ISTFA 2017, Pasadena, CA, USA, 5 – 9 November 2017

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Combining Hardware Security, Failure Analysis and Forensic Analysis for the benefit of all

Dr Sergei Skorobogatov

University of Cambridge
Cambridge, UK

http://www.cl.cam.ac.uk/~sps32
email: sps32@cam.ac.uk

Outline

- Introduction
- Embedded Memory in Semiconductor Devices
- Where do Failure Analysis, Forensic Analysis and Hardware Security meet together?
- Challenges, Pros and Cons
  - Failure Analysis
  - Forensic Analysis
  - Hardware Security
- What can we learn from each other?
- Limitations, Achievements and Improvements
- Future Work and Collaboration
- Conclusion

Introduction

- Multidisciplinary Background and Skills
  - Electronics, Chemistry, Physics and Computer Science
- Hardware Security research since 1995
  - testing microcontrollers and smartcards for security
  - semi-invasive methods (PhD, 2005, Cambridge, UK)
  - backdoors in semiconductors (2012)
  - iPhone 5C NAND mirroring (2016)
  - solutions for security challenges in real-world devices
- Some research related to Failure Analysis
  - data remanence in Flash/EEPROM (CHES 2005)
  - combined optical and emission methods (CHES 2006)
  - PVC SEM for EEPROM and Flash (ISTFA 2016)

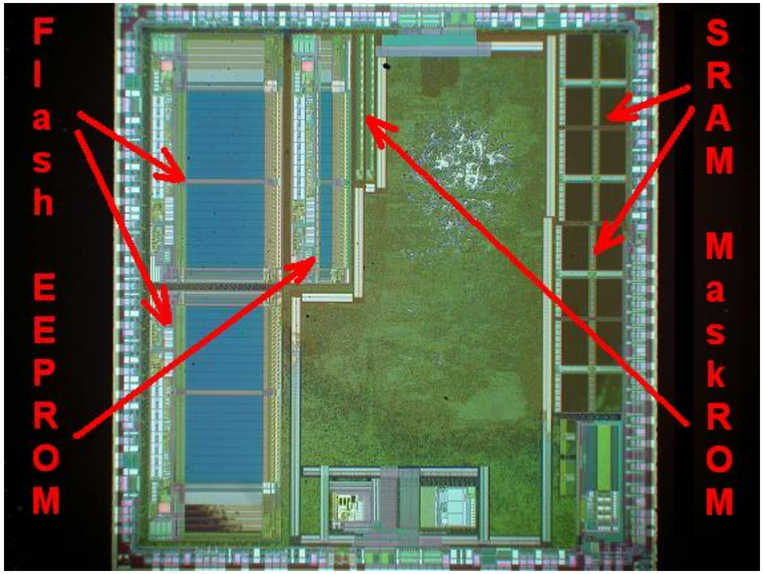
Hardware Security

- High importance and growing demand
  - data protection
  - cyber security
  - preventing attacks on services
  - preventing data and intellectual property (IP) theft
  - developing countermeasures against all known attacks
  - predicting new attacks
- Need for educated hardware engineers
  - hardware security as part of design, not add-on
  - knowledge of countermeasures
  - implement protection at all levels

Embedded Memory in ICs

- Secure devices to thwart hardware attacks
  - Low end: standard microcontrollers (µC)
  - Intermediate: secure memory, secure µC, FPGA, ASIC
  - High end: smartcard, secure ASIC
- Embedded Non-Volatile Memory (NVM)
  - Mask ROM: bootloader, firmware, algorithms
  - EEPROM: variables, keys, passwords
  - Flash: bootloader, firmware, algorithms, keys, passwords
- Memory extraction is the crucial step in attacks
  - access to firmware for reverse engineering
  - extraction of crucial algorithms
  - access to sensitive data, keys and passwords

Where do all parties meet?



