Side-channel attacks:
new directions and horizons

Dr Sergei Skorobogatov

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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Introduction: Who needs secure chips?

- **car industry:** anti-theft protection, spare parts identification
- **service providers:** access cards, payment tokens, RFID tags, electronic keys, software license dongles
- **mobile phone manufacturers:** batteries and accessories control
- **printer manufacturers:** toner cartridges, memory modules
- **manufacturers of entertainment systems:** copy protection, consumables and accessories control
- **manufacturers of devices and equipment:** protection against cloning and reverse engineering, IP protection (hardware, software, algorithms)
- **banking industry:** secure payment cards, secure processing
- **military applications:** data protection, encrypted communication

Attack categories

- **Side-channel attacks**
  - techniques that allows the attacker to monitor the analog characteristics of power supply and interface connections and any electromagnetic radiation
- Software attacks
  - use the normal communication interface and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation
- Fault generation
  - use abnormal environmental conditions to generate malfunctions in the system that provide additional access
- **Microprobing**
  - can be used to access the chip surface directly, so we can observe, manipulate, and interfere with the device
- Reverse engineering
  - used to understand the inner structure of the device and learn or emulate its functionality; requires the use of the same technology available to semiconductor manufacturers and gives similar capabilities to the attacker

Side-channel attacks

- Easy to understand
  - simple principles
  - straightforward implementation
- Affordable
  - off-the-shelf equipment is available
  - no special computational hardware is required apart from PC
  - broad knowledge is build with over a decade of research
- Reliable
  - easy to reproduce
- Quick turnaround
  - fast result with minimal effort
- Dangerous for secure chip manufacturers
  - attackers can share information without the need of hardware

Attack methods

- Non-invasive attacks (low-cost)
  - observe or manipulate the device without physical harm to it
  - require only moderately sophisticated equipment and knowledge to implement
- Invasive attacks (expensive)
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - normally require expensive equipment, knowledgeable attackers and time
- Semi-invasive attacks (affordable)
  - semiconductor chip is depackaged but the internal structure of it remains intact
  - fill the gap between non-invasive and invasive types, being both inexpensive and easily repeatable

Non-invasive attacks

- Non-penetrative to the attacked device
  - normally do not leave tamper evidence of the attack
- Tools
  - digital multimeter
  - IC soldering/desoldering station
  - universal programmer and IC tester
  - oscilloscope and logic analyser
  - signal generator
  - programmable power supplies
  - PC with data acquisition board
  - FPGA board
  - prototyping boards

Non-invasive attacks: side-channel

- Timing attacks aimed at different computation time
  - incorrect password verification: termination on incorrect byte, different computation length for incorrect bytes
  - incorrect implementation of encryption algorithms: performance optimisation, cache memory usage, non-fixed time operations
- Today: timing attacks became harder to apply
  - common mistakes were fixed by manufacturers
  - internal clock sources and use of PLL made analysis difficult
  - countermeasures are in place: randomised clock, dummy cycles
  - careful selection of hardware eliminates many problems

Non-invasive attacks: side-channel

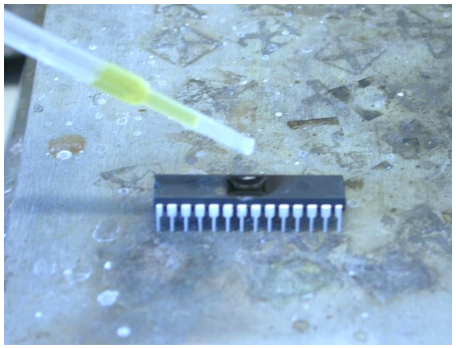
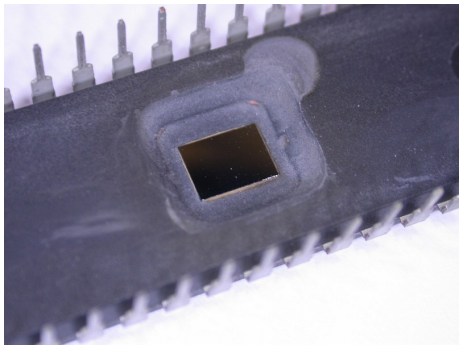
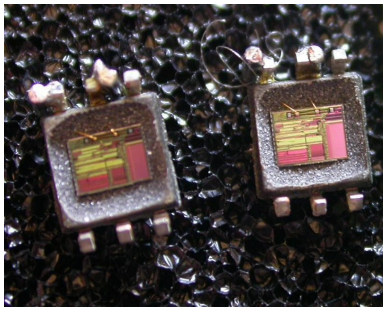
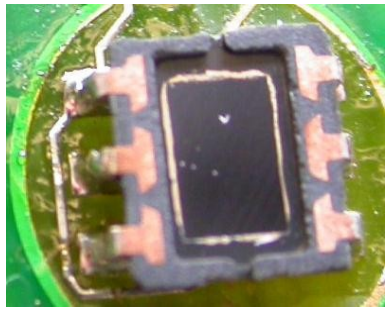
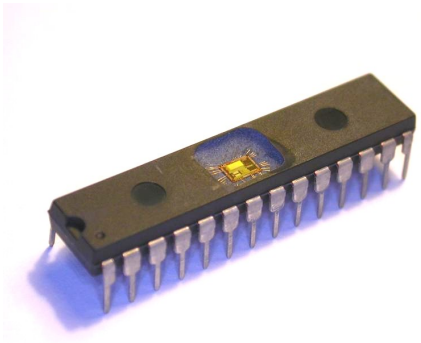
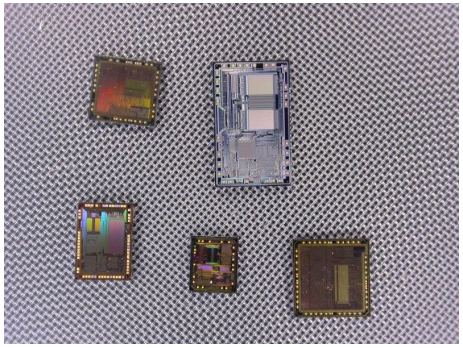
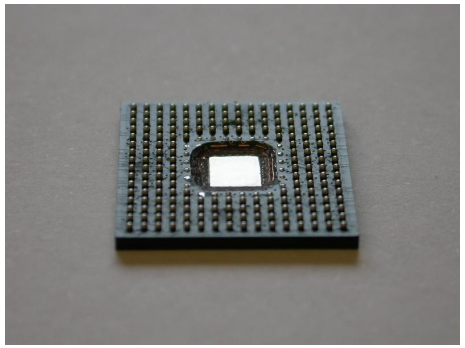
- Power analysis: measuring power consumption in time
  - very simple set of equipment – a PC with an oscilloscope and a small resistor in power supply line; very effective against many cryptographic algorithms and password verification schemes
  - some knowledge in electrical engineering and digital signal processing is required
  - two basic methods: simple (SPA) and differential (DPA)
- Electro-magnetic analysis (EMA): measuring emission
  - similar to power analysis, but instead of resistor, a small magnetic coil is used allowing precise positioning over the chip
- Today: SPA/DPA and EMA became more challenging
  - higher operating frequency and noise: faster equipment is required
  - power supply is reduced from 5V to 1V: lower signal, more noise
  - 8-bit data vs 32-bit data: harder to distinguish single-bit change
  - more complex circuits: higher noise from other parts, hence, more signal averaging and digital signal processing are required
  - effective countermeasures for many cryptographic algorithms

Invasive attacks

- Penetrative attacks
  - leave tamper evidence of the attack or even destroy the device
- Tools
  - IC soldering/desoldering station
  - simple chemical lab
  - high-resolution optical microscope
  - wire bonding machine
  - laser cutting system
  - microprobing station
  - oscilloscope and logic analyser
  - signal generator
  - scanning electron microscope
  - focused ion beam workstation

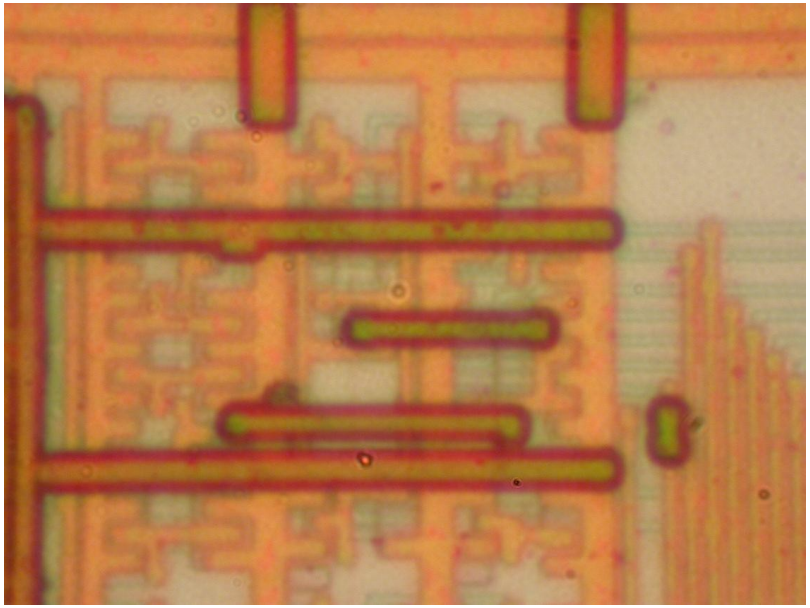
Invasive attacks: sample preparation

- Decapsulation
  - manual with fuming nitric acid (HNO_3) and acetone at 60ºC
  - automatic using mixture of HNO_3 and H_2SO_4
  - full or partial
  - from front side and from rear side
- Today: more challenging due to small and BGA packages

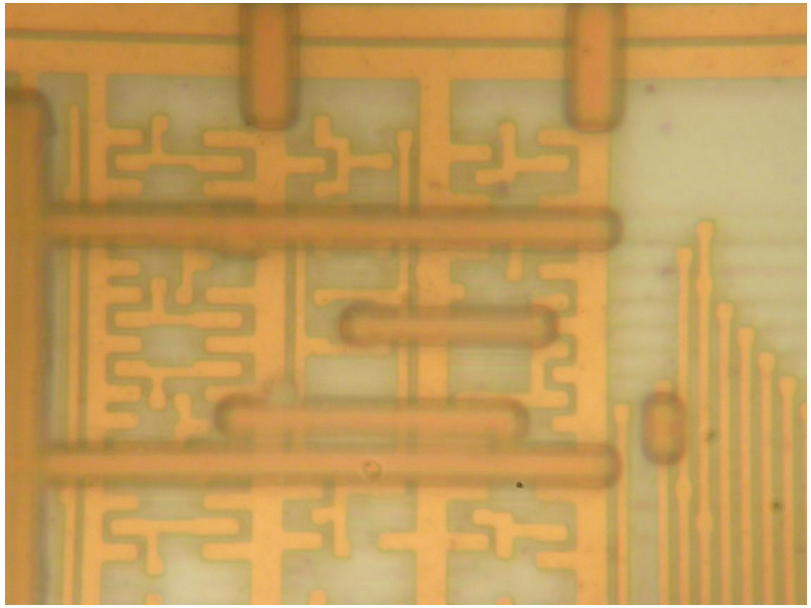








Invasive attacks: imaging

- Optical imaging
  - resolution is limited by optics and wavelength of a light:
    R = 0.61 λ / NA = 0.61 λ / n sin(μ) – best is 0.18μm technology
    - reduce wavelength of the light using UV sources
    - increasing the angular aperture, e.g. dry objectives have NA = 0.95
    - increase refraction index of the media using immersion oil (n = 1.5)
- Today: optical imaging is replaced by electron microscopy



