Tamper resistance and physical attacks

Part III: Security analysis and defence

Dr Sergei Skorobogatov

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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

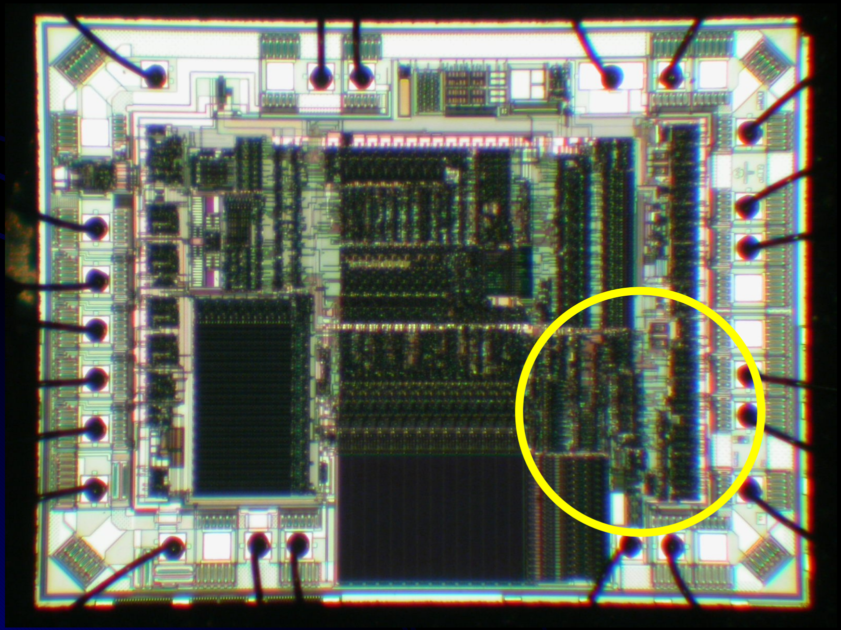
Security Group, TAMPER Lab

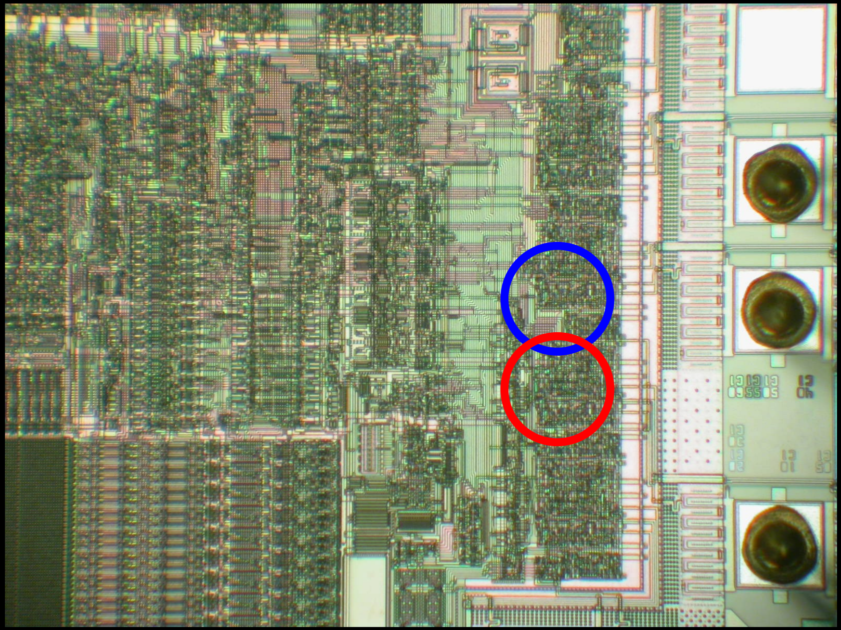
Hardware security analysis

- Design overview
  - Localisation of potentially weak points
  - Analysis of security critical paths
- Finding attack points
  - Systematic search
  - Brute force search
  - Fuzzy search
  - Modelling attacks through simulation

Hardware security analysis

- Using semi-invasive attacks for testing security protection
  - Exposing large area to light flashes
  - Reducing the area of search by using higher magnification and apertures
  - For multipoint security systems, overlapping area shows potential threat

