Tamper resistance and physical attacks

Part IV: Hardware security research

Dr Sergei Skorobogatov

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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Security Group, TAMPER Lab

Hardware security research

- Hardware research lab (TAMPER Lab)
  - Part of the Security Group at the Computer Laboratory Department
  - Research focused on the hardware aspects of semiconductor devices, computers and communication security
  - 3 associated staff members, 1 postdoc and 2 research students
  - Cooperates with interested researchers of other university departments, other universities, government institutions and industrial companies

Hardware security research

- Perform analysis of on-the-market semiconductor devices against known attacks
- Develop new attack methods and countermeasures
- Develop efficient, inexpensive and fast analysis methods
  - Semi-invasive methods are in higher demand
- Provide consulting for various organisations
  - Manufacturers of test equipment
  - Chip manufacturers
  - Developers of secure devices

Hardware security research

- Sample preparation
  - Manual decapsulation and chemical etching
  - Laser cutting system
  - Externally: plasma etching, backside preparation, CMP, FIB
- Analysis
  - Optical imaging with a high-resolution microscope
  - Microprobing station
  - Various laser scanning techniques
  - Special microscopes for optical fault injection analysis (sponsors)
  - Externally: optical imaging, SEM, FIB, reverse engineering, emulation techniques
- Feedback
  - Reports, consulting, collaboration
  - In plans: special courses on hardware security and semi-invasive attacks (lectures, seminars, demonstrations and practical labs)

Hardware security research

- Semi-invasive analysis using equipment from Semiresearch Ltd.
  - Ex-demo version of Trioscan BSL2R with NWR QuikLaze-II TriLaze laser cutter
    - Dual-mode advanced laser scanning
      - Large-area scanning (12×12 mm^2)
      - High-resolution scanning (0.05 µm)
    - Long-working distance objectives (10 mm minimum for high-magnification objectives)
    - Dual-use laser cutting system
      - Sample preparation
      - Fault injection (Trig in/out synchronisation)
    - Optical fault injection capability for NWR and BSL lasers (external triggering)
      - Evaluation showed that NWR pulsed laser is not suitable for some types of optical fault injection attacks