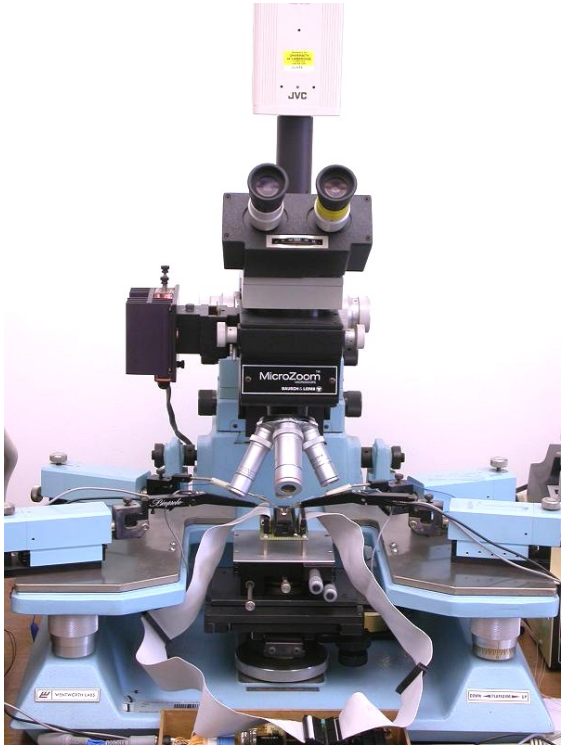
Bausch&Lomb MicroZoom, 50×2×, NA = 0.45

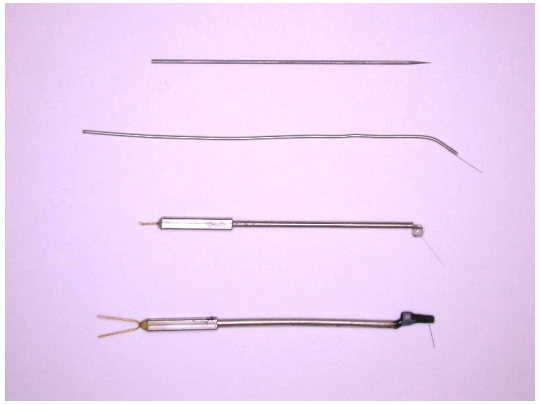


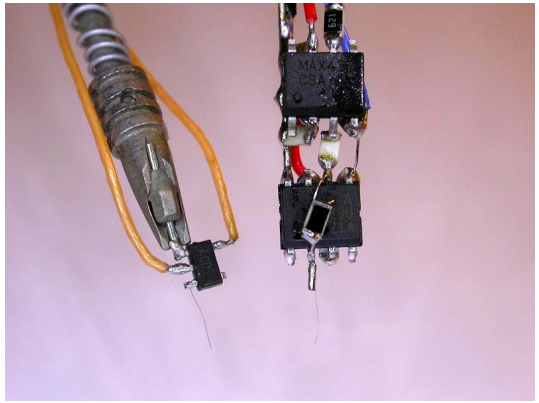
Leitz Ergolux AMC, 100×, NA = 0.9

Invasive attacks: microprobing

- Microprobing with fine electrodes
  - eavesdropping on signals inside a chip
  - injection of test signals and observing the reaction
  - can be used for extraction of secret keys and memory contents
  - limited use for 0.35μm and smaller chips

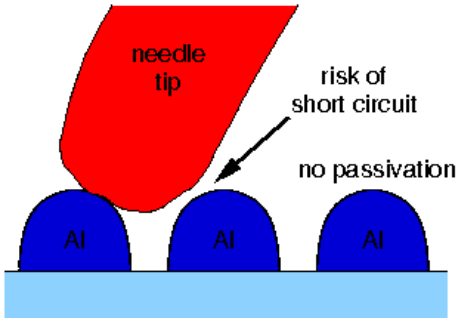


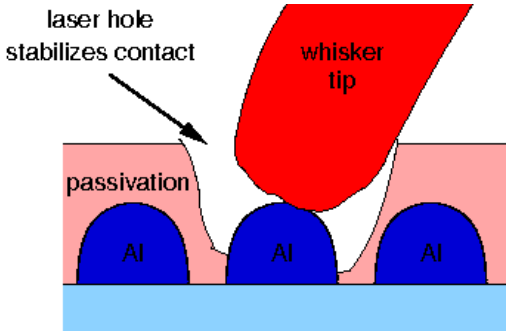




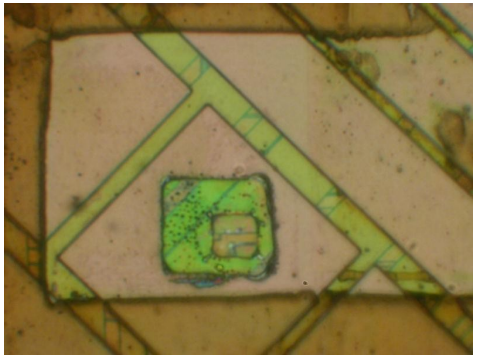
Invasive attacks: microprobing

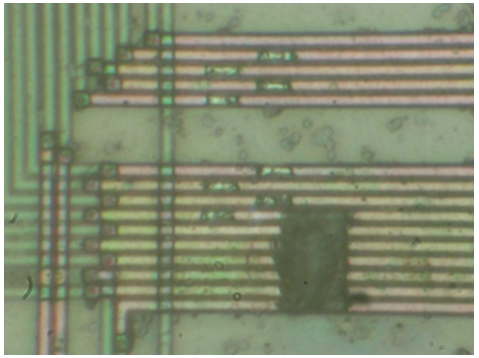
- Laser cutting systems
  - removing polymer layer from a chip surface
  - local removing of a passivation layer for microprobing attacks
  - cutting metal wires inside a chip down to a third metal layer
  - EMA can be performed without removing the passivation layer





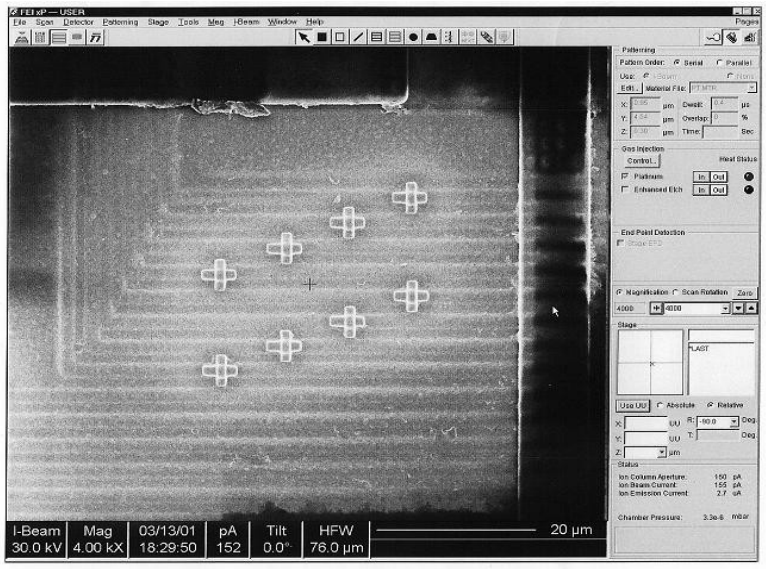
Picture courtesy of Dr Markus Kuhn

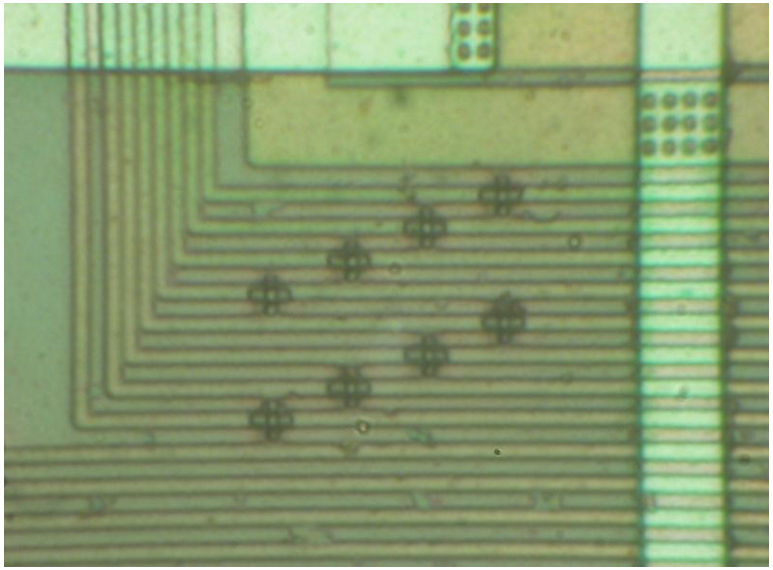




Invasive attacks: chip modification

- Today: Focused Ion Beam workstation
  - chip-level surgery with 10nm precision
  - create small antennas and probing points inside secure chips and eavesdrop on internal communication
  - modern FIBs allow backside access, but require special chip preparation techniques to reduce the thickness of silicon



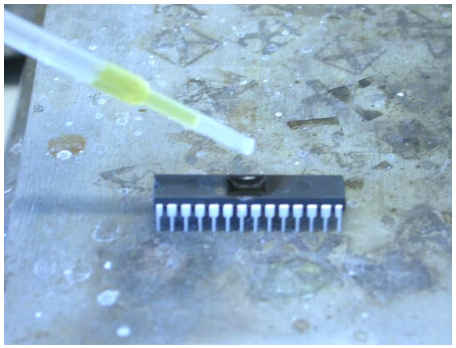
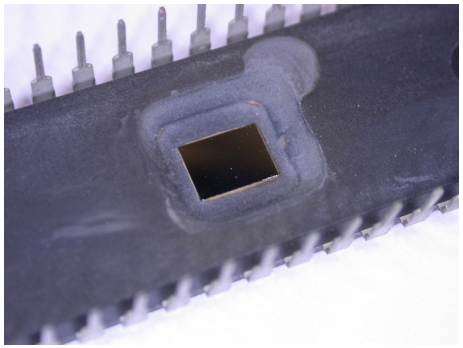
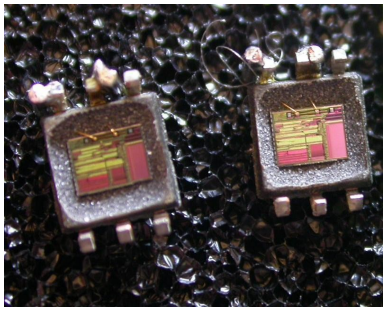
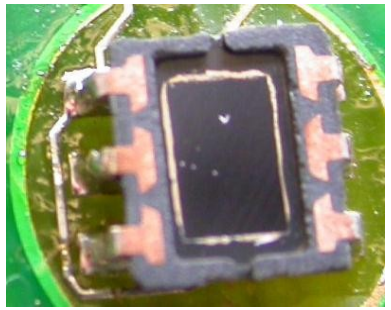
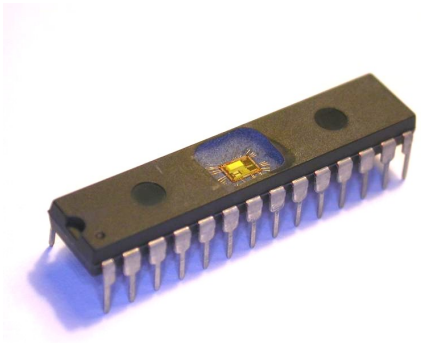
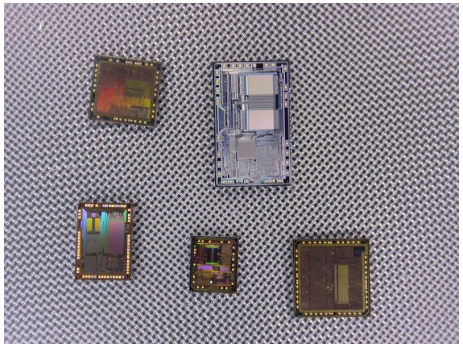
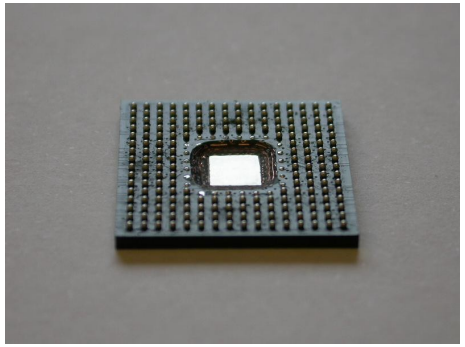


Semi-invasive attacks

- Filling the gap between non-invasive and invasive attacks
  - less damaging to target device (decapsulation without penetration)
  - less expensive and easier to setup and repeat than invasive attacks
- Tools
  - IC soldering/desoldering station
  - simple chemical lab
  - high-resolution optical microscope
  - UV light sources
  - lasers
  - oscilloscope and logic analyser
  - signal generator
  - PC with data acquisition board
  - FPGA board
  - prototyping boards
  - special microscopes (laser scanning, infrared etc.)