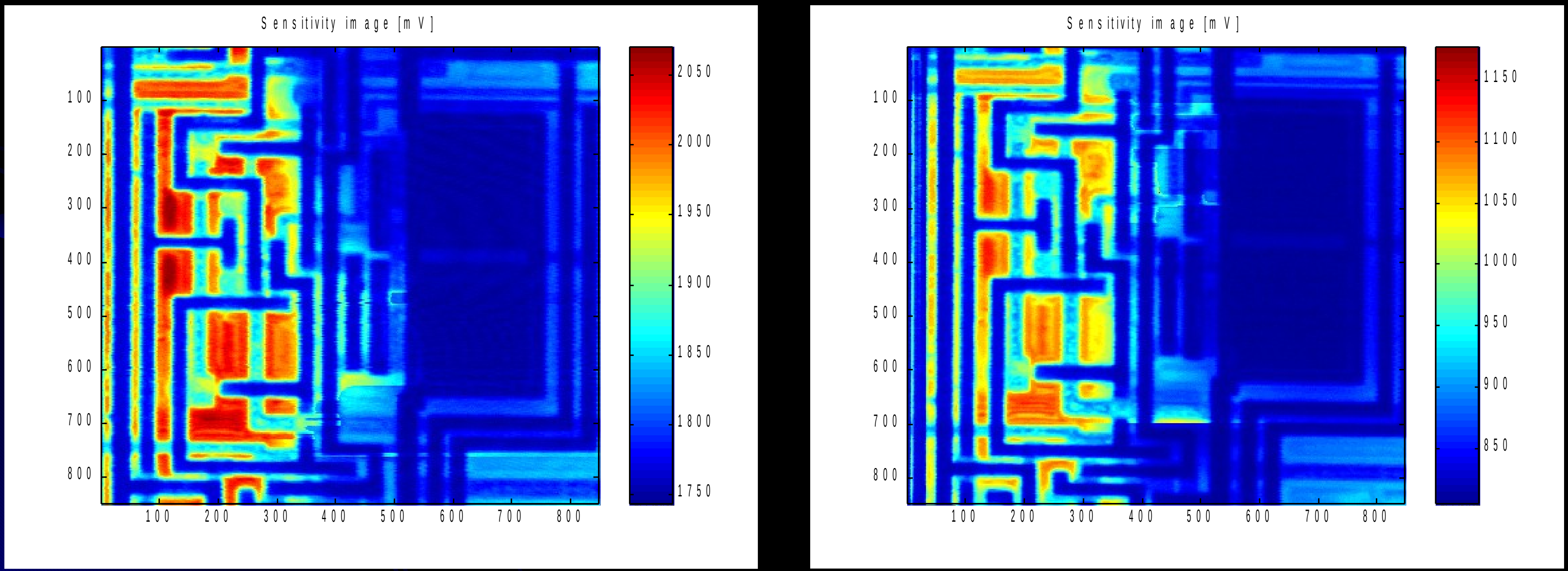




Microchip PIC16C622A microcontroller

Hardware security analysis

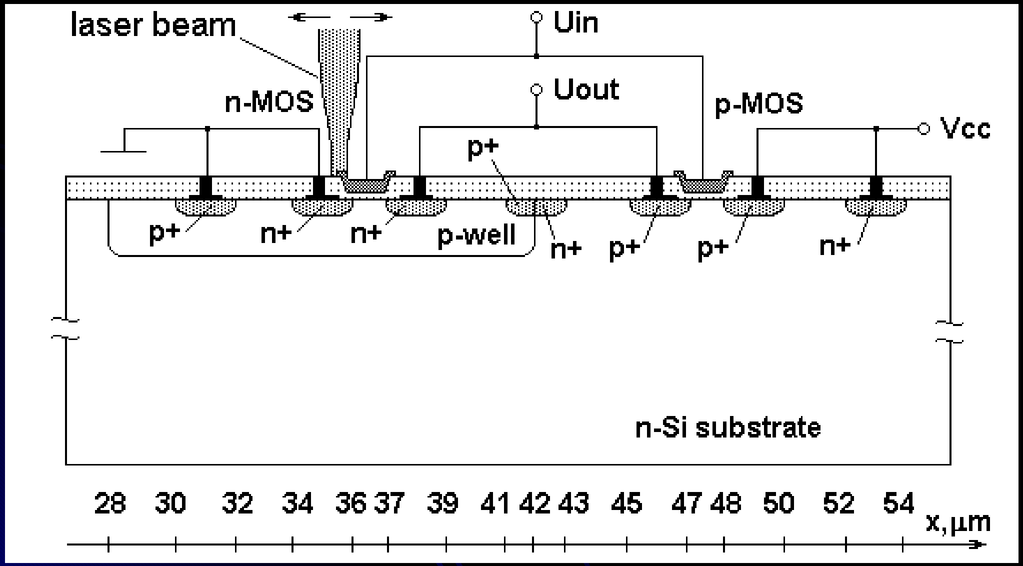
- Using semi-invasive imaging techniques to locate the security fuses
  - Light-induced current variation method
  - Comparing two scans – one for non-secure device, other for secure

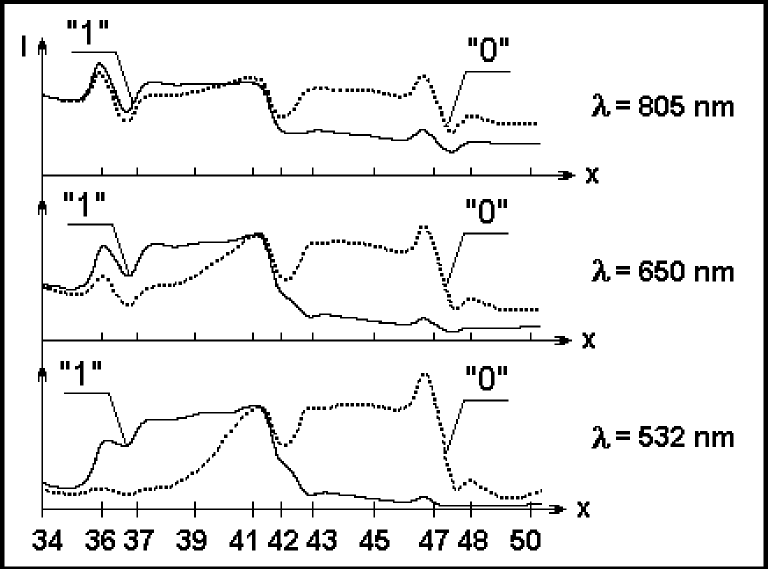


Microchip PIC16F84 microcontroller

Hardware security analysis

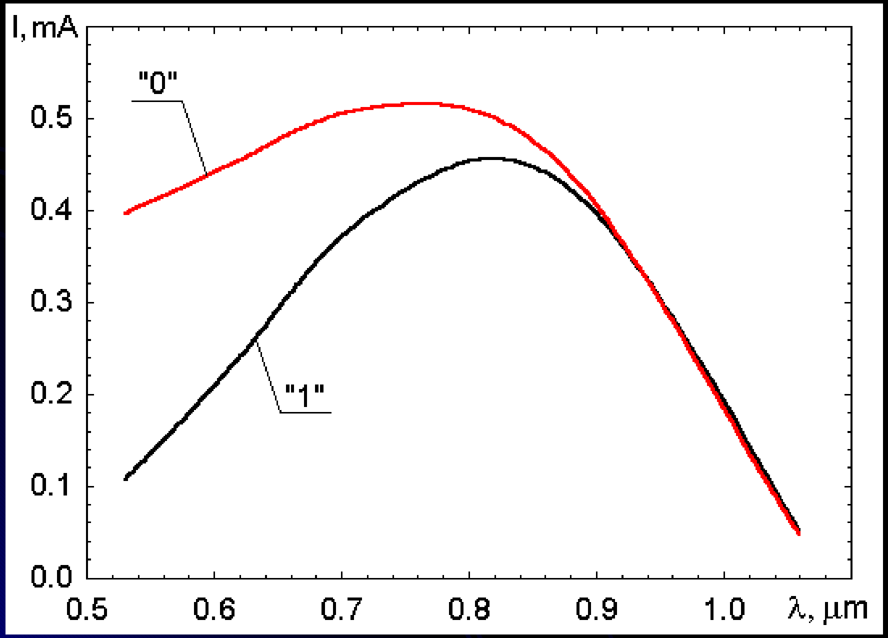
- Modelling of semi-invasive attacks (DIODE-2D software)
  - Detecting the logic state of CMOS transistors through photocurrent
    - Wavelength and location dependence
    - Technology dependence