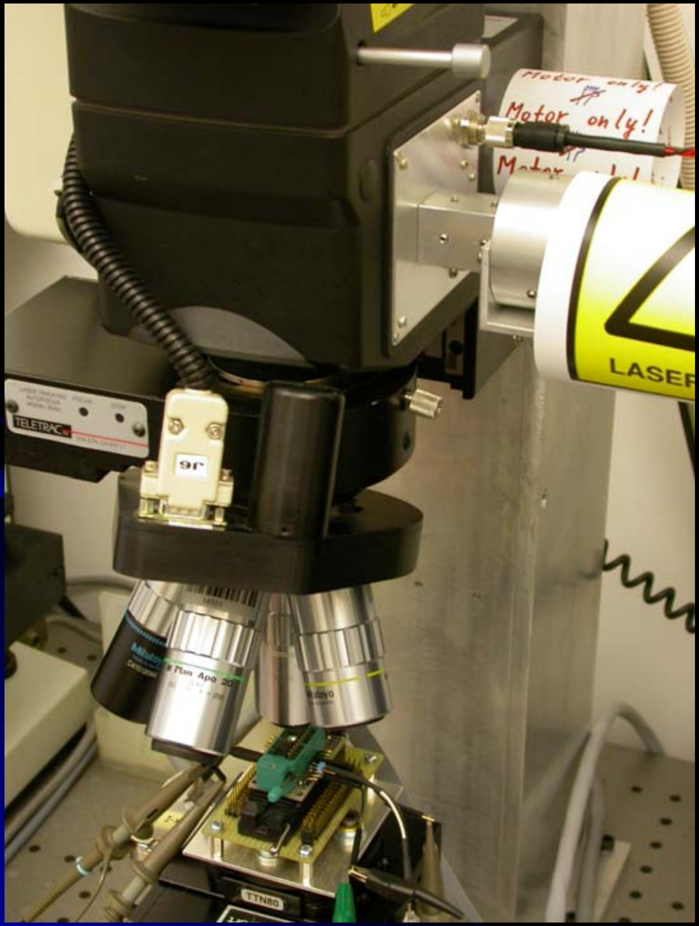
Hardware security research

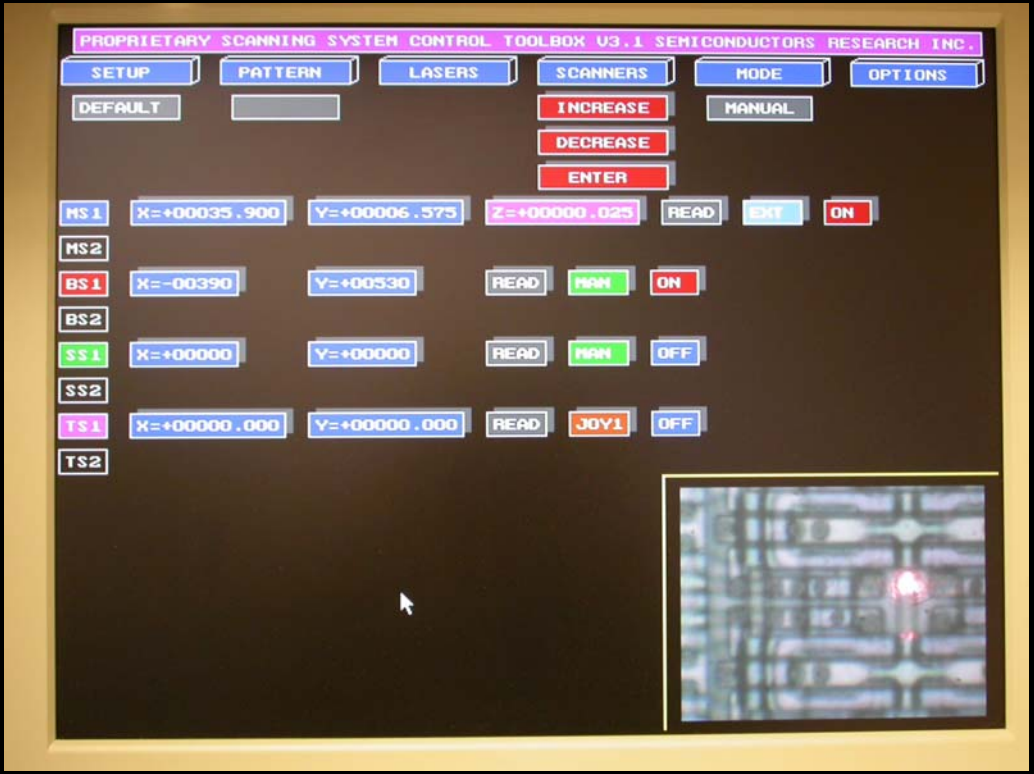
- Semi-invasive analysis using equipment from Semiresearch Ltd.
  - Demo version of Multioscan BTSL4RGI
    - Triple-mode advanced laser scanning
      - Large-area scanning (18×18 mm^2)
      - High-resolution scanning (0.025 µm)
      - Real-time scanning
    - Dual wavelength lasers for convenient operation from front and rear sides
    - Improved IR and UV optics plus special CCD cameras for backside navigation
    - Long-working distance objectives (10 mm minimum for high-magnification objectives)
    - Optical fault injection capability for any of the lasers (software, pattern and external triggering)
      - Evaluation showed high effectiveness of the system for many types of optical attacks

CLASS 3B laser product
AVOID EXPOSURE TO BEAM
LASER RADIATION
DANGER!!!
SINGLE SHOT INTO EYE WILL BE THE LAST THING EYE HAS SEEN
OSE THE DOOR BEHIND YOU!!!
CORRECT
Newport

Hardware security research

- Experiments using Semiresearch Trioscan BSL2R special laser system for optical analysis of semiconductors