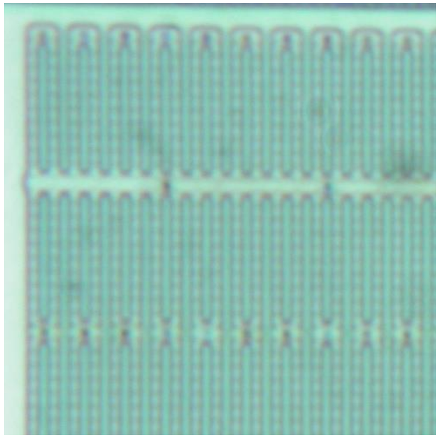
- **Failure Analysis methods**
  - reliability of data storage
  - advanced extraction methods
  - slow and expensive
  - not for large memory extraction
- **Forensic Analysis methods**
  - damaged samples (electrical or mechanical)
  - very few samples to deal with
  - large amount of data
- **Hardware Security methods**
  - defeat protection and improve the defence
  - efficient data extraction methods
  - rely on Failure Analysis methods for advanced attacks

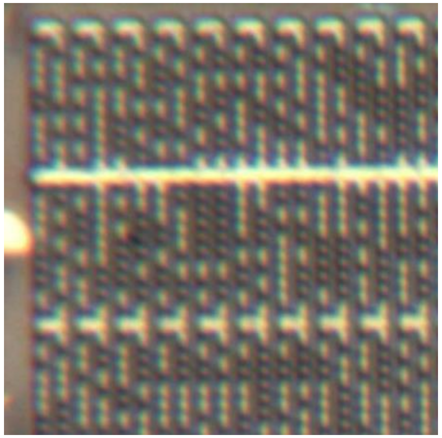
Memory extraction methods

- Failure Analysis methods
  - chemical de-processing (CMP, RIE)
  - Scanning Probe Microscopy (SCM, SKPM)
  - Scanning Electron Microscopy (SE, PVC)
  - microprobing (FIB)
  - direct readout with chip manufacturer support
- Forensic Analysis methods
  - software approach
  - use of standard interfaces
- Hardware Security methods
  - defeat protection (non-invasive and invasive attacks)
  - reverse engineering
  - combined attacks

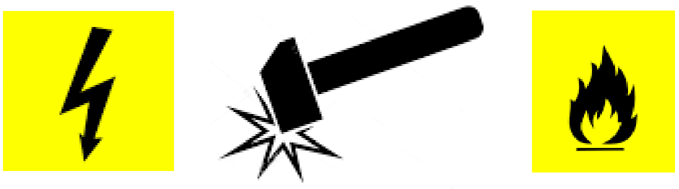
Challenges, Pros and Cons

- **Failure Analysis methods**
  - test for reliability of data storage
  - advanced extraction methods
  - slow and expensive
  - inefficient for large memory extraction
- **Pros**
  - test latest fabrication processes
  - reliable and repeatable methods
  - wide availability of tools
  - help from chip manufacturer
- **Cons**
  - high cost of equipment and analysis
  - time consuming process
  - require high skills





Challenges, Pros and Cons



- Forensic Analysis methods
  - data extraction for analysis
  - eavesdropping
  - information retrieval
- Pros
  - fast way of getting the data for analysis
  - inexpensive and high volume
  - can be carried out by less skilled personnel
- Cons
  - limited in budget
  - limited by security features
  - damaged devices pose big challenge
  - very challenging for latest fabrication processes

Challenges, Pros and Cons

- Hardware Security methods
  - reverse engineering of devices
  - direct memory extraction
  - keys and passwords extraction
  - advanced methods to bypass encryption
- Pros
  - approach even the most protected devices
  - combined methods to reduce cost and time
  - repeatable process
- Cons
  - expensive for modern devices
  - time consuming process to develop attacks
  - some skills are required

How can we benefit?