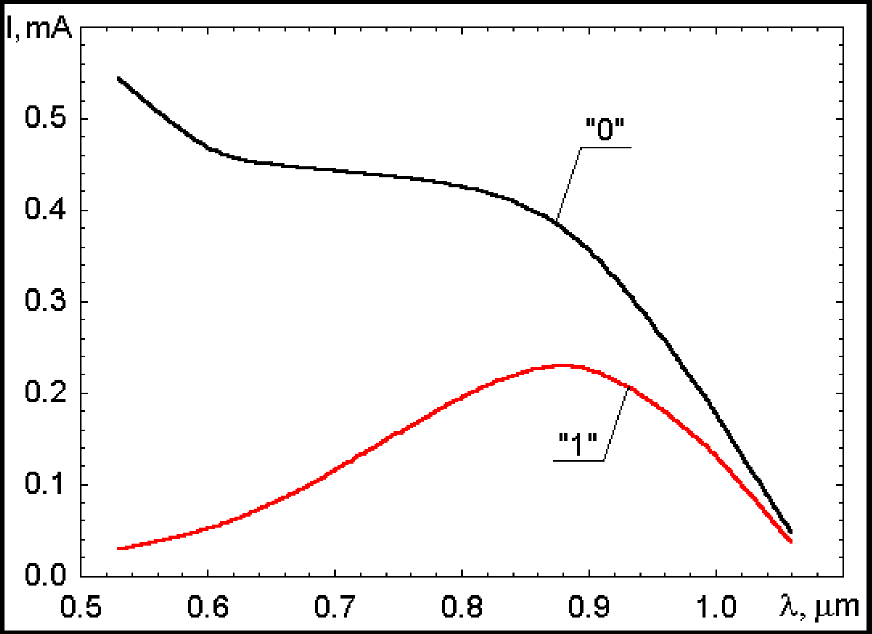




Hardware security analysis

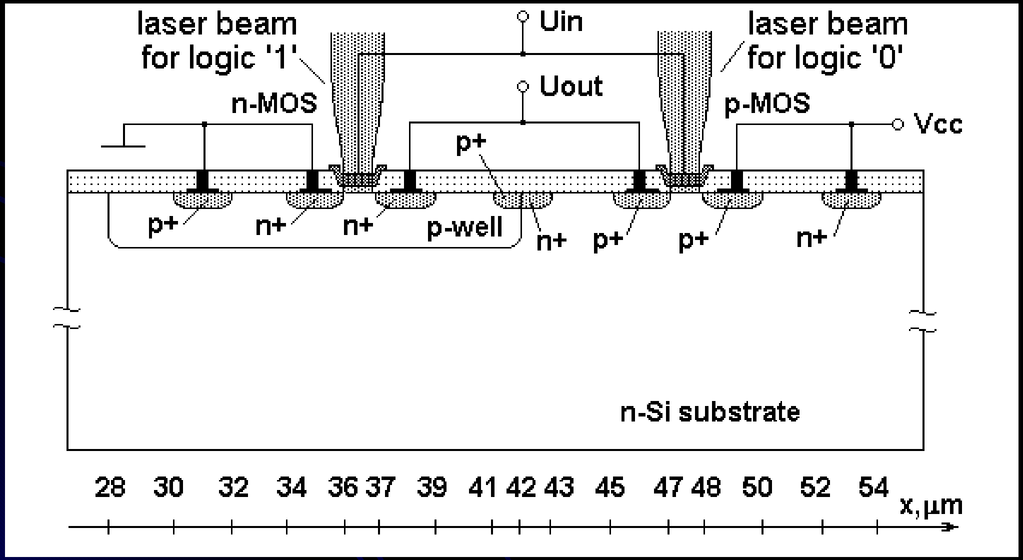
- Modelling of semi-invasive attacks
  - Detecting the logic state of CMOS transistors through photocurrent
    - Dependence on laser wavelength for p-MOS and n-MOS transistors in CMOS inverter

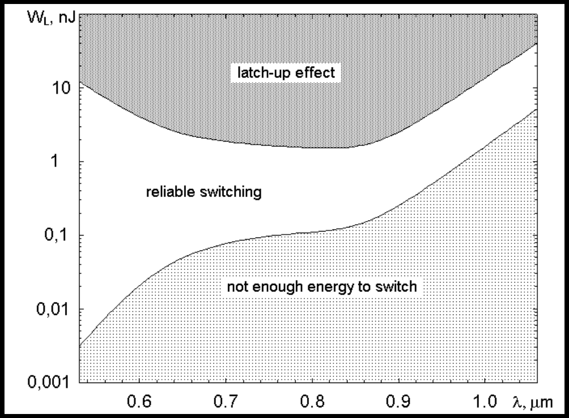


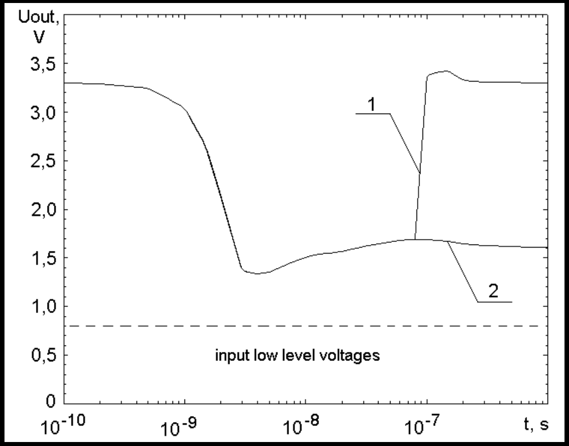


Hardware security analysis

- Modelling of semi-invasive attacks
  - Optical fault injection
  - For n-type substrates: switching is easier for p-MOS transistor
  - For p-type substrates: opposite result