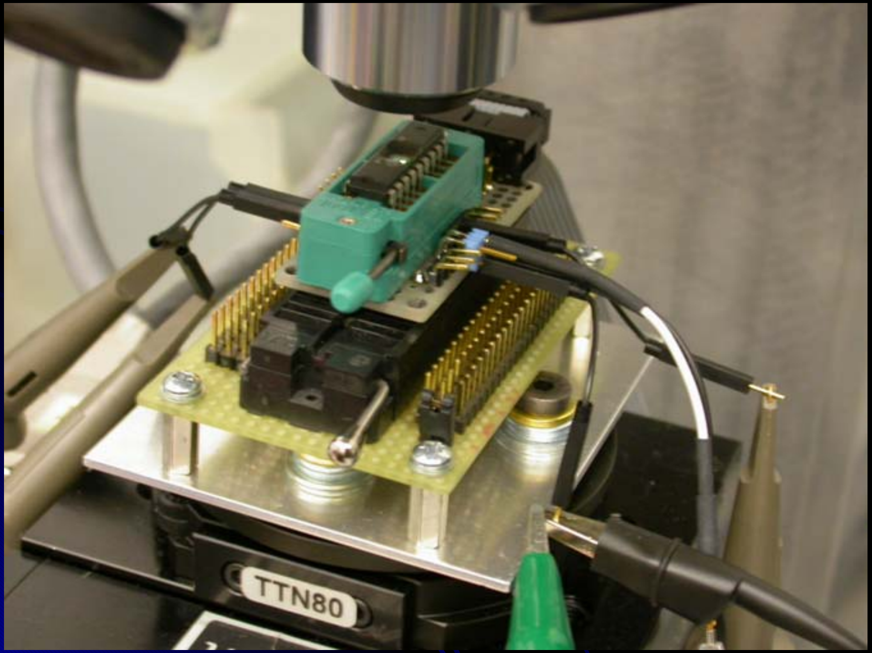


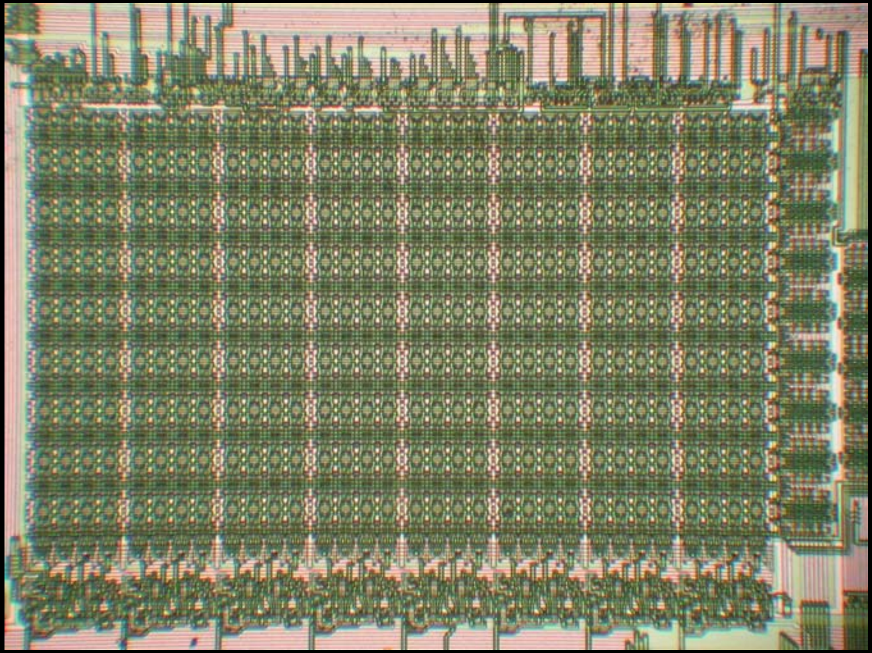

PROPRIETARY SCANNING SYSTEM CONTROL TOOLBOX V3.1 SEMICONDUCTORS RESEARCH INC.

MS1 X=+00035.900 Y=+00006.575 Z=+00000.025 READ EXT ON
MS2
BS1 X=-00390 Y=+00530 READ MAN ON
BS2
SS1 X=+00000 Y=+00000 READ MAN OFF
SS2
TS1 X=+00000.000 Y=+00000.000 READ JOY1 OFF
TS2

Hardware security research

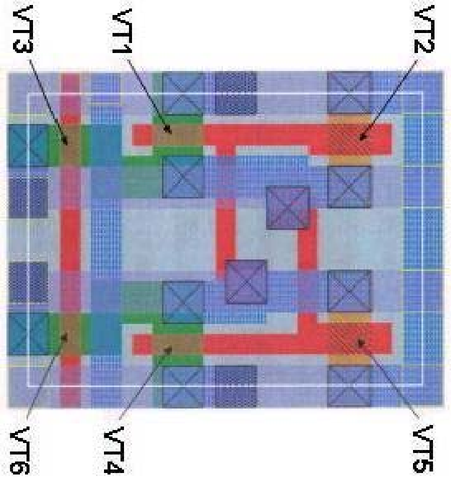
- Optically enhanced position-locked power analysis
  - Microchip PIC16F84 microcontroller
  - Classic power analysis setup (10 Ω resistor in GND, 500 MHz digital oscilloscope) and Trioscan BSL2R special laser system

