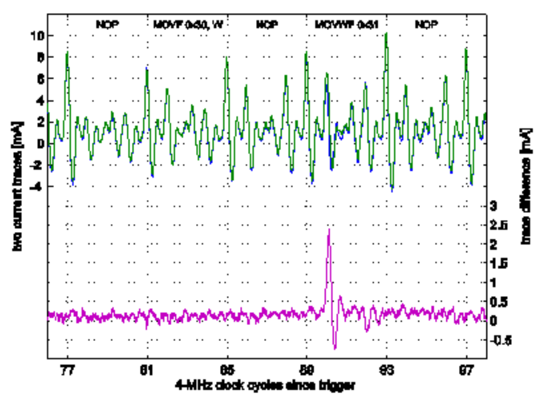
S. Skorobogatov: Data Remanence in Flash Memory Devices. CHES 2005

History of disturbing physical attacks

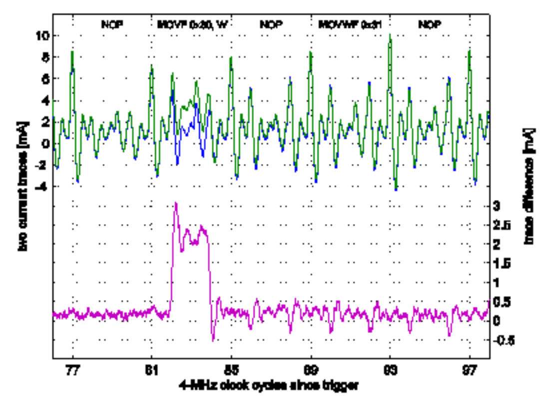
- Combined attacks
  - Power analysis + Fault injection
  - More powerful and localised
  - Countermeasures are hard to implement



read memory location (laser Off - On)



write memory location (laser Off - On)



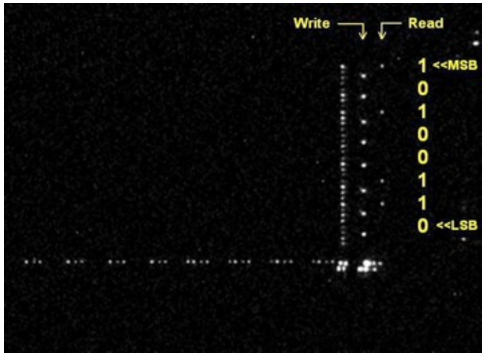
read memory location (laser Off – On)
contents of memory changed by laser

S. Skorobogatov: Optically Enhanced Position-Locked Power Analysis. CHES 2006

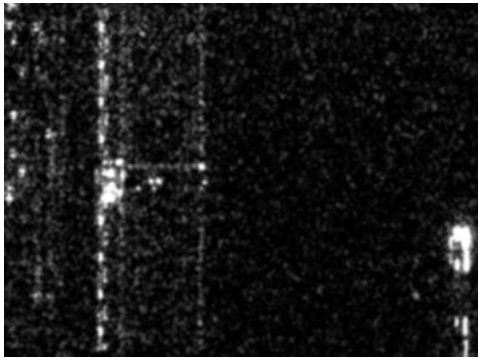
History of disturbing physical attacks

- Optical emission analysis
  - Switching CMOS transistors emit photons
  - Can be detected with CCD cameras (2D) and photomultiplier tubes (time resolved)
  - Countermeasures are hard to implement