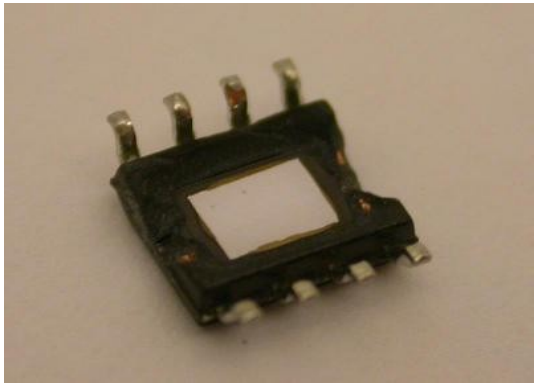
Semi-invasive attacks: sample preparation

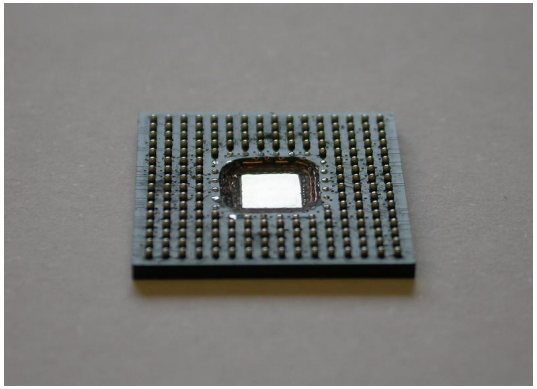
- Decapsulation
  - manual with fuming nitric acid (HNO_3) and acetone at 60ºC
  - automatic using mixture of HNO_3 and H_2SO_4
  - full or partial
  - from front side and from rear side
- Today: more challenging due to small and BGA packages

Backside sample preparation

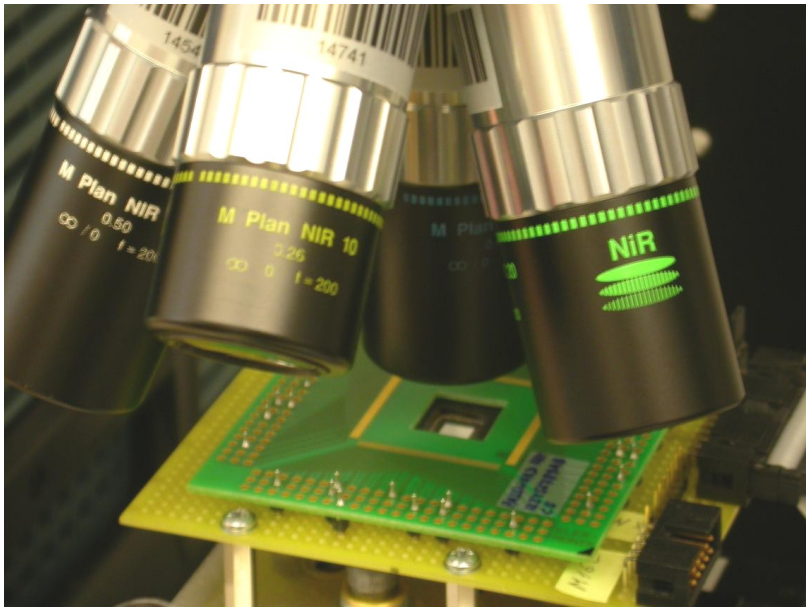
- Sample preparation for modern chips (<0.5μm and >2M)
  - only backside approach is effective
  - it is very simple and inexpensive
  - no chemicals are required





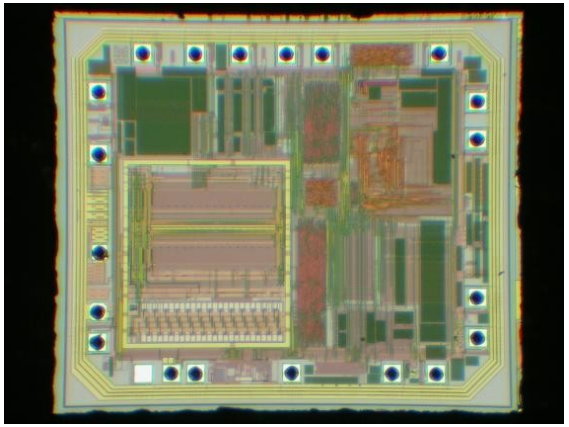
Semi-invasive attacks: imaging

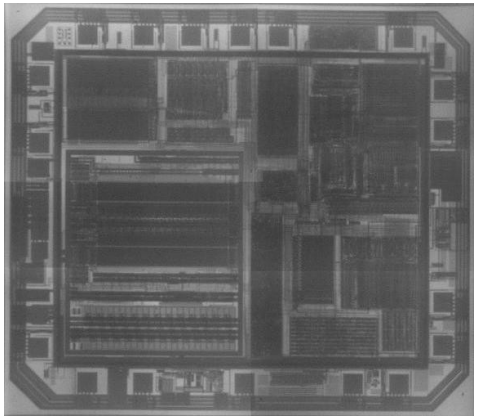
- Backside infrared imaging
  - microscopes with IR optics give better quality of image
  - IR-enhanced CCD cameras or special cameras must be used
  - resolution is limited to ~0.6μm by the wavelength of used light
  - view is not obstructed by multiple metal layers



Semi-invasive attacks: imaging

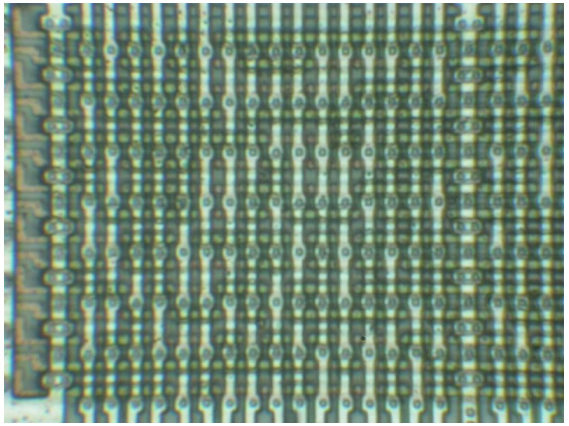
- Backside infrared imaging
  - Mask ROM extraction without chemical etching
- Today: the main option for 0.35µm and smaller chips
  - multiple metal wires do not block the optical path

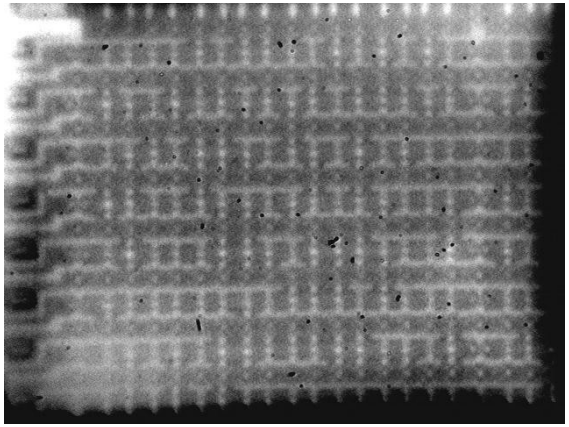




Texas Instruments MSP430F112 microcontroller

0.35 µm



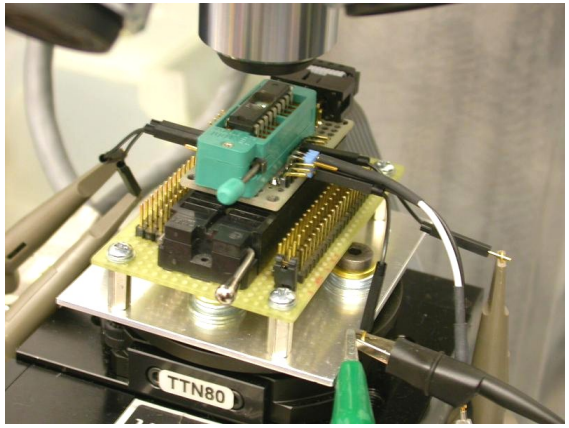


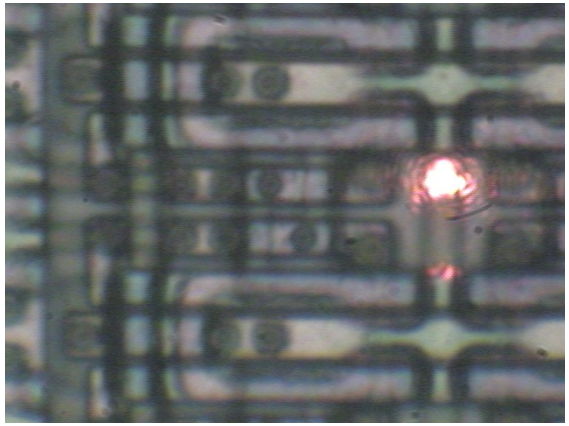
Motorola MC68HC705P6A microcontroller

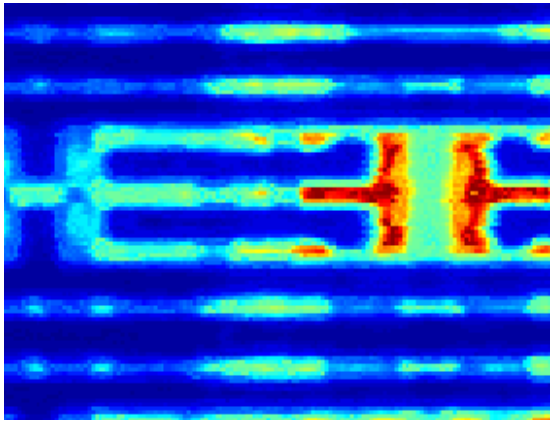
1.2 µm

Semi-invasive attacks: side-channel

- Optically enhanced position-locked power analysis
  - Microchip PIC16F84 microcontroller with test program at 4MHz
  - classic power analysis setup (10Ω resistor in GND, digital storage oscilloscope) plus laser microscope scanning setup
  - test pattern
    - run the code inside the microcontroller and store the power trace
    - point the laser at a particular transistor and store the power trace
    - compare two traces