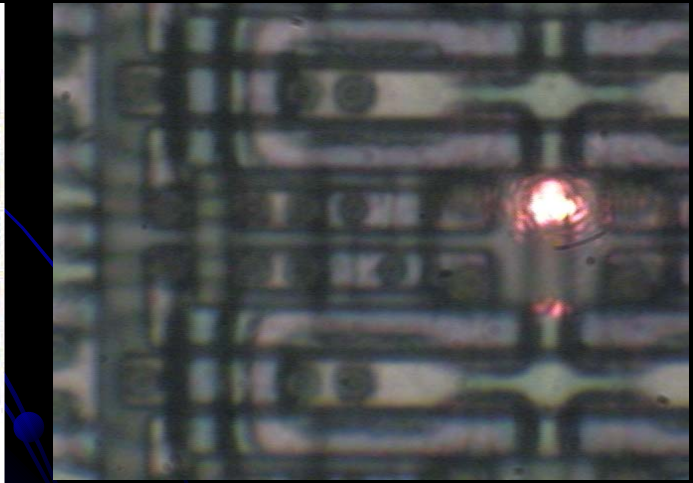


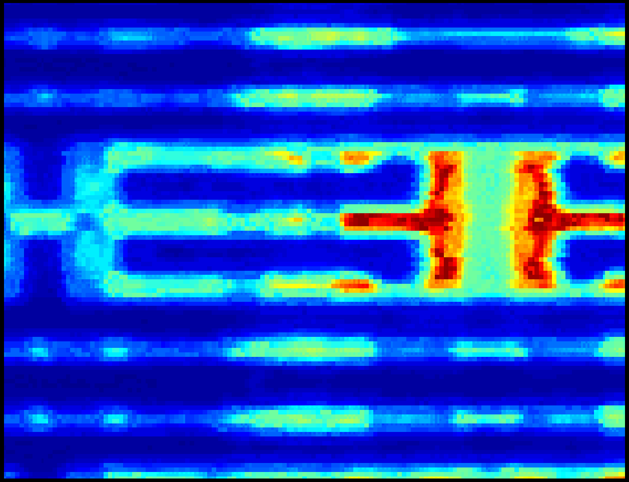


Hardware security research

- Optically enhanced position-locked power analysis
  - Standard laser scanning operation reveals all sensitive areas
  - Microcontroller was programmed with the program which accesses certain memory locations and output result to the ports
  - Test pattern
    - Run the code inside the microcontroller and store the power trace
    - Trigger fault injection event and store the power trace
    - Compare two traces

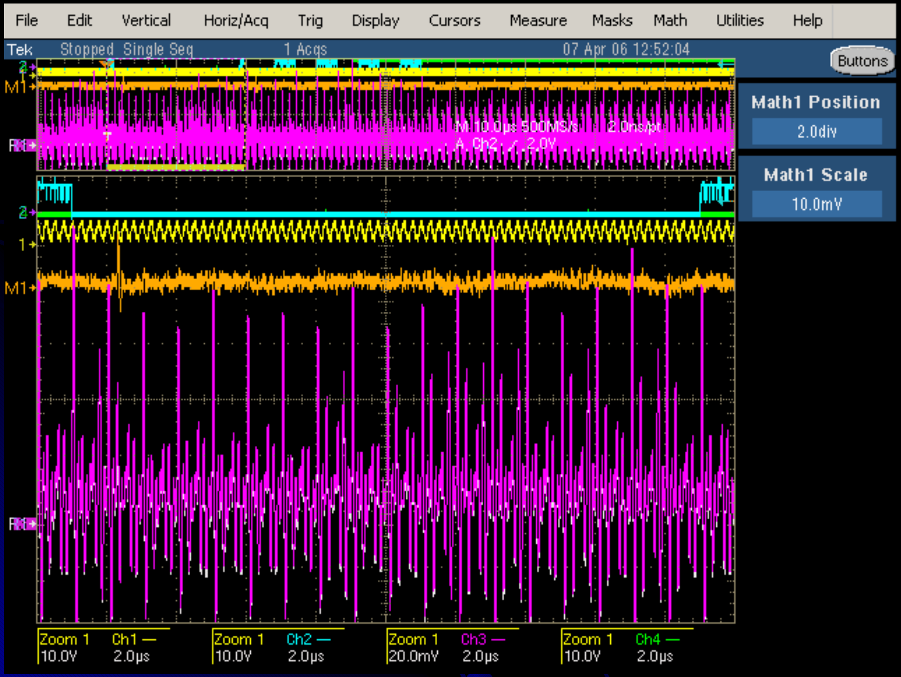






Hardware security research

- Optically enhanced position-locked power analysis
  - Single acquisition with 250 Ms/s
  - Results for memory read operations
    - Non-destructive analysis of active memory locations (‘0’ and ‘1’)