PMT response over large area



CCD image acquired on SRAM

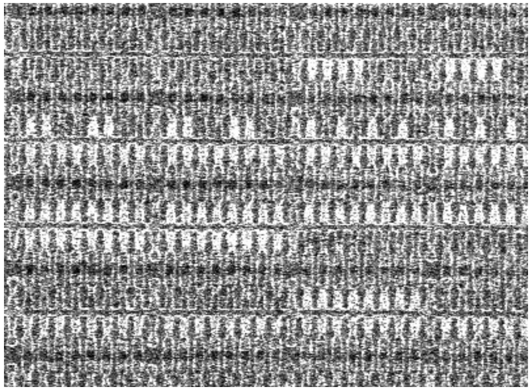


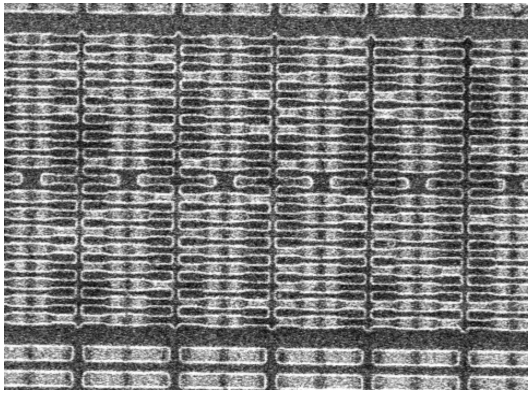
CCD image acquired on AES, 130nm

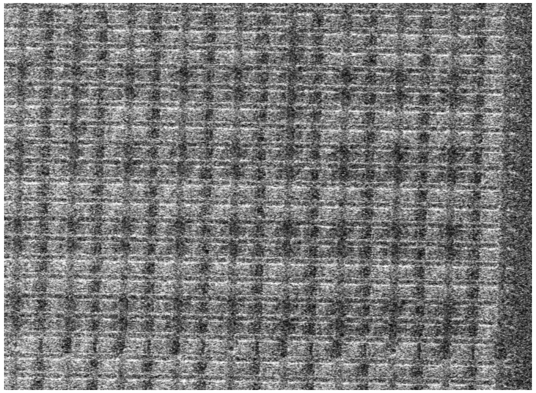
S. Skorobogatov: Using Optical Emission Analysis for Estimating Contribution to Power Analysis. FDTC 2009

History of disturbing physical attacks

- Flash/EEPROM imaging under SEM
  - More efficient and faster than SPM
  - Destructive to memory cells
  - Physical limits for detectable charge
  - Countermeasures are hard to implement







F. Courbon, S. Skorobogatov, C. Woods: Direct charge measurement in Floating Gate transistors of Flash EEPROM using Scanning Electron Microscopy. ISTFA 2016

History of disturbing physical attacks

- CPU speculative execution bug
  - Design flaw in most modern CPUs
  - Attack names: Meltdown, Spectre
  - Allows eavesdropping on internal CPU data from independent processes
  - Countermeasures at OS and silicon level

M. Lipp et al: Meltdown. USENIX 2018
P. Kocher et al: Spectre. S&P 2018

History of attack technologies

- Did all those attacks came unexpected or they could have been predicted?
  - Mask ROM visibility
    - manufacturers new what they were doing
  - Power analysis
    - standard tool to calculate power dissipation
  - Optical fault injection
    - radiation causes circuits to malfunction
  - Data remanence
    - was known for magnetic media

History of attack technologies

- Did all those attacks came unexpected or they could have been predicted?
  - Combined attacks
    - were not considered as simpler attacks existed
  - Optical emission analysis
    - was known for many years and is used in LEDs
  - Flash/EEPROM imaging under SEM
    - was not considered until latest SEMs with PVC
  - CPU speculative execution bug
    - possible to predict if you have security review

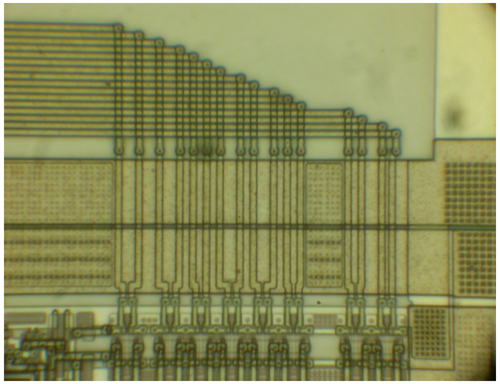
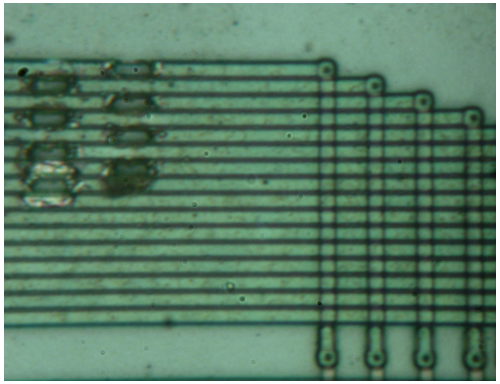
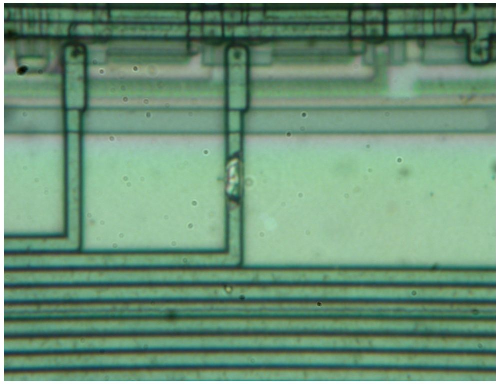
Impossible attacks – very high drive

- Reading data if there is no readback
  - Devices were considered secure by design
    - bypassed with bumping attacks
- Accessing data through backdoor
  - Was considered to be impossible by design
    - proved to work via undocumented debugging
- Reset passcode attempt counter in iPhone
  - FBI claimed that NAND mirroring will not work
    - proved to work with hardware cloning prototype

S. Skorobogatov: Flash Memory 'Bumping' Attacks. CHES 2010
S. Skorobogatov, C. Woods: Breakthrough silicon scanning discovers backdoor in military chip. CHES 2012
S. Skorobogatov: The bumpy road towards iPhone 5c NAND mirroring. arXiv 2016