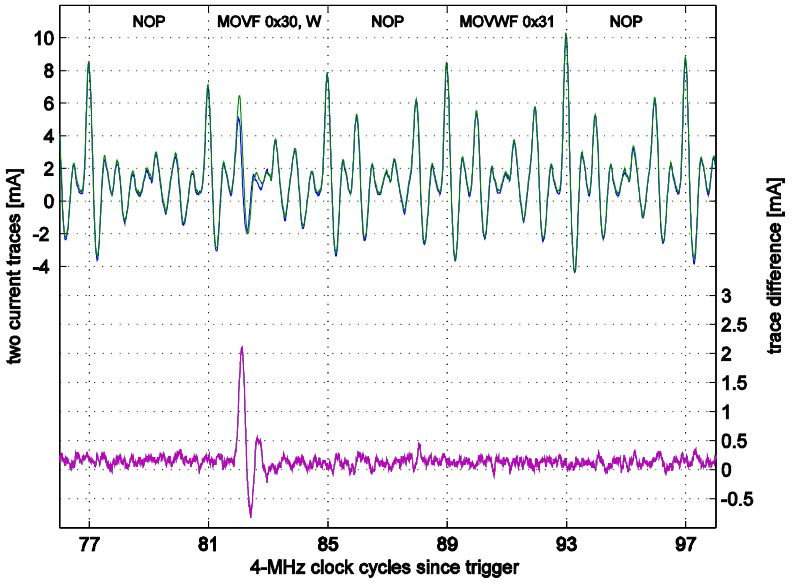


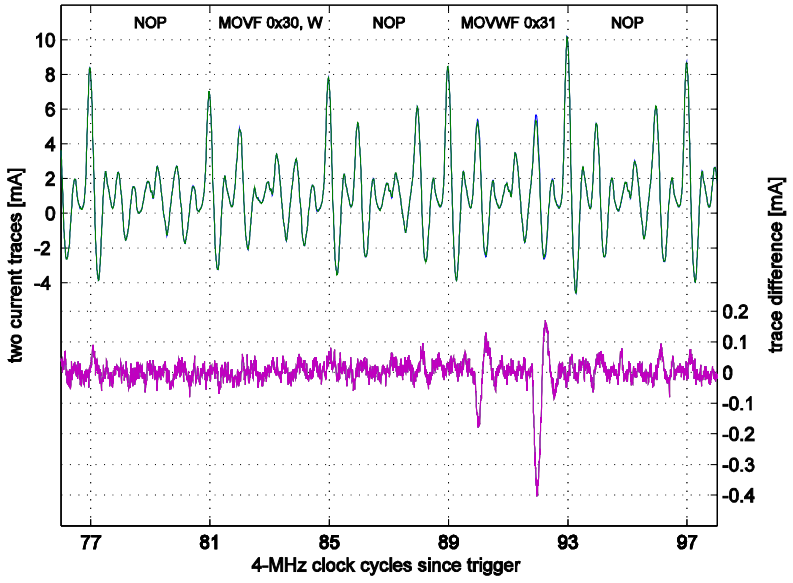




Semi-invasive attacks: side-channel

- Optically enhanced position-locked power analysis
  - results for memory read operations: non-destructive analysis of active memory locations (‘0’ and ‘1’)
  - results for memory write operations: non-destructive analysis of active memory locations (‘0→0’, ‘0→1’, ‘1→0’ and ‘1→1’)
- Today: backside approach for 0.35µm and smaller chips
  - single-cell access is limited to 0.5µm laser spot





Semi-invasive attacks: side-channel

- Operating semiconductor circuits emit photons
  - known for over 40 years
  - actively used in failure analysis for over 20 years
- Existing failure analysis techniques
  - picosecond imaging circuit analysis (PICA) uses photomultiplier array
  - photon emission microscopy (PEM) uses special IR cameras
  - both techniques are expensive and require sophisticated sample preparation
- What about hardware security?
  - any possibility of seeing internal signals?
  - any leaks from memory arrays?

Semi-invasive attacks: side-channel

- Challenges
  - find low-cost detectors suitable for optical emission analysis
  - reduce the cost of sample preparation
- Any technical progress for the past 20 years?
  - are modern CCD cameras good for the attack?
  - what about photomultipliers (PMT)?
  - what parameters are essential for such detectors?
- If optical emission from operating chip has correlation with processed data, is there any correlation between photon emission and power consumption?
  - if found, this can be used for finding weak spots in protection against power analysis attacks
  - optical emission can be scaled down to an individual transistor

Semi-invasive attacks: side-channel

- What is the problem with optical emission analysis attacks?
- Number of photons emitted per every switch of a transistor

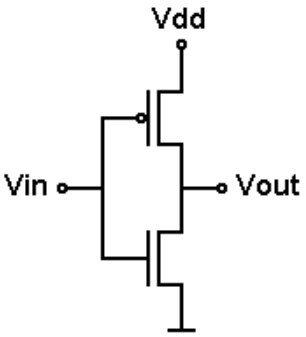
  $N_e = S_e B(L_H I_d / q v_s) T_s \sim 10^{-2}...10^{-4}$ photons/switch

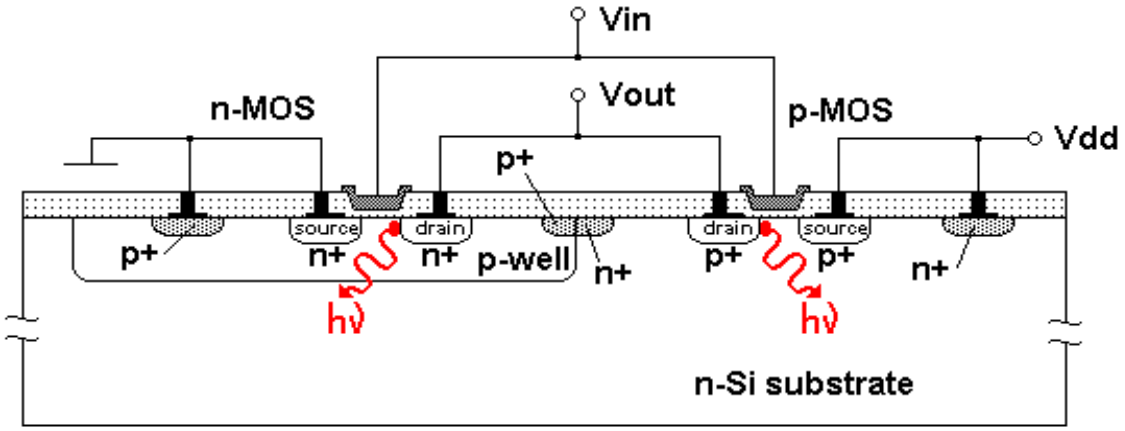
  S_e – spectral emission density, B – emission bandwidth, L_H – hot-carrier region length,

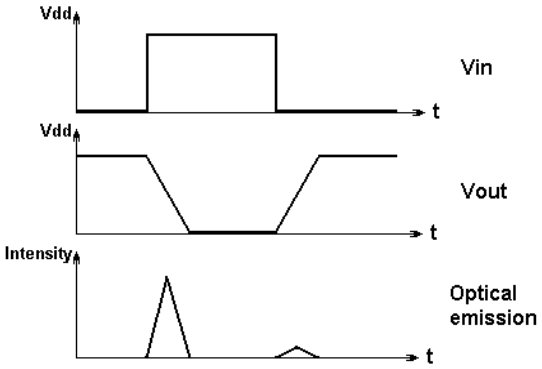
  I_d – drain current, q – e^- charge, v_s – carrier saturated velocity, T_s – transition time
- Emission spectrum is from ~500nm to above 1200nm with maximum emission at 900nm…1100nm (NIR region)
- Small fraction of emitted photons can be detected: <1%
  - emission is isotropic, so with a lens only 25%…45% is observed
  - there are losses in optics due to reflections and absorption (80%)
  - low quantum efficiency (QE) of detectors in NIR region: 1%…20%
- Backside approach: <0.1%
  - high refractive index of silicon (n_{1000nm}=3.58) causes high reflection (32%) and low critical angle (θ=16.2º) results in reduced aperture

Background

- Optical emission is higher from the n-MOS transistor due to higher mobility of electrons
- Emission takes place near the drain area where the speed of carriers declines





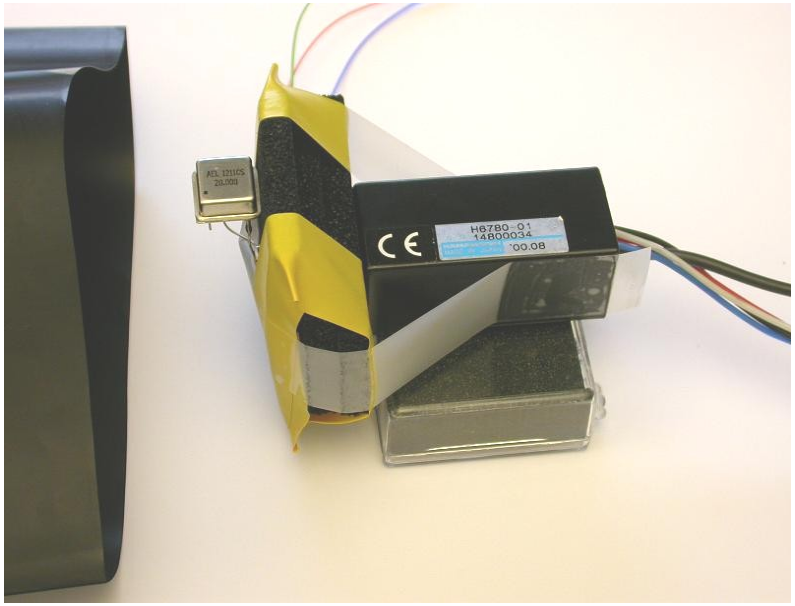


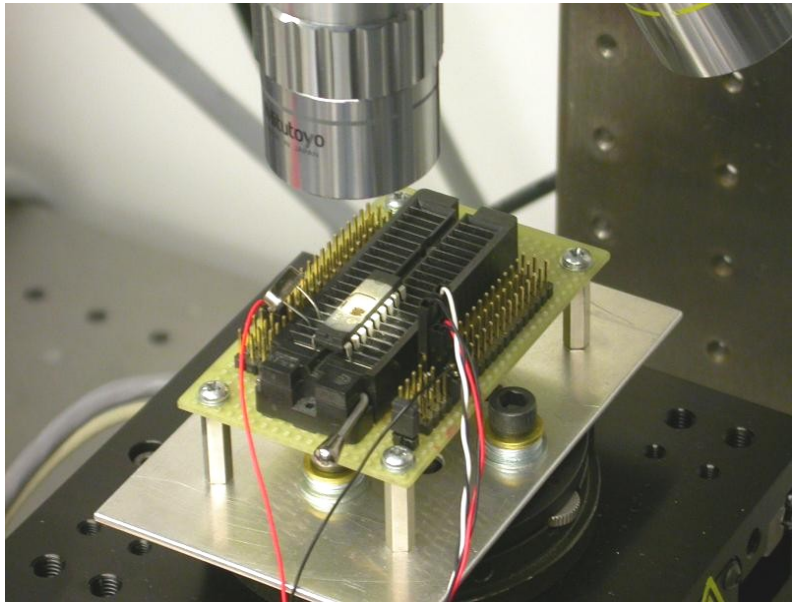
Experimental setup

- Challenges in choosing the right detector
  - single-photon sensitivity
  - low emission intensity requires longer integration time, hence, detectors must have low noise and low dark current
  - NIR emission spectrum requires detectors sensitive in that area
- Photomultiplier (PMT)
  - single-sensor detector with large aperture and fast detection
- Avalanche photodiode (APD)
  - single-sensor detector with small aperture and fast detection
- Cameras with charge-coupled devices (CCD)
  - 2D detector with high resolution: 500x500 to 4000x3000
  - very low frame rate: 10μs to 1s
  - CCTV and hobbyist astronomical cameras have low dark current, good NIR sensitivity and affordable price