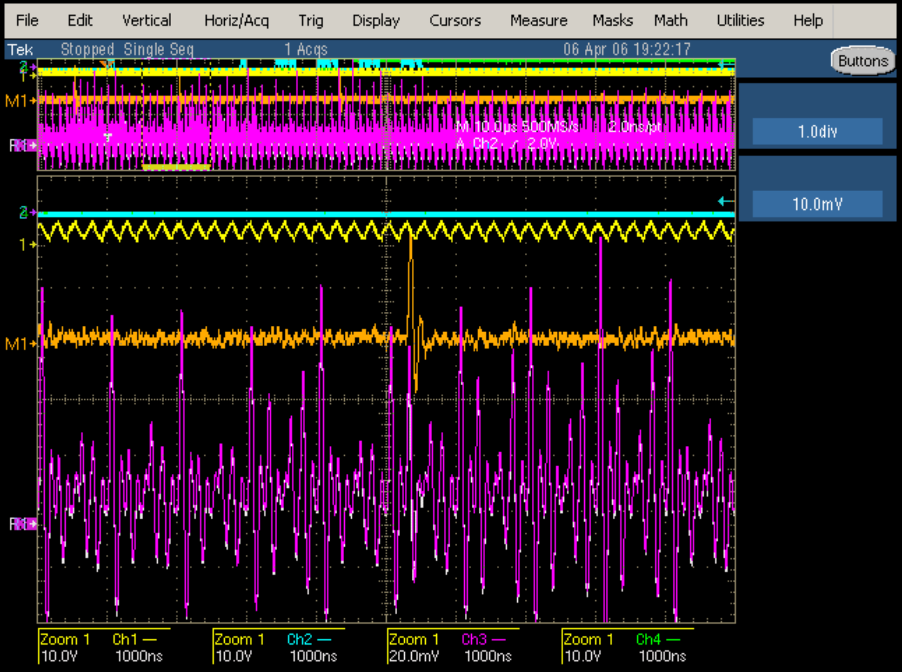
Tek Stopped Single Seq 1 Acqs 07 Apr 06 12:52:04

M 10.0µs 500MS/s 2.0ns/pt
A Ch2 ↗ 2.0V

Math1 Position 2.0div

Math1 Scale 10.0mV

Zoom 1 Ch1 — 10.0V 2.0µs
Zoom 1 Ch2 — 10.0V 2.0µs
Zoom 1 Ch3 — 20.0mV 2.0µs
Zoom 1 Ch4 — 10.0V 2.0µs