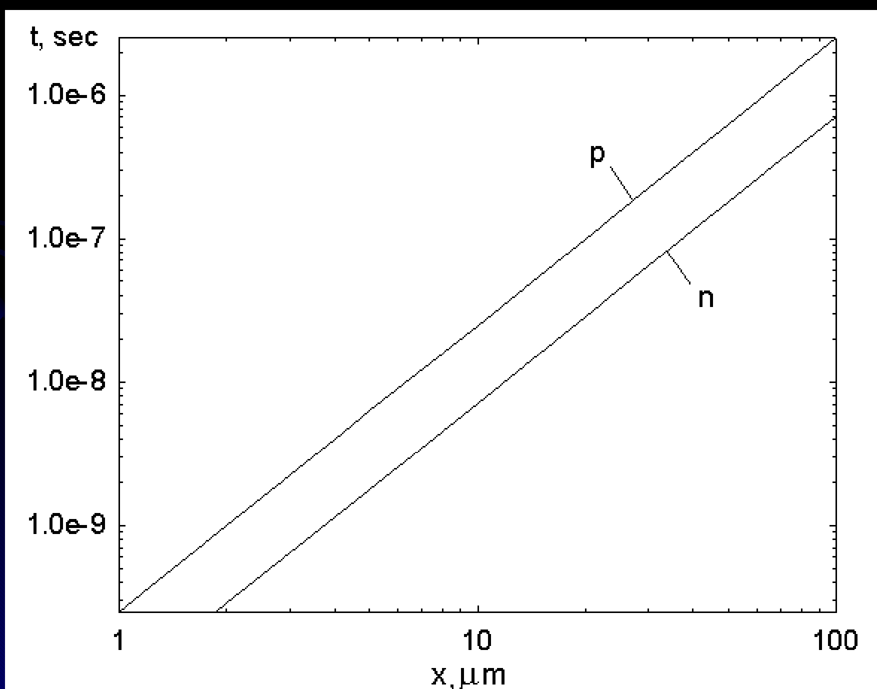


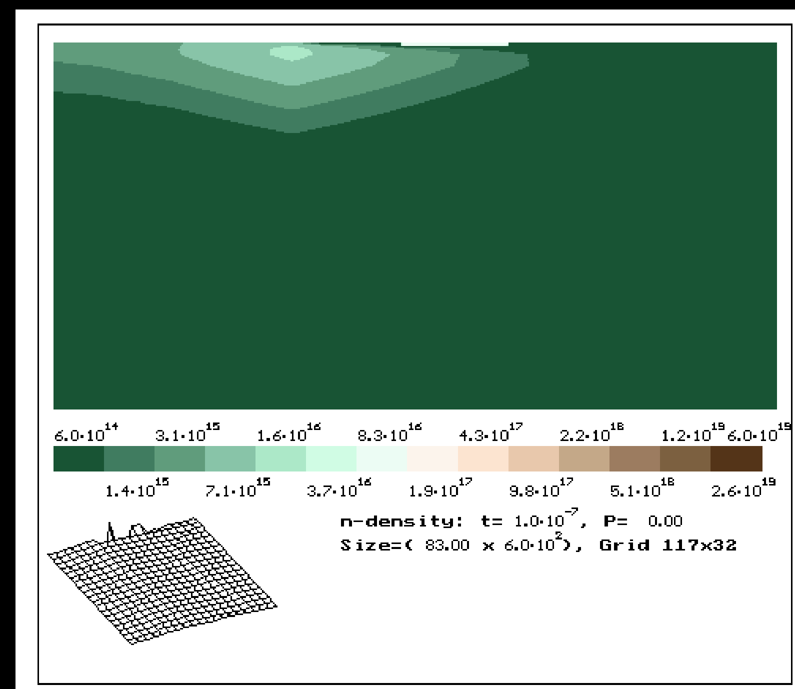




Hardware security analysis

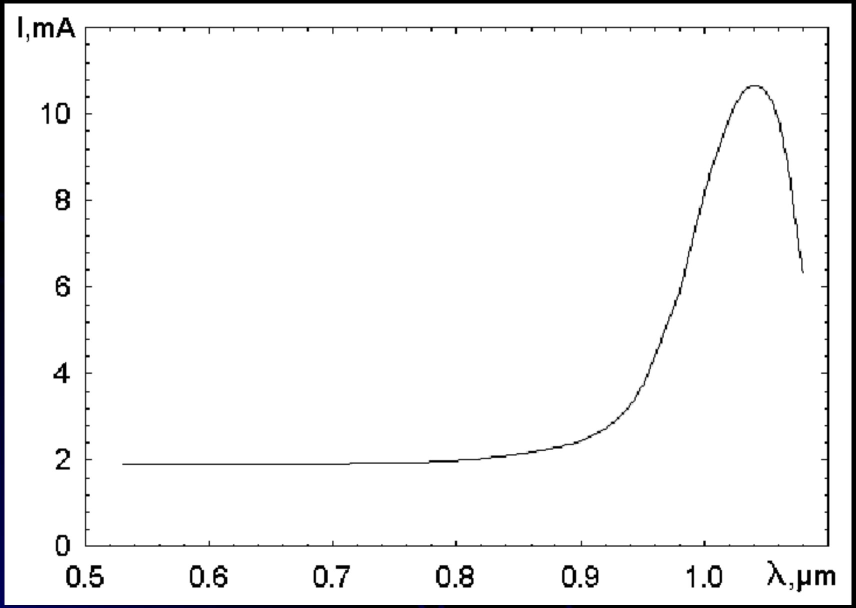
- Modelling of semi-invasive attacks
  - Signal distribution
  - Location dependence: $t = x^2/4D_{p(n)}$