Experimental setup

- PMT setup: decapsulated chip facing sensor's aperture
  - Hamamatsu H6780-01 PMT sensor
- CCD setup: camera mounted on a microscope with the chip placed in a test socket
  - Starlight Xpress SXV-H9 CCD camera



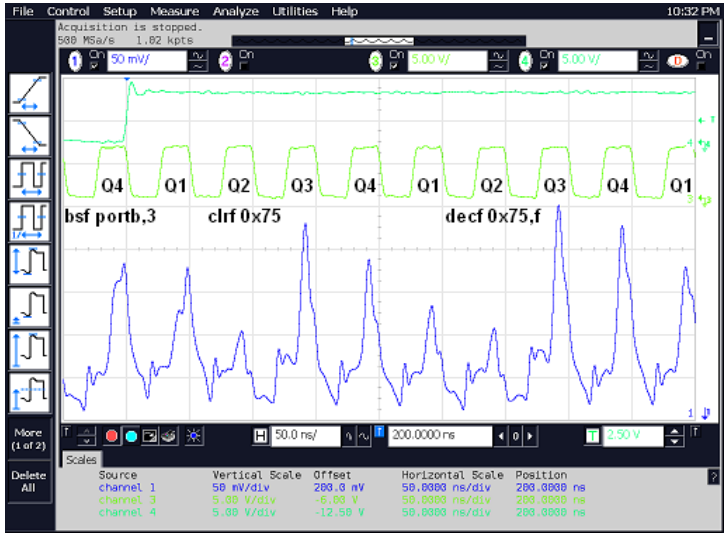


Results

- PMT: 60' acquisition time, digital storage oscilloscope in color-graded mode with infinite persistence with histogram
- SPA: 10Ω resistor, digital storage oscilloscope with active probe
- Test code:

```
bsf portb,3
clrf 0x75
decf 0x75,f
bcf portb,3
goto loop
```

- PMT vs SPA
  - higher bandwidth
  - special hardware will suit better as oscilloscope is not designed for long-time integration (latency issue)



Results

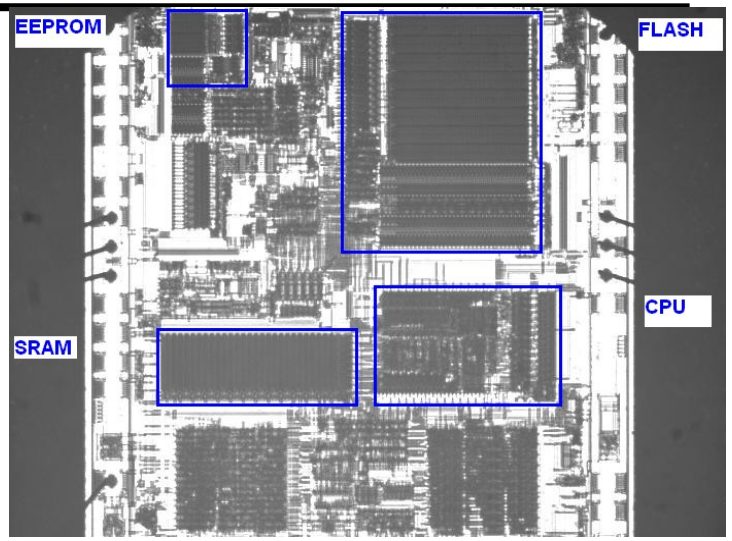
- CCD
  - 2× objective lens
  - 30' integration time
  - EEPROM data: 00h, FFh
  - SRAM data: variable 00h…FFh
  - continuous EEPROM reading and SRAM writing and reading
- Test code: incf EEADR,f

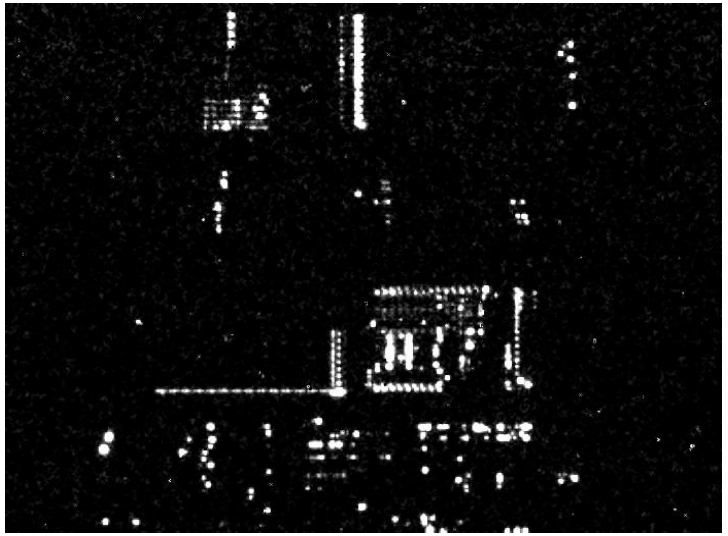
  bsf EECON1,RD

  movf EEDATA,w

  decf 0x75,f

  goto loop
- 2D image with recognisable areas of emission from Flash, EEPROM, SRAM and CPU





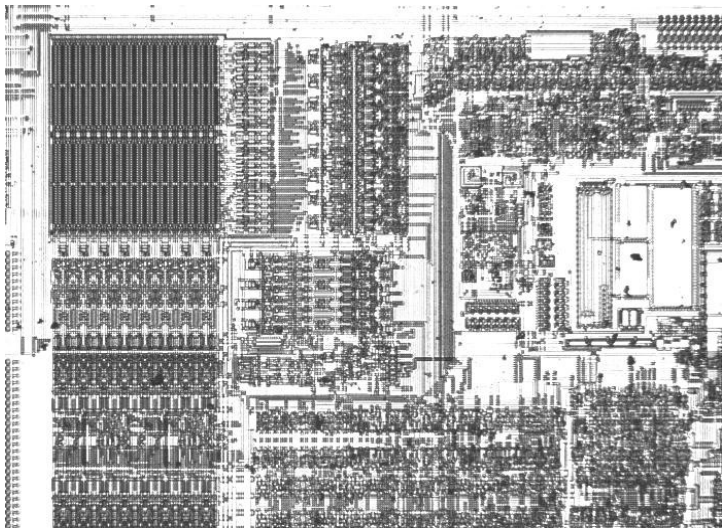
Results

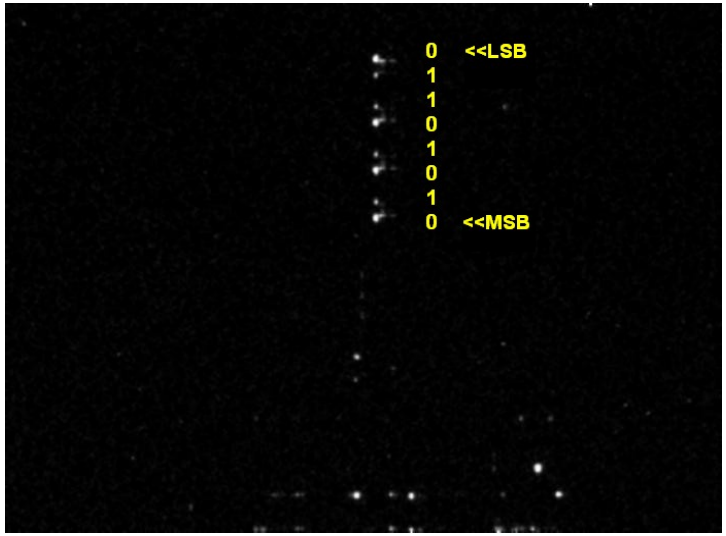
- EEPROM area
  - 10× objective lens
  - 10' integration time
  - data: 56h, 56h, 56h…56h, 00h
  - continuous EEPROM reading
- Test code: incf EEADR,f

  bsf EECON1,RD

  movf EEDATA,w

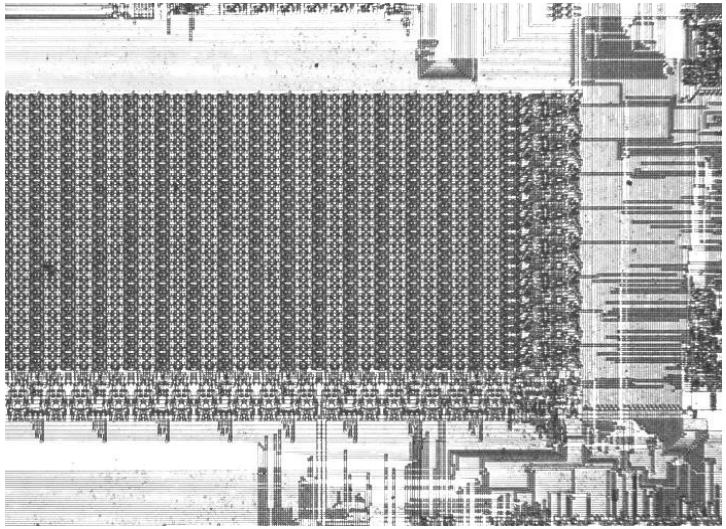
  goto loop
- Flash memory has similar structure and gives similar result
  - data extraction is complicated by the fact that program code is executed from the flash memory

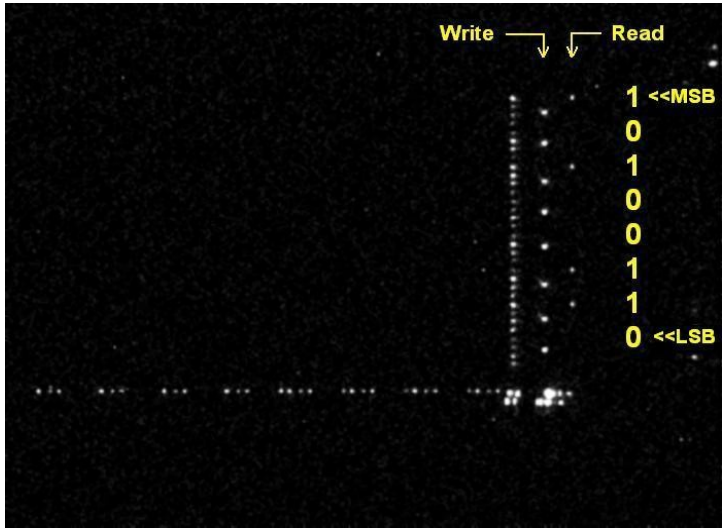




Results

- SRAM area
  - 10× objective lens
  - 10' integration time
  - data: A6h, W=A6h
  - continuous reading and writing
- Test code: movf 0x75, w movwf 0x75
  goto loop goto loop
- Low emission from memory cells
  - write drivers, bus drivers, row and column selectors leak the most
- Write data have the same emission for ‘0’ and ‘1’
  - dual-rail logic used in SRAM: separate bit lines for writing ‘0’ & ‘1’
  - difference in the emission could predict leakage in the power trace





Limitations and improvements

- Data recovery
  - slow process: minimum 1 minute per byte
- Modern chips
  - three or more metal layers prevent direct observation and analysis
  - smaller technologies will require longer integration time
- Backside approach
  - silicon is transparent to light with wavelengths above 1000 nm
  - lower spatial resolution of ~1μm ($R=0.61\lambda/NA$)
  - longer integration time due to higher losses in silicon and optics
  - higher magnification lenses give better result
  - use of NIR optics improves result, but expensive
  - substrate thinning and AR coating are useful, but expensive
  - increase of the power supply voltage boosts the optical emission

Limitations and improvements

- Increasing the power supply voltage: every 10% of increase above nominal voltage boosts the emission by 40%…120%
- PIC16F628: EEPROM reading