Tek Stopped Single Seq 1 Acqs 06 Apr 06 19:22:17

M 10.0µs 500MS/s 2.0ns/pt
A Ch2 ↗ 2.0V

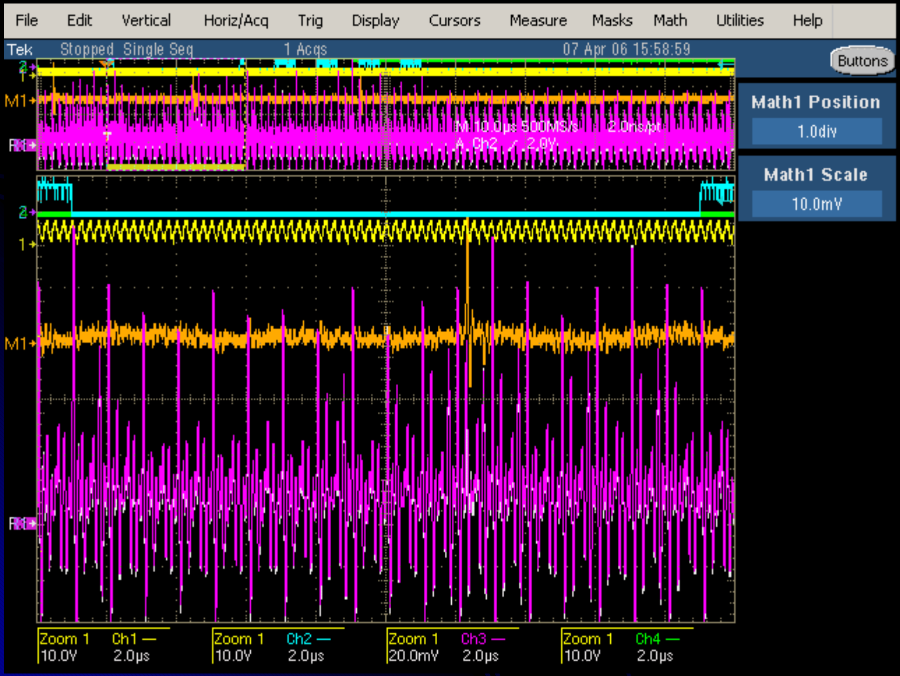
1.0div

10.0mV

Zoom 1 Ch1 — 10.0V 1000ns
Zoom 1 Ch2 — 10.0V 1000ns
Zoom 1 Ch3 — 20.0mV 1000ns
Zoom 1 Ch4 — 10.0V 1000ns

Hardware security research

- Optically enhanced position-locked power analysis
  - Single acquisition with 250 Ms/s
  - Results for memory write operations
    - Non-destructive analysis of active memory locations (‘0→0’, ‘0→1’, ‘1→0’ and ‘1→1’)

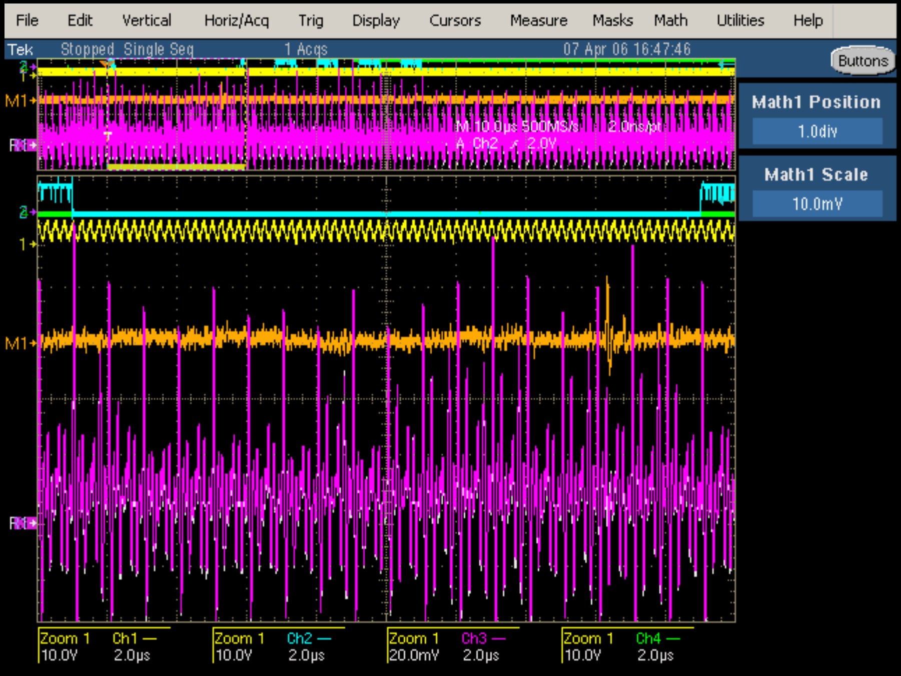


Tek Stopped Single Seq 1 Acqs 07 Apr 06 15:58:59

M 10.0µs 500MS/s 2.0ns/pt
A Ch2 ↗ 2.0V

Math1 Position 1.0div
Math1 Scale 10.0mV

Zoom 1 10.0V Ch1 2.0µs
Zoom 1 10.0V Ch2 2.0µs
Zoom 1 20.0mV Ch3 2.0µs
Zoom 1 10.0V Ch4 2.0µs