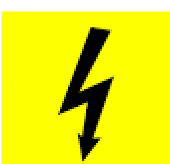
- **Failure Analysis (high end, slow)**
  - can help with smaller fabrication processes
  - can learn faster methods and innovative approaches
  - can access components directly (damaged parts)
- **Forensic Analysis (low end, fast)**
  - can learn methods for extreme cases (damaged parts)
  - can learn faster methods
- **Hardware Security (innovative, medium)**
  - can help with sophisticated methods (damaged parts)
  - can help with faster methods
  - can learn methods for smaller fabrication processes

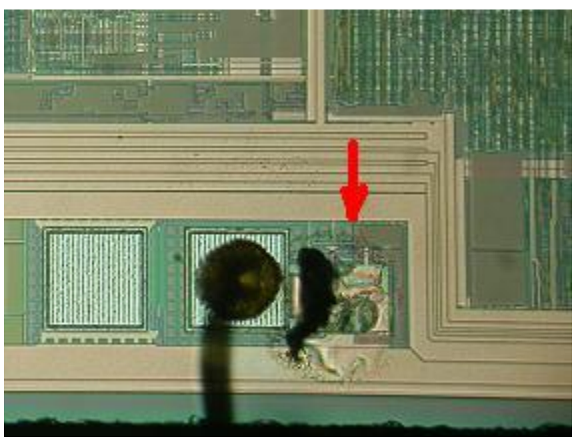
How can we benefit?

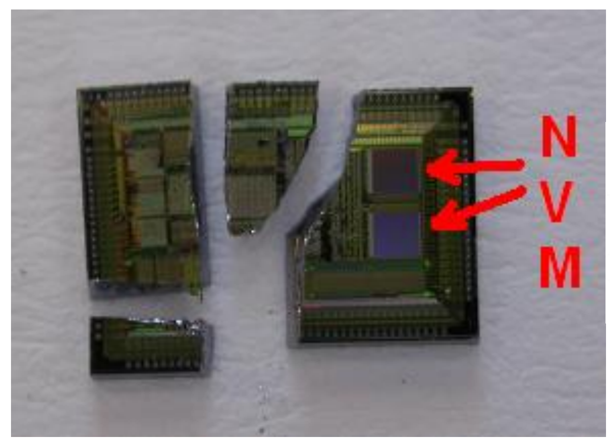
- Failure Analysis
  - PVC SEM methods were developed as part of Hardware Security research project
- Forensic Analysis
  - data extraction from custom NAND Flash was part of Hardware Security research project
- Hardware Security
  - microprobing using FIB machines
  - SEM imaging for Reverse Engineering
  - Mask ROM extraction using selective chemical etching
  - detection of Trojans in logic by delineation using selective chemical etching
  - advanced microscopy for data extraction

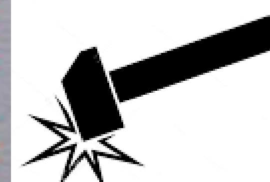
Limitations

- **Size of transistors**
  - smaller feature sizes: from >1µm to <10nm
  - extremely thin layers: <1nm gate oxide, <2nm tunnel oxide
  - non-planar structures (3D gate, FinFET, 2 or 3 poly layers)
- **Measurement noise**
  - non-uniform emissions
  - thermal noise of detectors
  - amplifiers noise
  - averaging adds time to the processing