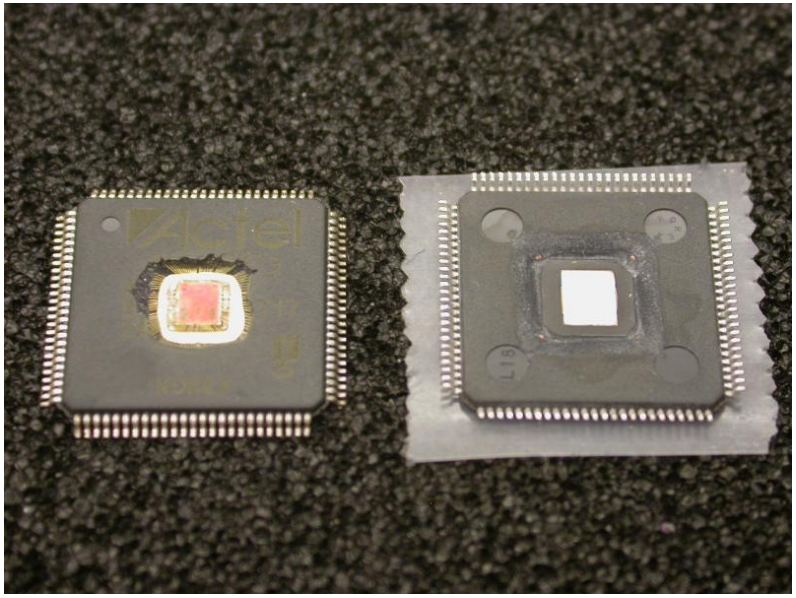
Power supply voltage	3.5V	4.0V	4.5V	5.0V	5.5V	6.0V
Photometry results	1046	1286	2427	8400	23292	43026

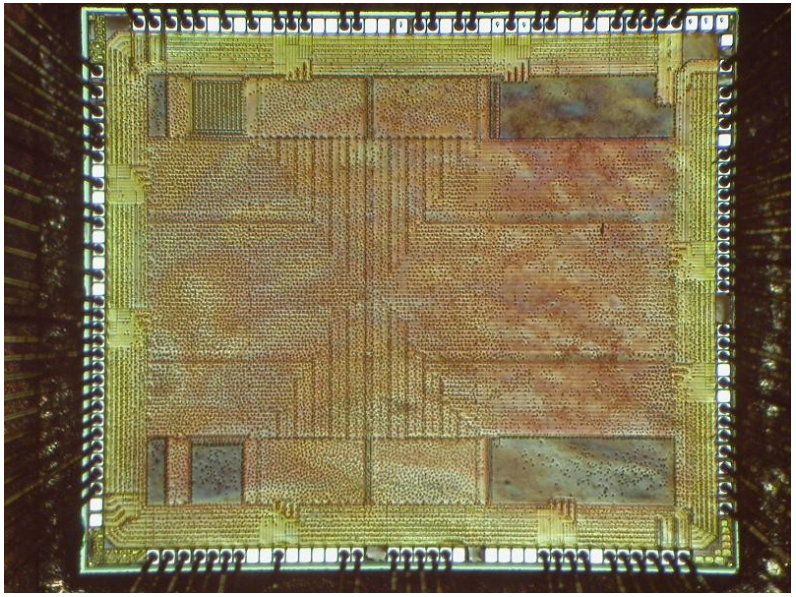
Semi-invasive attacks: side-channel

- Optical emission analysis: new challenges
  - Actel® ProASIC3® 0.13µm, 7 metal layers, flash FPGA
  - *"highly secure FPGA"* which is reprogrammable, non-volatile, single-chip and live-at-power-up solution
  - *"offer one of the highest levels of design security in the industry"*
  - robust design security features: flash logic array, flash ROM, security fuses, FlashLock™, AES
  - *"even without any security measures (such as FlashLock with AES), it is not possible to read back the programming data from a programmed device"*
  - allows secure ISP field upgrades using 128-bit AES-encrypted bitstream with AES authentication and MAC verification
  - other security measures: voltage monitors, internal charge pumps, asynchronous internal clock and many others

Semi-invasive attacks: side-channel

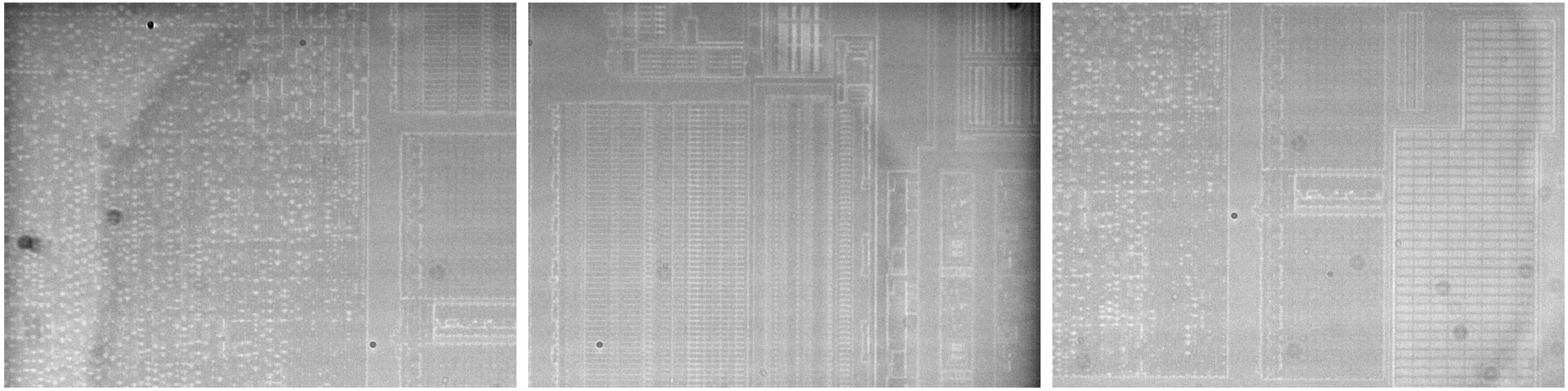
- Sample preparation of A3P060 FPGA: front and rear
  - the surface is covered with sticky polymer which needs to be removed for physical access to the surface
  - >99% of the surface is covered with supply grid and dummy fillers
  - backside: low-cost approach used – without any treatment





Semi-invasive attacks: side-channel

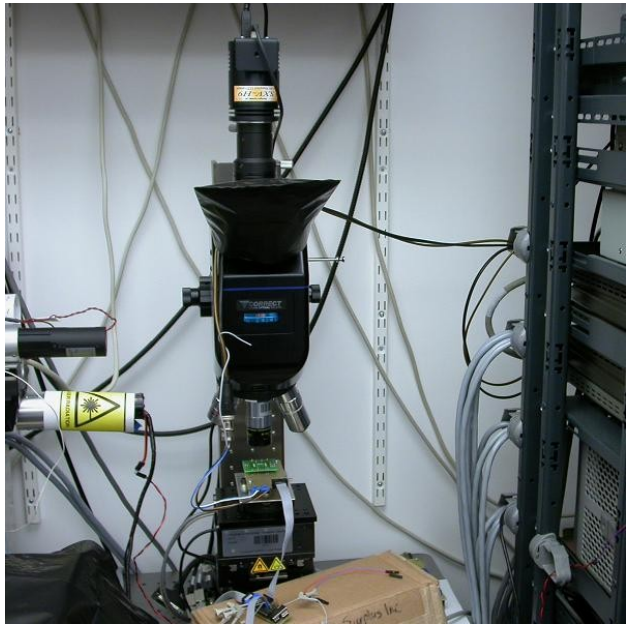
- Backside imaging is the only possibility
  - low spatial resolution of about 1μm (R=0.61λ/NA=0.61·1000/0.5)
- 20× NIR objective lens, light source with Si filter
- Locating internal blocks: JTAG, Flash ROM, SRAM
- Optical emission analysis
  - power supply was increased from 1.5V to 2.0V to boost the emission

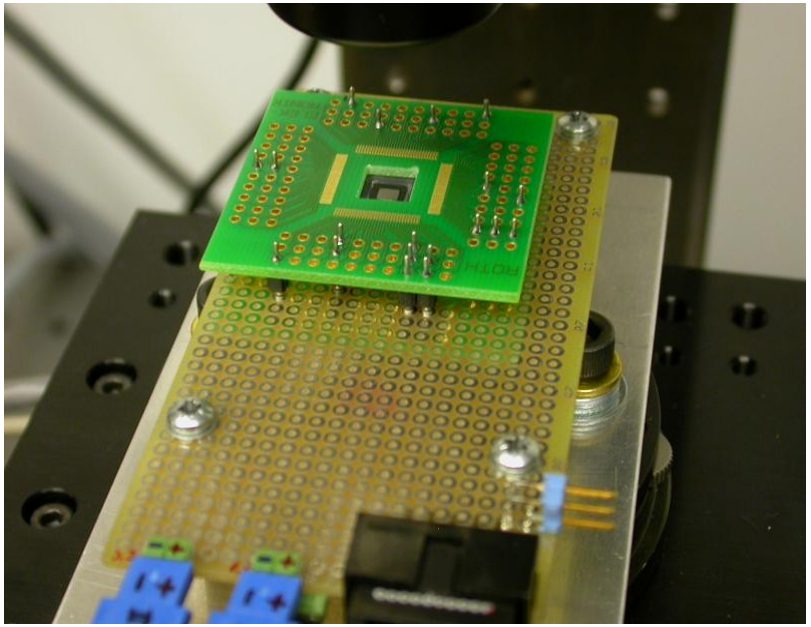


Semi-invasive attacks: side-channel

- Increasing the power supply voltage: every 10% of increase above nominal Vcc boosts the emission by 40%…120%
- A3P060: JTAG ID reading

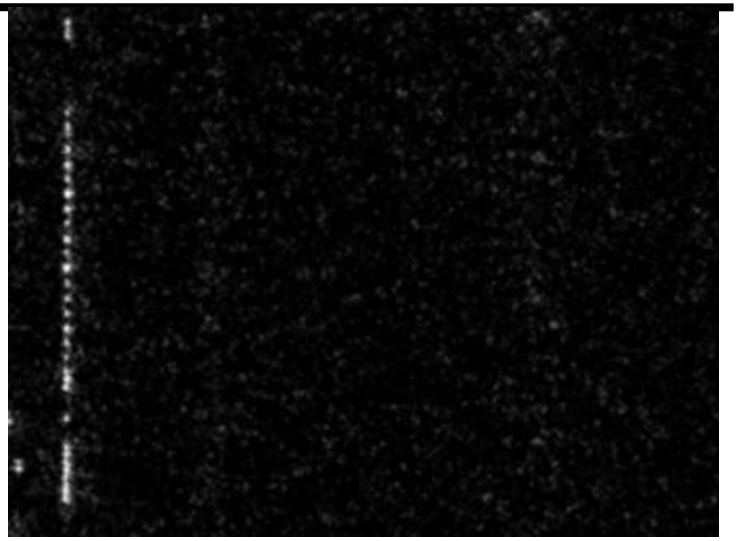
Power supply voltage	1.5V	1.6V	1.8V	2.0V	2.2V	2.5V
Photometry results	889	1194	1953	5270	9536	23270