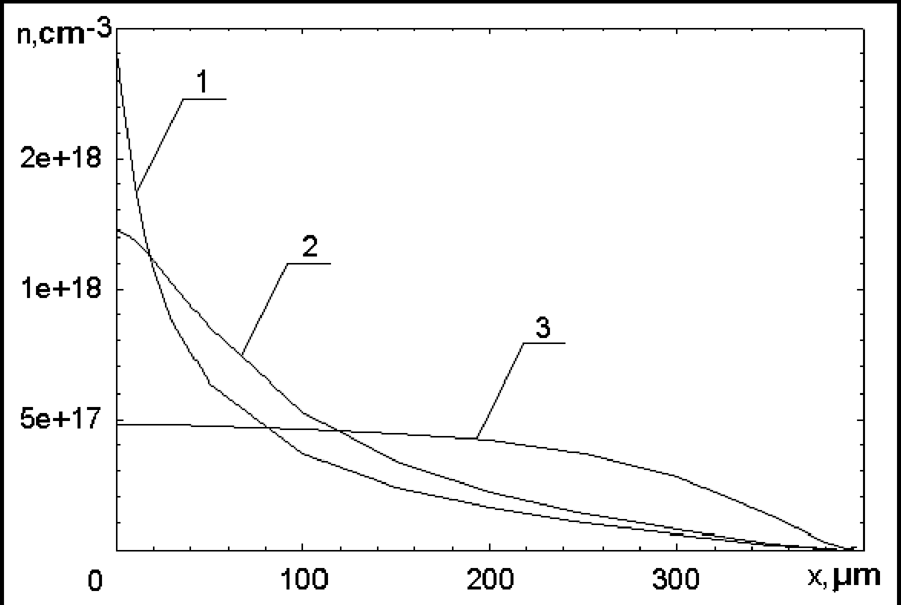




Hardware security analysis

- Modelling of backside semi-invasive attacks
  - Approaching from rear side (OBIC and current variation)
  - Sufficient ionization current for wavelengths less than 1000 nm

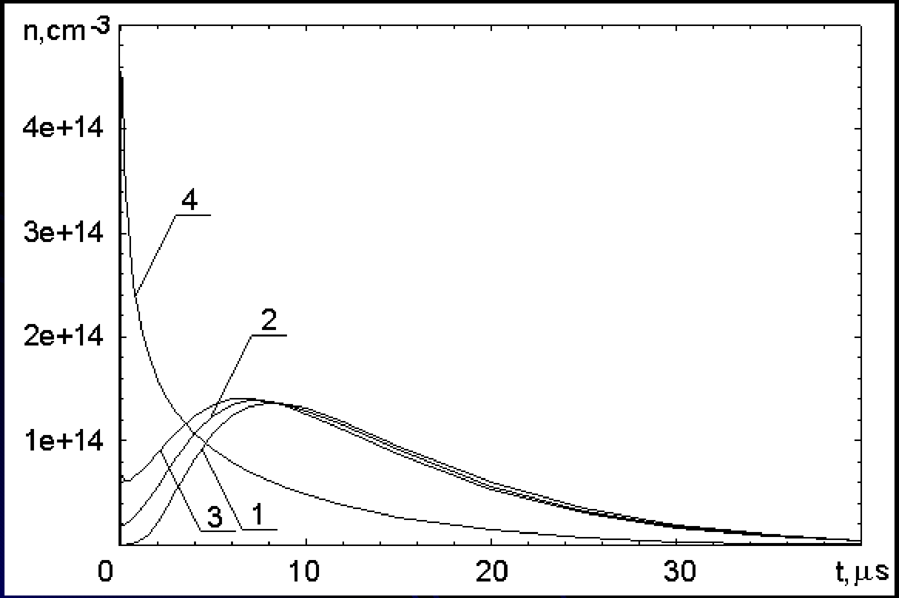




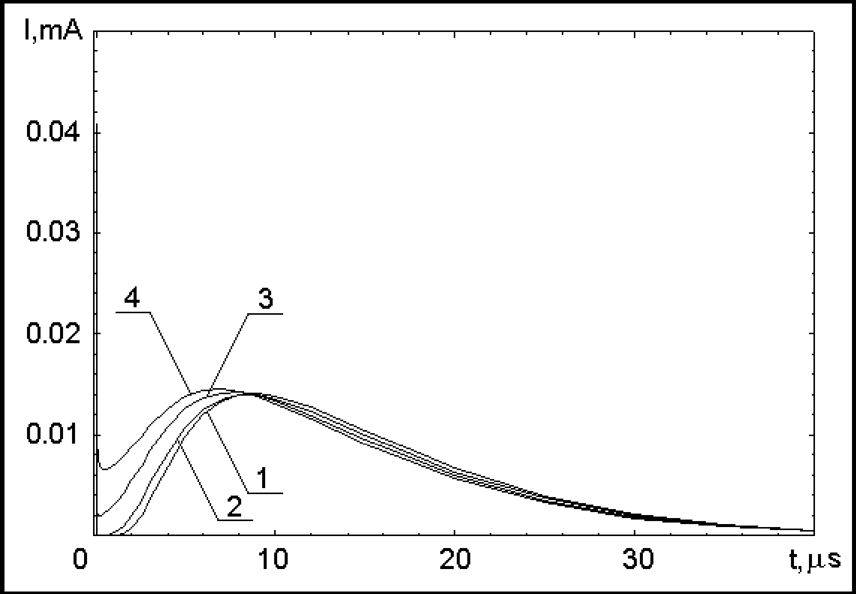
1. 530 nm 2. 900 nm 3. 1060 nm

Hardware security analysis

- Modelling of backside semi-invasive attacks
  - Fault injection from rear side
  - Delayed and smoothed response from shorter wavelengths



1. 900 nm 2. 950 nm 3. 970 nm 4. 1060 nm



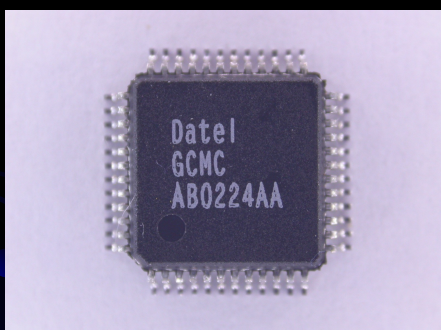
1. 530 nm 2. 900 nm 3. 950 nm 4. 970 nm

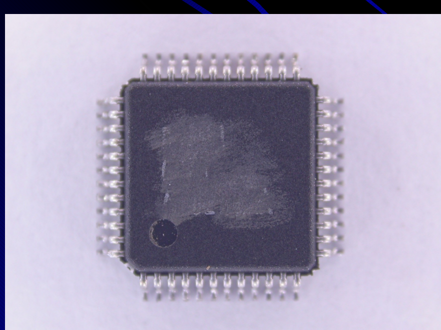
Conclusions

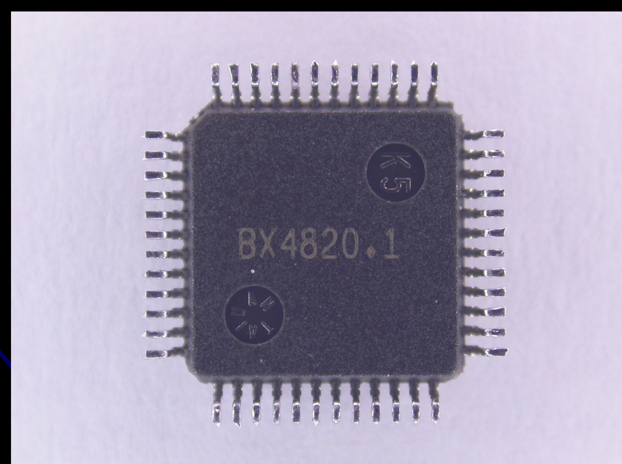
- Laser irradiation is a very effective tool for investigating IC properties and changing circuit states
- The effectiveness can be optimised through numerical simulation, using, for example, “DIODE-2D” software