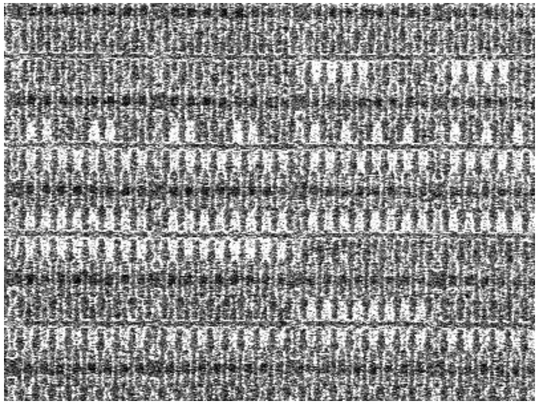
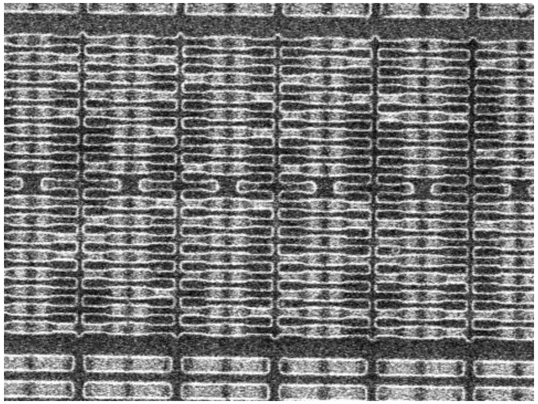
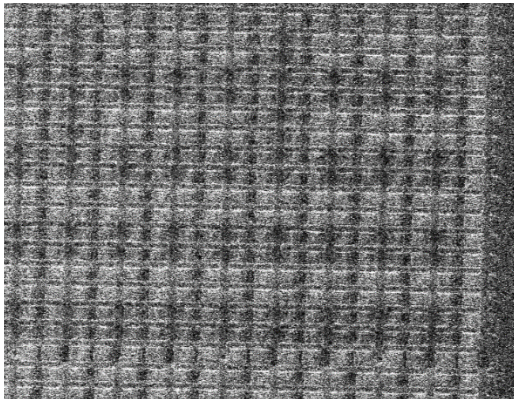


Limitations in Flash/EEPROM

- Size of transistors
  - EEPROM: 65nm/90nm process, cells size 4F×6F (0.5µm)
  - eFlash: 28nm/45nm/65nm process, cell size 3F×4F (0.2µm)
  - NAND Flash: 15nm/19nm/25nm process, cell size 2F×2F
- PVC SEM challenges
  - beam energy high enough to penetrate dielectric (>500eV)
  - low beam energy to avoid discharge (<50eV)
  - keep dielectric barrier thick enough to avoid discharge
  - difficult trade off but not entirely impossible
- Number of electrons
  - significant drop between old processes and latest ones
  - from >50,000e^- for 0.35µm to <50e^- for 16nm process

Achievements

- EEPROM (2T cell) imaging using PVC SEM
  - good contrast down to 210nm process
  - being replaced with more efficient Flash memory
- Flash (1T cell) imaging using PVC SEM
  - high noise even at 250nm process
  - need for more advanced methods and technologies
- Can 100% extraction be achieved?
  - EEPROM: 0.35µm 2kB (100%), 0.21µm 1kB (99.5%)
  - Flash: 0.35µm 4kB (99%), 0.25µm 16kB (90%)

Improvements

- SPM methods
  - more sensitive equipment with less noise: high cost
  - faster equipment: high cost
- PVC SEM methods
  - more sensitive equipment with less noise: high cost
  - signal processing: affordable
  - parallel scanning: impact on PVC
- New methods
  - combined methods did work for semi-invasive techniques
  - more research and development is needed to find new innovative solutions
  - Work-in-Progress webpage for latest breakthrough news: http://www.cl.cam.ac.uk/~sps32/dec_proj.html

Future Work and Collaboration

- SPM improvements
  - SKPM is more promising than SCM: sample preparation
  - Smart scanning could improve the speed
  - post processing of images
- SEM improvements
  - improving setup and detectors
  - digital signal processing of detector signal
  - post processing of images
- Collaboration with industry
  - bring new ideas and test new methods
  - apply interdisciplinary approach
  - funding is essential
  - possibility to go beyond state-of-the-art

Conclusion

- **Failure Analysis, Forensic Analysis and Hardware Security can learn something from each other**
  - **need for more interdisciplinary research**
- **Need for closer collaboration between industry and academia**
  - **test innovative ideas (sometime non-standard and crazy)**
- **What was impossible a few years ago could become a mainstream tomorrow**
- **We are constantly working hard to improve the existing methods and find the best solutions to existing problems and challenges**

Thank You!

UNIVERSITY OF CAMBRIDGE

Computer Laboratory