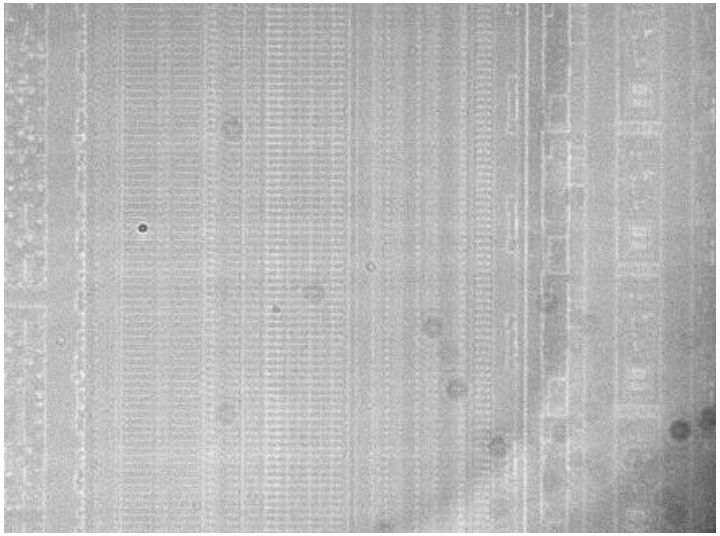


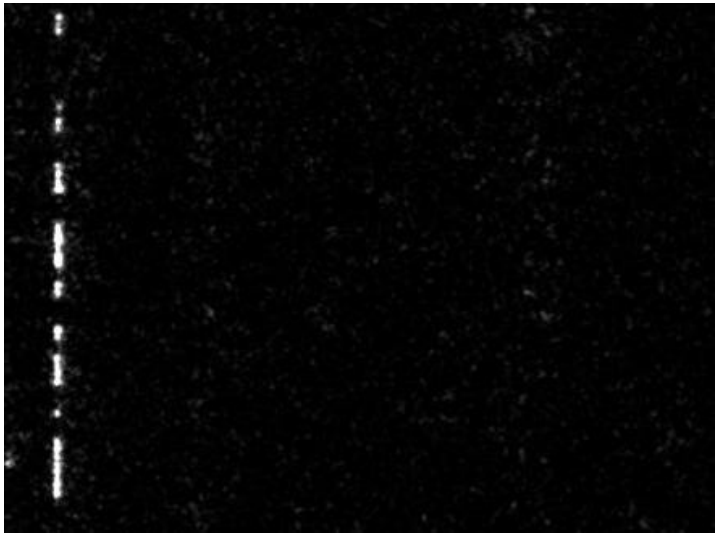


Semi-invasive attacks: side-channel

- Flash ROM (Settings + Data)
  - 20× NIR objective lens
  - 60' integration time
  - continuous reading
- Recognisable data pattern
  - some data can be extracted
  - gives information about location

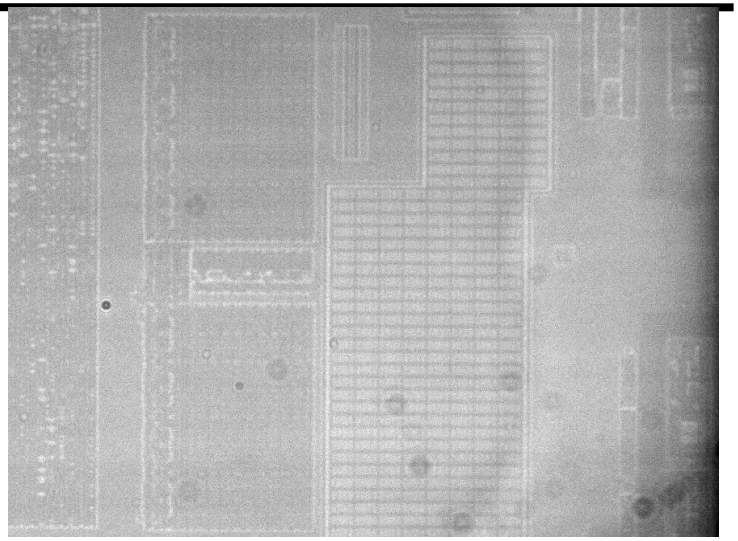


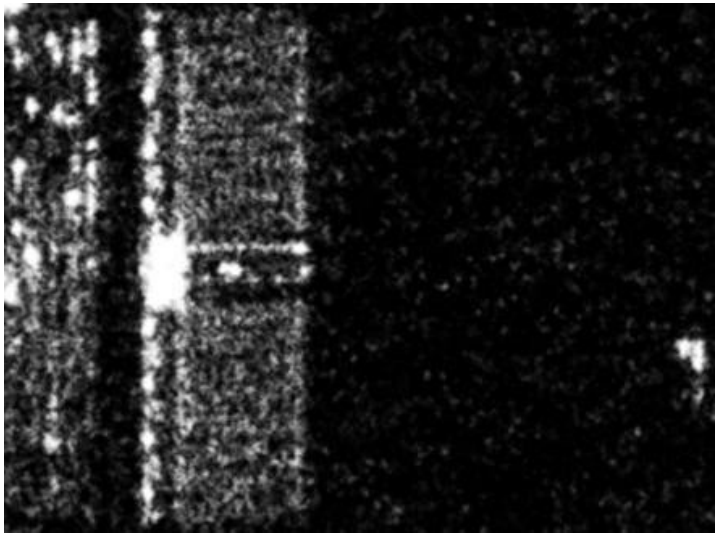




Semi-invasive attacks: side-channel

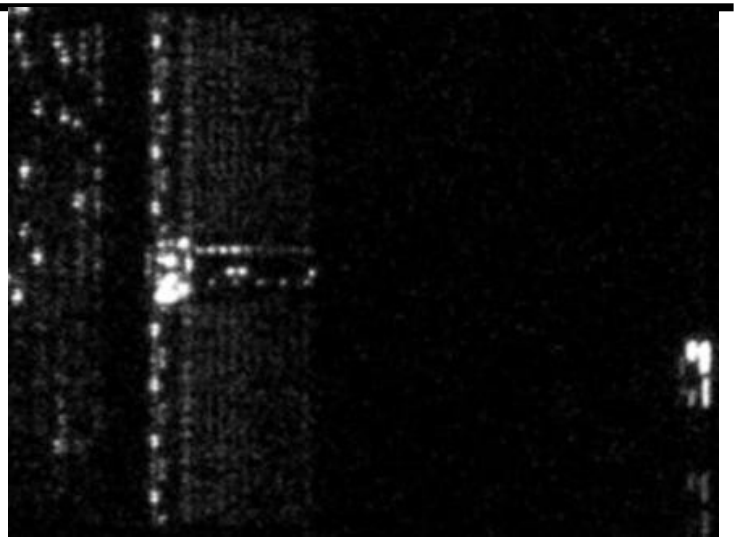
- SRAM dedicated for AES
  - 20× NIR objective lens
  - 120' integration time
  - continuous initialisation
- AES key recovery
  - key scheduling used in AES
  - AES key can be easily calculated from any round key
  - existence of separate JTAG commands for AES initialisation, authentication and decryption
  - information is leaked by the SRAM array and write drivers

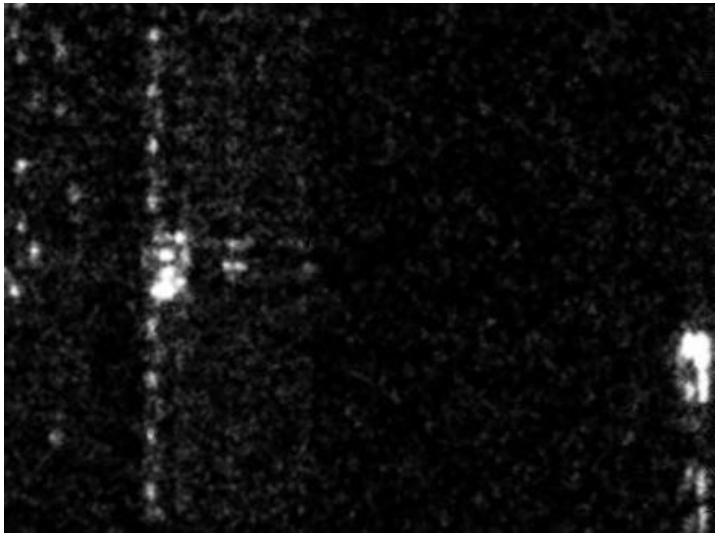




Semi-invasive attacks: side-channel

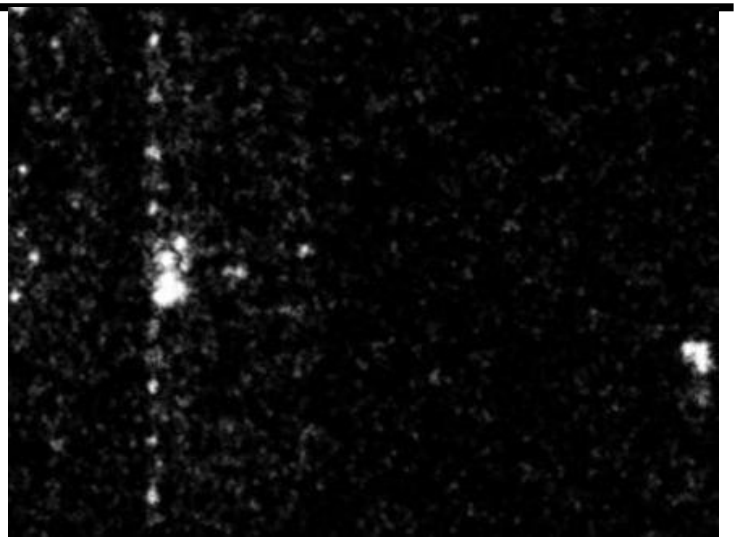
- SRAM dedicated for AES
  - 20× NIR objective lens
  - 120' integration time
  - continuous initialisation
- Exploiting power supply trick
  - alternating the supply voltage during the operation: 2.0V peak
  - 16μs per AES initialisation
  - 1.6μs per each round key: calculation + storage
  - 16 bit at a time: 8 write cycles

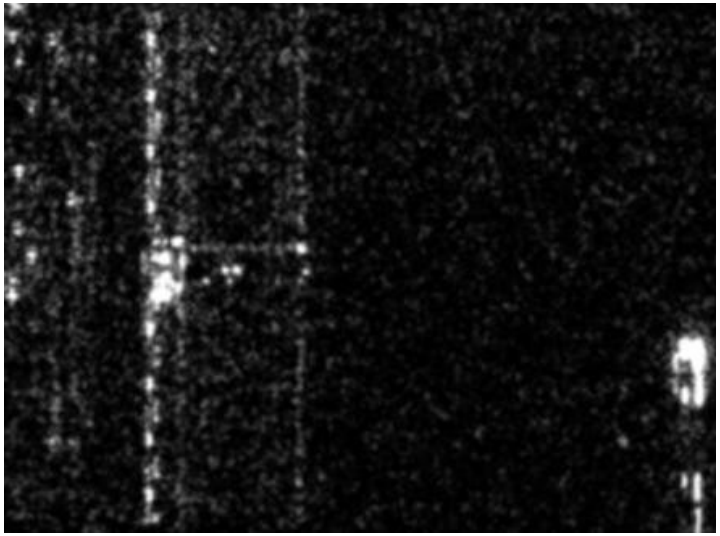


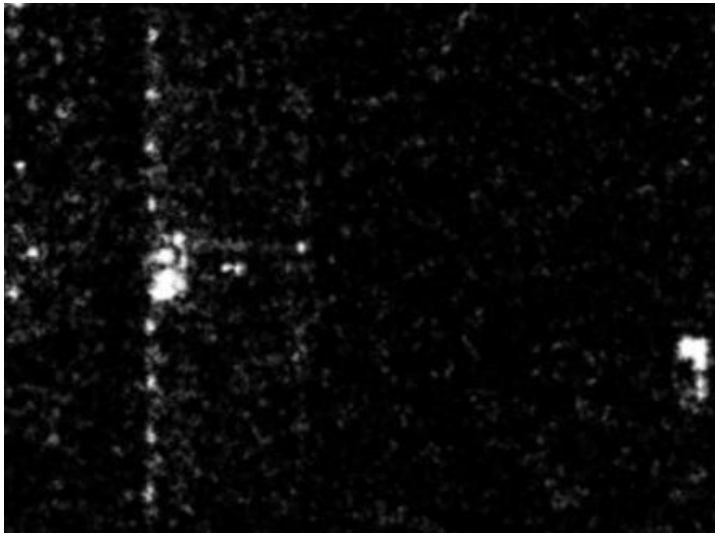


Semi-invasive attacks: side-channel

- SRAM dedicated for AES
  - 20× NIR objective lens
  - 120' integration time
  - continuous initialisation
- Exploiting power supply trick
  - alternating the supply voltage during the round key operation: 2.5V peak
  - 0.2μs increase of the supply voltage from 1.5V to 2.5V for one write cycle