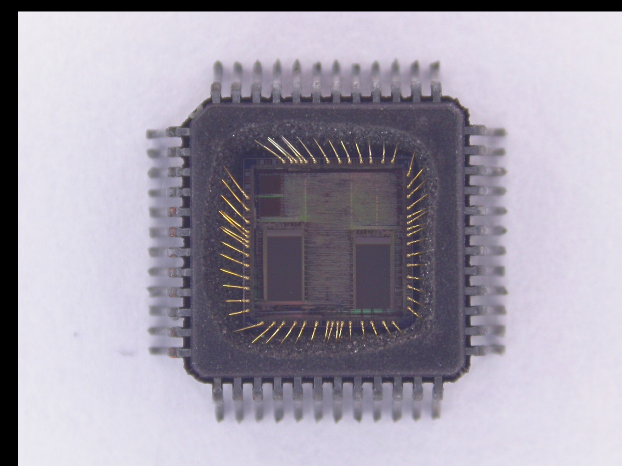
Defence technologies

- Low-cost solutions
  - Can be used to increase the protection from level ZERO or LOW to LOW or MODL
- Unmarking, remarking and repackaging
  - Available as option from chip manufacturers





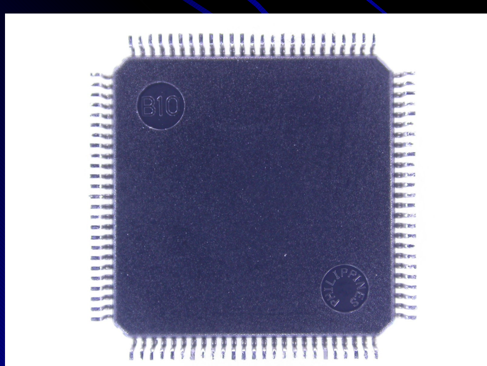


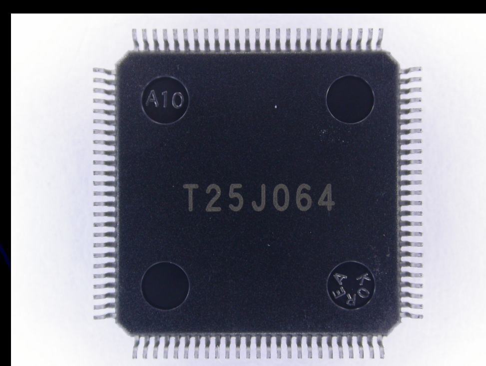


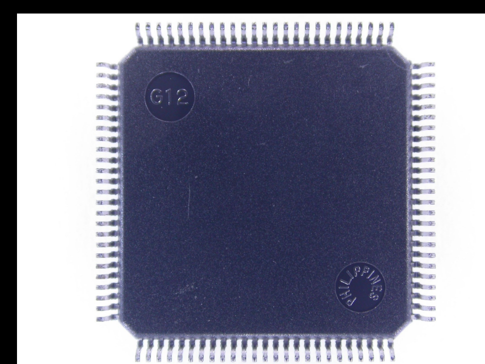
Scenix SX48 microcontroller

Defence technologies

- Low-cost solutions
  - Can be used to increase the protection from level ZERO or LOW to LOW or MODL
- Remarking to look like high-security product (MODL to MODH) – illegal as it violates trademark laws