Tek Stopped Single Seq 1 Acqs 07 Apr 06 16:47:46

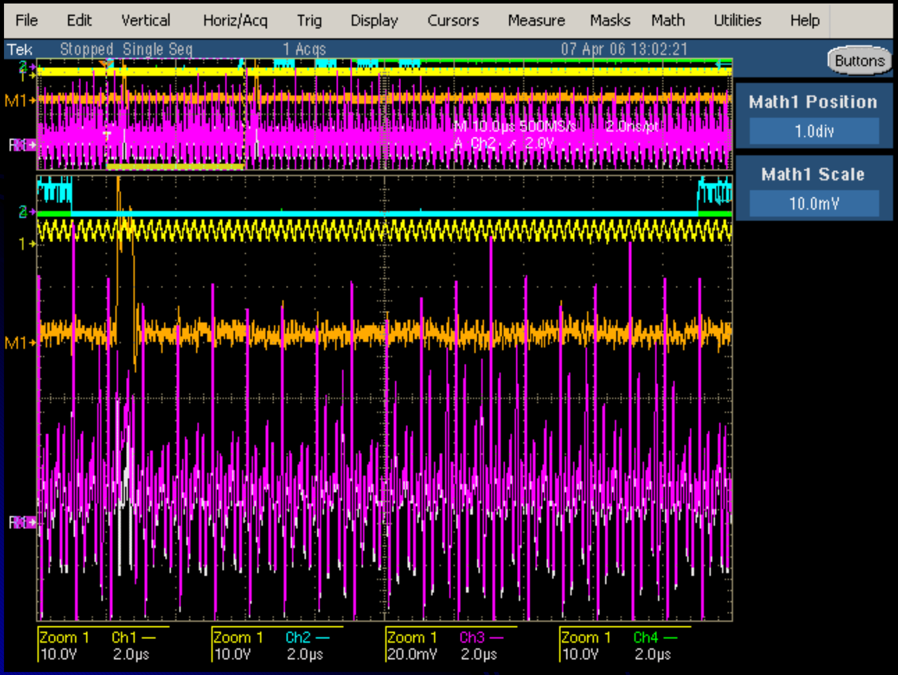
M 10.0µs 500MS/s 2.0ns/pt
A Ch2 ↗ 2.0V

Math1 Position 1.0div
Math1 Scale 10.0mV

Zoom 1 10.0V Ch1 2.0µs
Zoom 1 10.0V Ch2 2.0µs
Zoom 1 20.0mV Ch3 2.0µs
Zoom 1 10.0V Ch4 2.0µs

Hardware security research

- Optically enhanced position-locked power analysis
  - Single acquisition with 250 Ms/s
  - Results for memory read and write destructive operations
    - Detecting active cells
    - Detecting active columns in the memory array



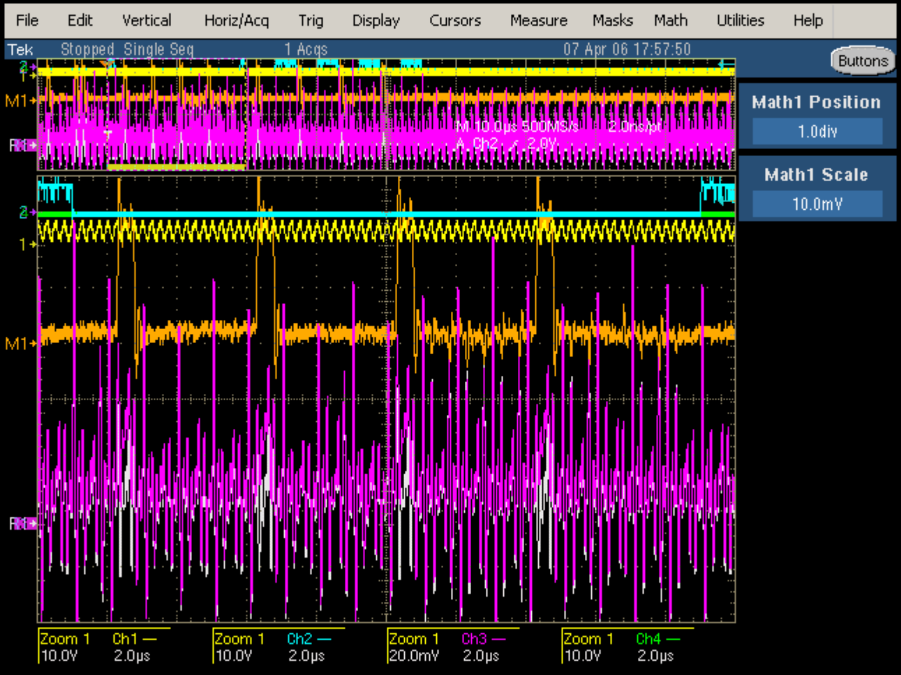
Tek Stopped Single Seq 1 Acqs 07 Apr 06 13:02:21