Comparing the attack methods

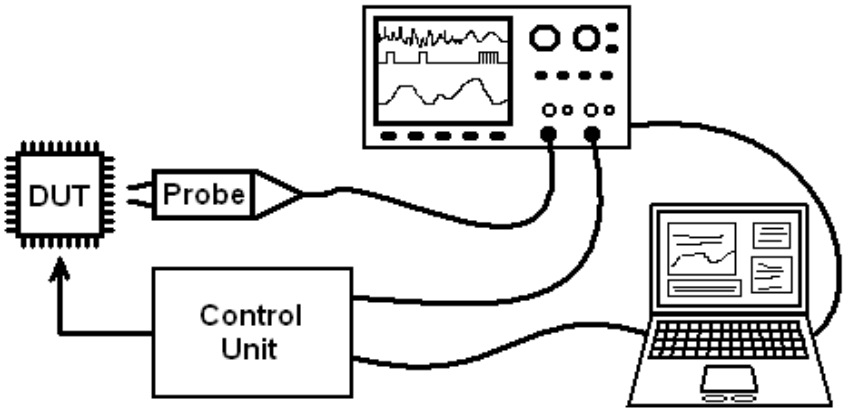
- Target: Actel ProASIC3 secure FPGA family (military use)
  - secure configuration data update using AES-128 encryption
  - designed to prevent IP theft, cloning and overbuilding
- Can we attack the AES key used for bitstream encryption?
  - if the AES key is known then the device can be cloned
- Invasive attacks (expensive)
  - partial reverse engineering followed by microprobing
- Semi-invasive attacks (affordable)
  - optical fault injection attack
  - optical emission analysis
- Non-invasive attacks (simple)
  - side-channel attacks such as SPA, DPA, CPA, EMA, DEMA
  - poor signal-to-noise ratio of about −15dB due to low-power operation and multiple sources of noise (internal clock operaton, charge pumps, low level of the leakage signal)

How long does it take to get the AES key?

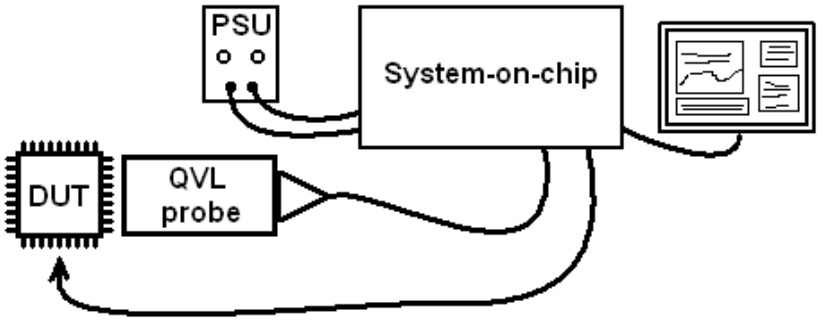
- Initial evaluation time for all attacks from 1 week – 1 month
- Invasive attacks (microprobing)
  - **1 day** with FIB and probing station
- Semi-invasive attacks (side-channel and fault attacks)
  - **1 week/1 hour** with optical emission analysis (FDTC2009)
  - **1 hour** with optical fault injection attack (CHES2002)
- Non-invasive attacks (side-channel attacks)
  - **1 day** with low-cost DPA setup: resistor in V_{CC} core supply line, oscilloscope with active probe and PC with MatLab software
  - **1 hour/10 minutes** with commercial DPA tools (DPA Workstation from Cryptography Research Inc. or Inspector SCA from Riscure)
  - **1 second** with QVL-E board using special SCA sensor from QVL
  - **0.01 second** with QVL/Espial tester using breakthrough approach to power analysis technique from QVL

New technology to improve attacks

- Standard side-channel analysis setup



- New more efficient setup



- Plus another 9 problems to address and solve in order to get from 100 to 1'000'000 times improvement
  - what if 99% of information is lost during acquisition or 99.9%?

QVL technology

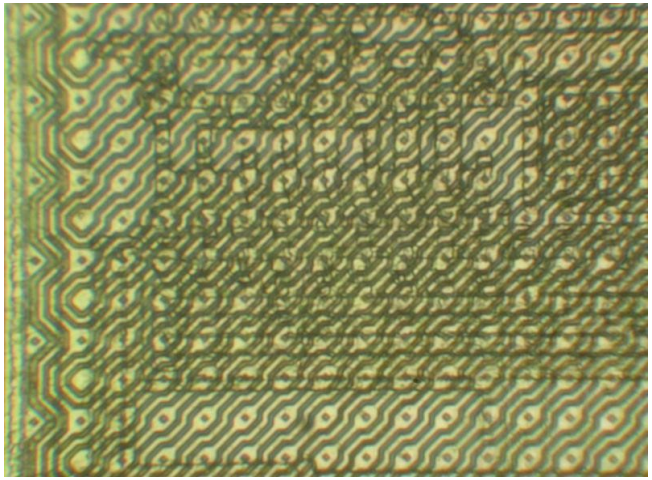
- Overview
  - new approach to sensor technology: precision measurements with higher sensitivity and lower noise compared to standard technology
  - does not add new attacks – just revisit the existing: what was not possible due to high cost and long time required, becomes feasible
- Capabilities
  - extract cryptographic keys and passwords
  - reverse engineering of algorithms and internal operations
  - monitor device activity to spot faults, trojans and backdoors
- Applications
  - failure analysis, security evaluation, chip health monitoring
  - scanning for trojans and backdoors inserted by third parties
- Information
  - QVL technology is being evaluated for various secure chips
  - http://www.quovadislabs.com/

Quest for trojans and backdoors

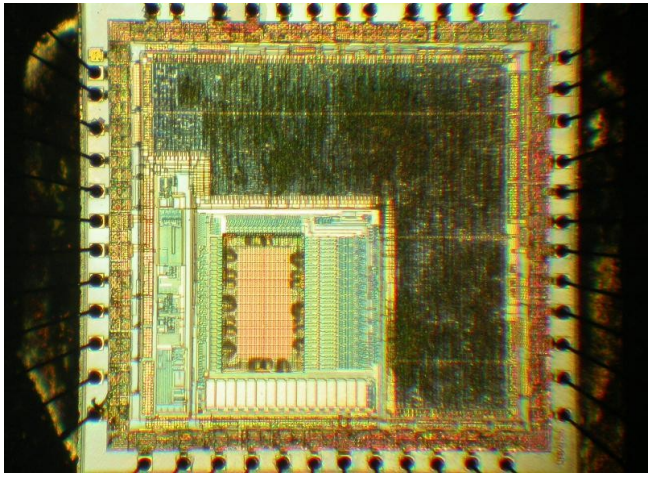
- What x1'000'000 improvement would mean for real device?
  - 1 day for an attack which normally takes 2000 years to succeed
  - 1 second for an attack which normally takes 10 days to succeed
- It might be OK to have backdoors and trojans in highly secure devices, but they should be kept secret and never used to boost the existing security measures
- QVL technology was successfully tested on real chips
  - Actel secure FPGAs: ProASIC3, Igloo, Fusion and SmartFusion
- Actel secure FPGAs have some security engineering bugs
  - it is possible to use the secret factory access key for generating authentication signature with AES and then attack it with SCA
  - latest generation of Flash FPGA devices share the same key
- What can be done if the backdoor secret key is known?
  - turn some ROM areas (OTP) into reprogrammable Flash areas
  - reprogram low-level features
  - access hidden JTAG registers
  - access secret data, information, configuration and IP

Defence technologies: tamper protection

- Additional protections
  - top metal layers with sensors
  - glue logic design hard to reverse engineer
  - voltage, frequency and temperature sensors
  - memory access protection, crypto-coprocessors
  - internal clocks, power supply pumps
  - asynchronous logic design, symmetric design, dual-rail logic
  - ASICs, secure FPGAs and custom-designed ICs
  - software countermeasures



STMicroelectronics ST16 smartcard



Fujitsu secure microcontroller

Defence technologies: what goes wrong?

- Security advertising without proof
  - no means of comparing security, lack of independent analysis
  - no guarantee and no responsibility from chip manufacturers
  - wide use of magic words: *protection, encryption, authentication, unique, highly secure, strong defence, unbreakable, impossible, cannot be attacked, uncompromising, buried under metal layers*
- Constant economics pressure on cost reduction
  - less investment, hence, cheaper solutions and outsourcing
  - security via obscurity approach
- Quicker turnaround
  - less testing, hence, more bugs
- What about back-doors?
  - access to the on-chip data for factory testing purposes
  - how reliably was the factory testing feature disabled?
  - how difficult is to attack the access port?

New directions for research

- Boosting side-channel attacks with new methods and techniques aimed at improvement by a factor of 1'000'000
  - off-the-shelf solution vs special hardware
  - what a million times improvement would mean for a real device?
    - 1 day for an attack which normally takes 2000 years to succeed
    - 1 second for an attack which normally takes 10 days to succeed
- Fixed funds and fixed term attacks?
  - how far could an attacker move given X budget and limited time?
- What is 'practical attack'?
  - could someone achieve key extraction within 1 second and 1000$
- Backdoors testing
  - many chips have Factory test and Debug modes, are they secure?
- Clone dilemma
  - how one can prove that another product is a clone and not a compatible product (forensic analysis within security constraints)?
  - if a product is cloned, how was it done (there are many ways)?

Future work

- Improving semi-invasive attacks
  - some of 180nm, 130nm and 90nm chips were tested
  - preparation for testing 65nm chips is under way
- Seeking collaboration with industry
  - evaluation of products against new attacks
  - developing new attack methods and techniques
  - focusing on low-cost attacks which are more dangerous
- New challenges
  - synchronisation techniques for side-channel attacks
  - improving side-channel attacks with new techniques
  - making previously infeasible attacks possible with the use of new technologies from QVL
- Developing new countermeasures
  - if it takes a few seconds to extract crypto-key or password then existing countermeasures may fail to protect from adversaries

Conclusions

- There is no such a thing as absolute protection
  - given enough time and resources any protection can be broken
- Side-channel attacks pose serious threat to hardware security
  - low-cost setup, small attack time, easy to reproduce
- Defence should be adequate to anticipated attacks
  - security hardware engineers must be familiar with attack technologies to develop adequate protection
  - choosing the correct protection saves money in development and manufacturing
- Attack technologies are constantly improving, so should the defence technologies
- Many vulnerabilities were found in various secure chips and more are to be found, that poses more challenges to hardware security engineers

References

- Slides
  - http://www.cl.cam.ac.uk/~sps32/ECRYPT2011_2.pdf
- Literature:
  - http://www.cl.cam.ac.uk/~sps32/
  - http://www.cl.cam.ac.uk/~sps32/#Publications