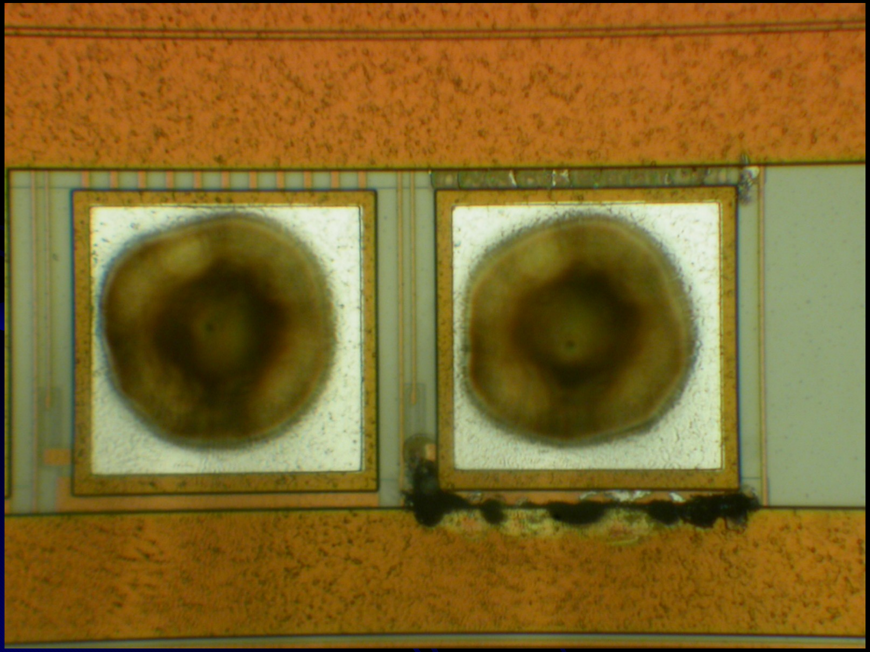




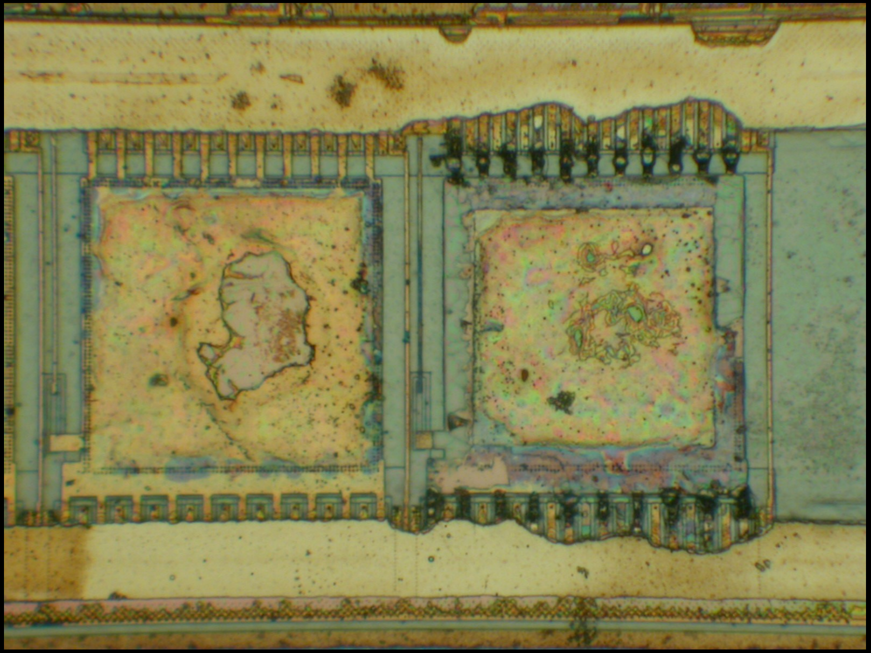


Defence technologies

- Low-cost solutions
  - Can be used to increase the protection from level LOW or MODL to MODL or MOD
- Destroying (burning) access and test circuit



Microchip PIC16F76 microcontroller

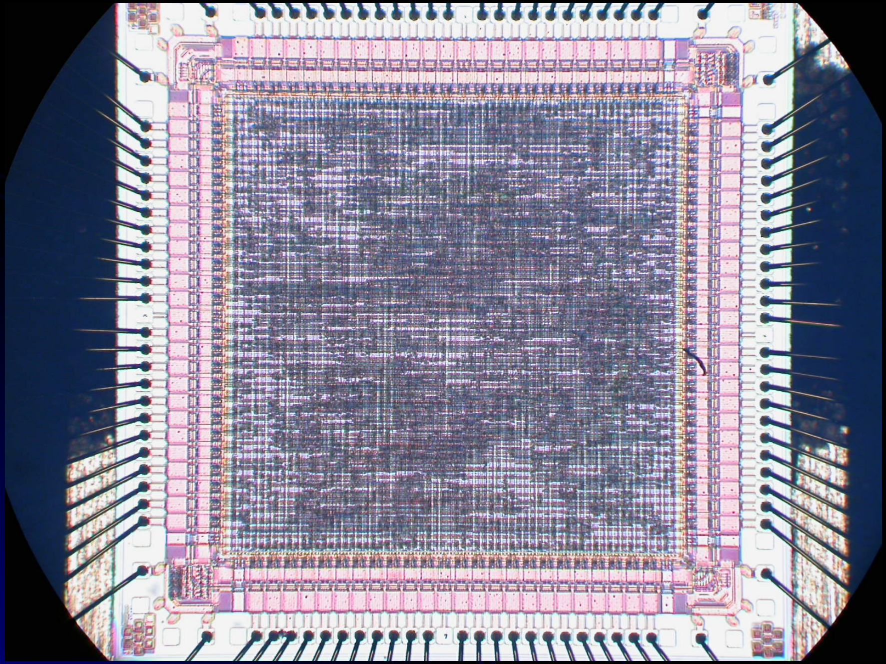


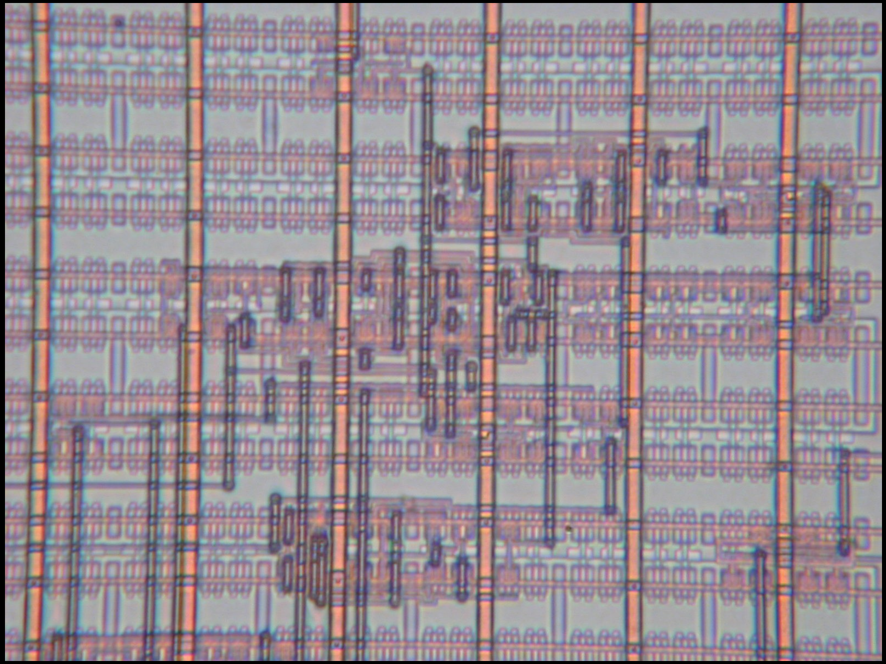
Defence technologies

- Smartcards and tamper protection
  - Glue logic design to make reverse engineering harder
  - Top metal protection and tamper sensors
  - Temperature, light, voltage and frequency monitoring
  - Bus encryption
  - Crypto-coprocessors