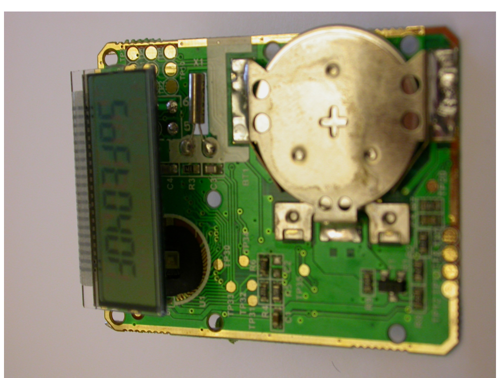
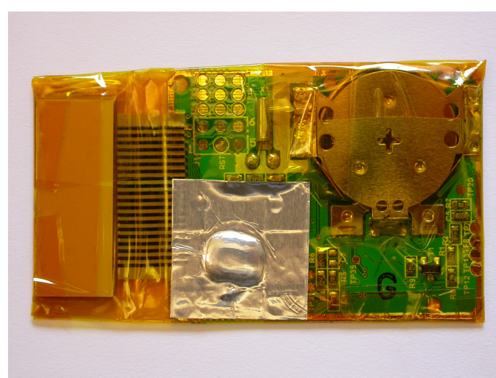
New attacks

- Microprobing CPU data bus
  - Hitachi HD6483102 smartcard controller
  - 16-bit Von-Neumann RISC CPU
  - Cutting bus line bit-15 will inject permanent '1'
    - CPU will execute non-branch 1-cycle instructions
  - Full memory extracted using one microprobe

New proof of concept attack

- Decapsulation on live circuits
  - Vasco Digipass 270 authentication token
  - Battery-backed SRAM storage for keys
    - on losing power or if Reset stops working
  - Sample preparation involves tape insulation, applying hot 100% Nitric Acid via stencil and washing with Acetone

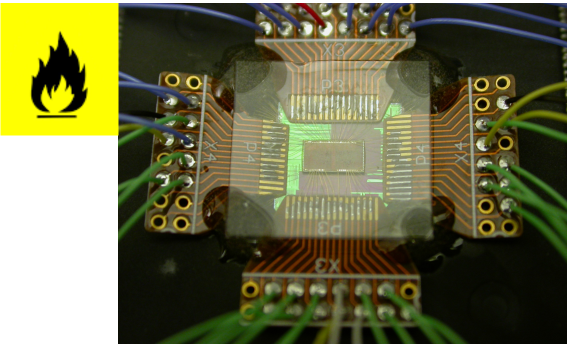



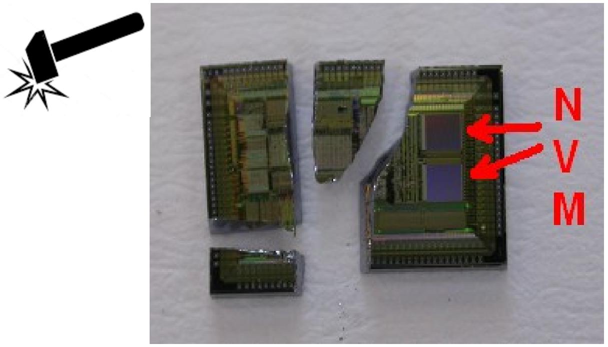

Discussions

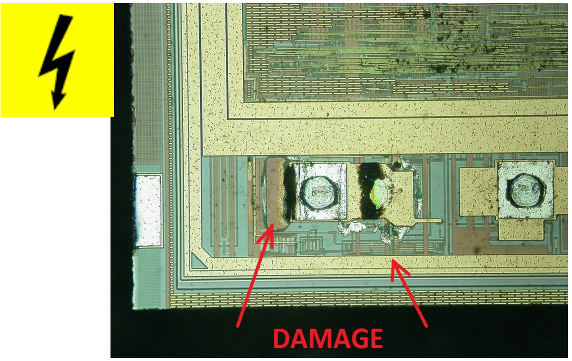
- Is it possible to predict new attacks?
  - Hardware security educated engineers
  - Open mind design reviewers
- Unexpected attack: bad or good
  - Helps in understanding the nature
  - What is bad for chip manufacturers might be good for technological progress
    - new materials could be created
    - new processes could be developed
    - new solutions to problems found

Challenges and Future Work

- Mechanical damage
  - Restore challenging packages (QFN, BGA)
  - Recovering information from shattered dies
- Electrical damage
  - Recovering information with burned I/O
  - Recovering information if logic is burned







Conclusion

- Many new attacks are based on well known facts and phenomena
- Instruction set in many CPUs is highly orthogonal, hence, susceptible to fault attacks
- Battery backed devices can be decapsulated without losing power
- New attacks are likely to emerge in the future
  - Are we ready to defeat?
- Collaboration between Industry and Academia
  - Implementing 'impossible' attacks
  - Coming up with new solutions and 'crazy' ideas