M 10.0µs 500MS/s 2.0ns/pt
A Ch2 ↗ 2.0V

Math1 Position 1.0div

Math1 Scale 10.0mV

Zoom 1 10.0V Ch1 — 2.0µs
Zoom 1 10.0V Ch2 — 2.0µs
Zoom 1 20.0mV Ch3 — 2.0µs
Zoom 1 10.0V Ch4 — 2.0µs



Tek Stopped Single Seq 1 Acqs 07 Apr 06 17:57:50

M 10.0µs 500MS/s 2.0ns/pt
A Ch2 ↗ 2.0V

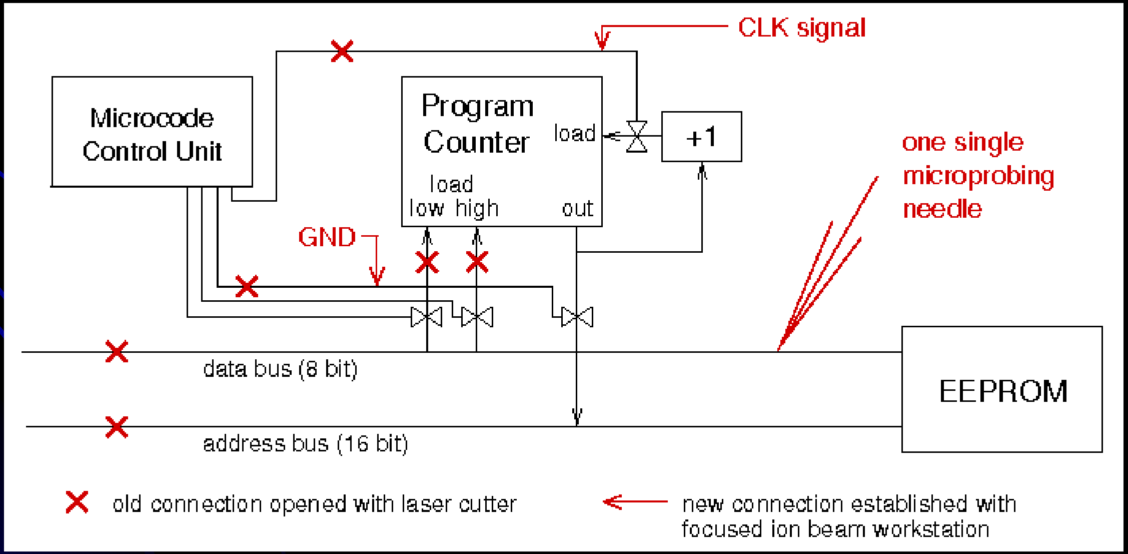
Math1 Position 1.0div

Math1 Scale 10.0mV

Zoom 1 10.0V Ch1 — 2.0µs
Zoom 1 10.0V Ch2 — 2.0µs
Zoom 1 20.0mV Ch3 — 2.0µs
Zoom 1 10.0V Ch4 — 2.0µs

Hardware security research

- Optically enhanced position-locked power analysis
  - Full story to be published later this year
  - Full presentation will appear at CHES-2006
- Other combinations of optical fault injection methods with conventional side-channel attacks
  - Fault injection in conjunction with power analysis
    - Temporary CPU modification followed by the Reset to prevent reaction


CLK signal
Microcode Control Unit
Program Counter
load
+1
one single microprobing needle
load
low high
out
GND
data bus (8 bit)
EEPROM
address bus (16 bit)
old connection opened with laser cutter
new connection established with focused ion beam workstation

Picture courtesy of Dr Markus Kuhn

Hardware security research

- Other interesting combinations of the attack methods were found
    - Will appear later in publications
    - Together with already known optical methods will become a part of the tuition courses on:
        - hardware security
        - semi-invasive attacks
        - optical attacks

Conclusions

- Having proper equipment for semi-invasive analysis is a vital part in the research
- It is not always necessary to have very expensive equipment to attack a semiconductor device, but the security analysis could be very expensive
  - Fault injection attacks are much easier to use and repeat, than to test the real device against these attacks
- New attacks could emerge when previously known attack methods are combined together
- Simulation does not always work reliably, by testing real hardware some unexpected problems could be spotted