Defence technologies

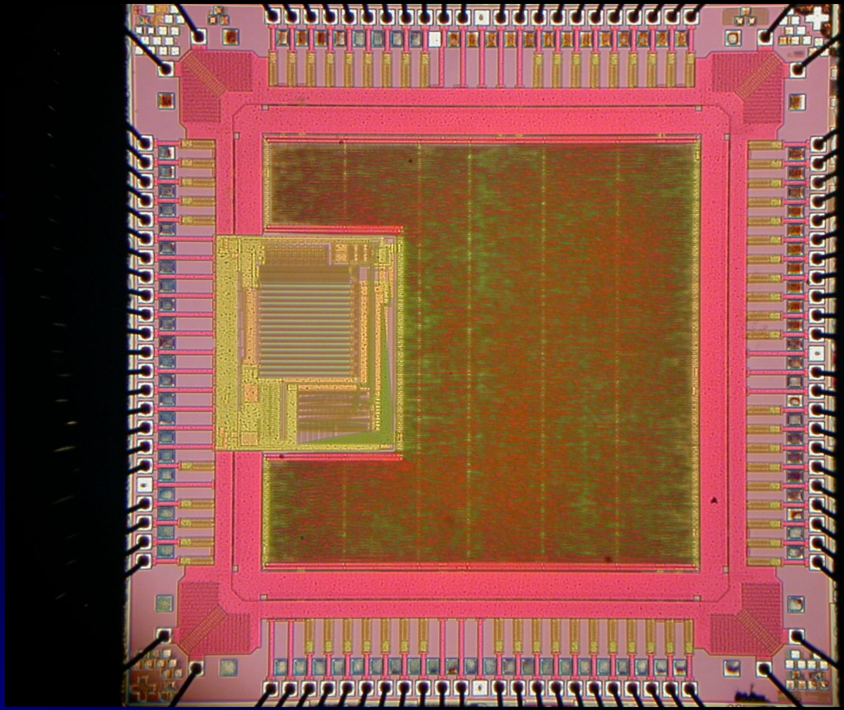
- ASICs and custom ICs
  - Types of ASIC design
    - Built from libraries using one or two factory programmable metal layers (very similar to Mask ROM fabrication)

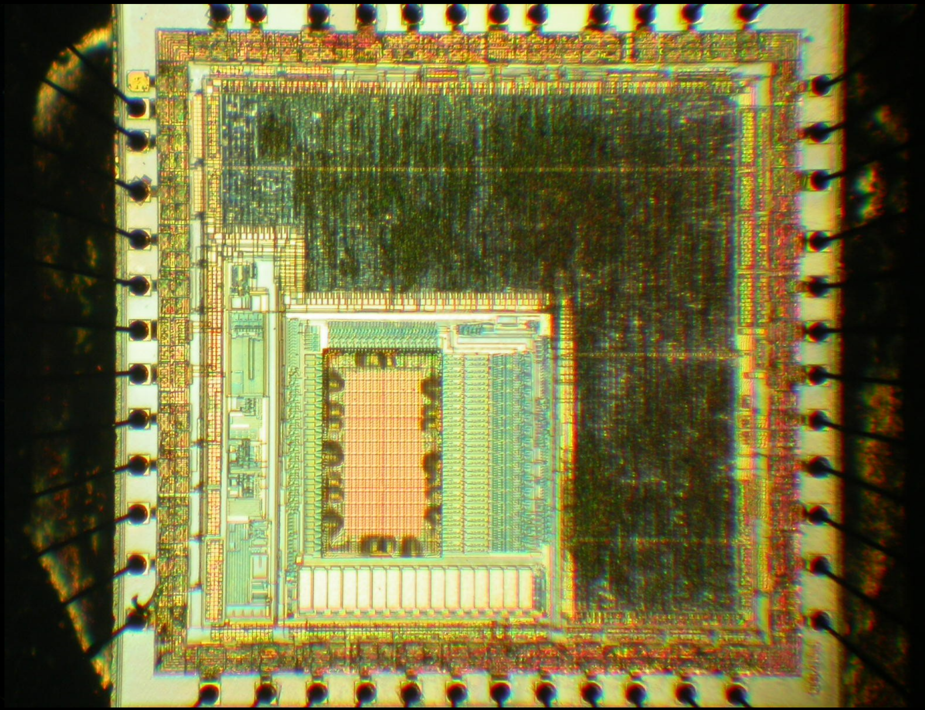




Defence technologies

- ASICs and custom ICs
  - Types of ASIC design
    - Glue logic design from VHDL or logic level (Netlist)
    - Fully custom design with security requirements





Defence technologies

- Silicon design level approach
  - Asynchronous logic circuits
    - Internal signals are not synchronised to external or internal clock – impossible to perform clock glitching attacks
    - Consumes less power making power analysis less efficient
    - Dual-rail logic has four states: 00=clear, 01=0, 10=1, 11=alarm
    - Dual-rail design uses ‘01’ and ‘10’ for low and high logic signals
      - power analysis less able to see number of set and reset data bits

Defence technologies

- Tamper protection enclosures
  - Give highest possible protection against invasive attacks
  - Not very compact, require constant battery power supply
  - High cost compared to silicon solution

Pictures courtesy of Dr Markus Kuhn

Defence from non-invasive attacks

- Countermeasures against data remanence
  - Cycle freshly manufactured EEPROM/Flash devices 10 – 100 times with new random data before writing sensitive information
  - Program all EEPROM/Flash cells before erasing them
    - Unable to successfully recover information from PIC16F84A if it was programmed to all 0's before the erase operation
    - This is standard procedure in some Flash and EEPROM devices (Intel ETOX Flash memory (P28F010), Microchip KeeLoq HCS200)
  - Remember about "intelligent" memories, backup and temporary files in file systems
  - Use latest high-density devices, as they benefit from technical improvements that make attacks less feasible
  - Cryptography can help to make data recovery more difficult. E.g. store longer pre-key R instead of key: $K = h(R)$
  - Test secure devices before using them in a real system

Defence from semi-invasive attacks

- Countermeasures against optical fault injection
  - Top metal protection layers
  - Highly doped silicon substrate to prevent rear side approach
  - Special non-transparent and hard-to-remove coatings
  - Active photon sensors
  - Special circuit design to reduce photonic influence

Conclusions

- There is no such a thing as absolute protection
  - Given enough time and resources any protection can be broken
- Technical progress helps a lot
  - Do not overestimate capabilities of the silicon circuits
  - Do not underestimate capabilities of the attackers
- Defence should be adequate to anticipated attacks
- Security hardware engineers must be familiar with attack technologies to develop adequate protection
- Attack technologies are constantly improving, so should the defence technologies