Hardware Security of Semiconductor Chips: Progress and Lessons

Dr Sergei Skorobogatov

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

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Introduction

- Attack scenarios on secure systems
  - theft of service – attacks on service providers: satellite TV, electronic meters, access cards, software protection dongles
  - access to information: information recovery and extraction, gaining trade secrets (IP piracy), ID theft
  - cloning and overbuilding: copying for making profit without investment in development, low-cost mass production by subcontractors
  - denial of service: dishonest competition, electronic warfare
- Attack technologies are being constantly improved
- There is growing demand for secure chips
- Who needs secure chips?
  - car industry, service providers, manufacturers of various devices
  - banking industry and military applications

Attack categories

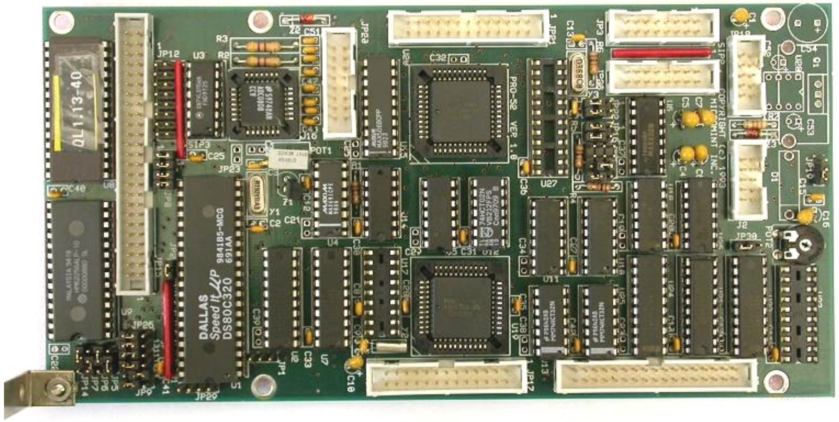
- **Side-channel attacks**
  - techniques that allow the attacker to monitor the analog characteristics of power supply and interface connections and any electromagnetic radiation
- Software attacks
  - use the normal communication interface and exploit security vulnerabilities found in the protocols, 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

Attack methods

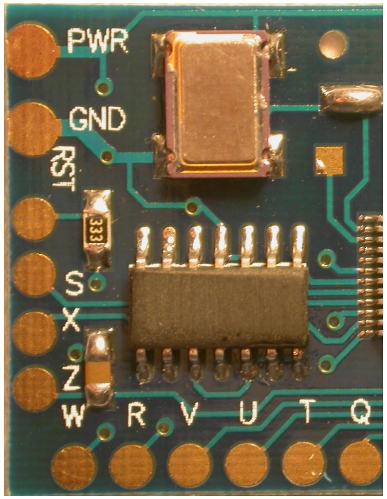
- Non-invasive attacks (low-cost)
  - observe or manipulate the device without physical harm to it
  - require only moderately sophisticated equipment and knowledge to implement
- Invasive attacks (expensive)
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - 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

Tamper protection levels

D.G.Abraham et al. (IBM), 1991

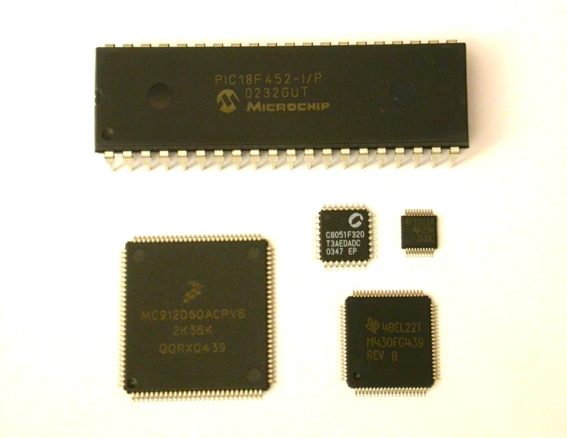


ZERO

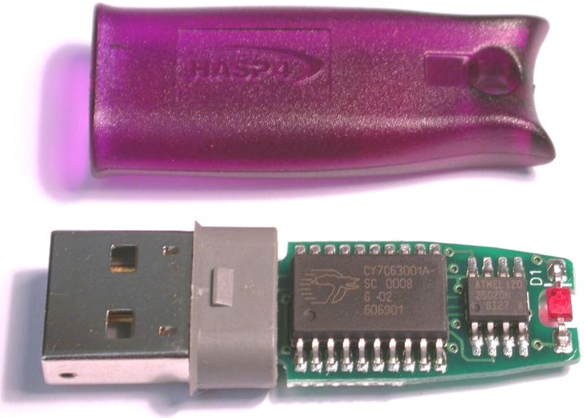


LOW

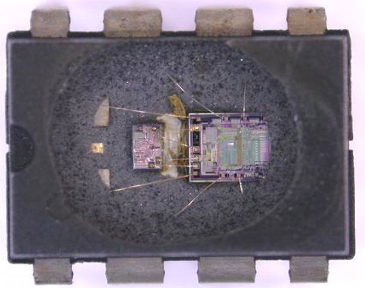
LOW



MODL



MODL

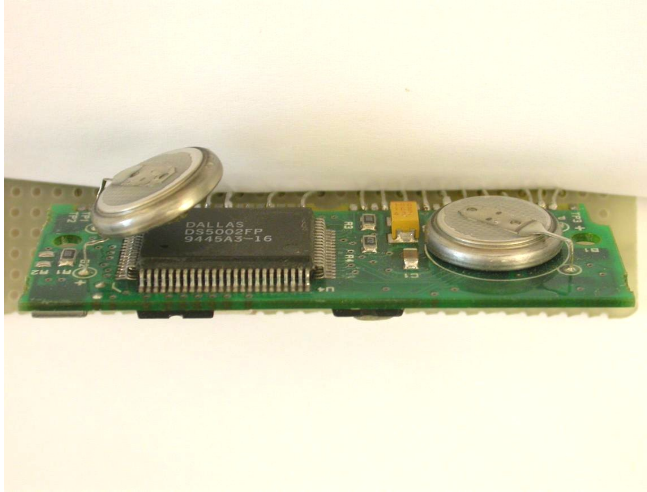


MODL

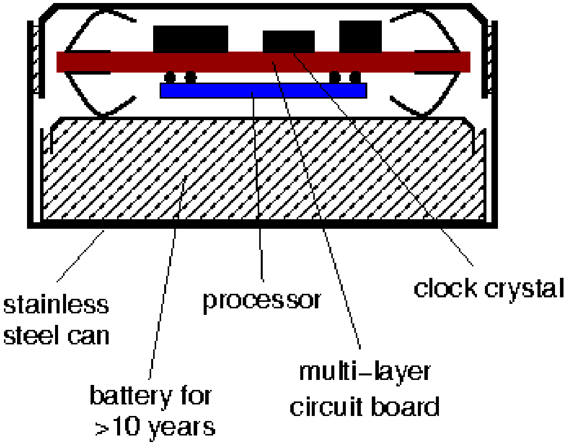
Tamper protection levels

MOD

MOD



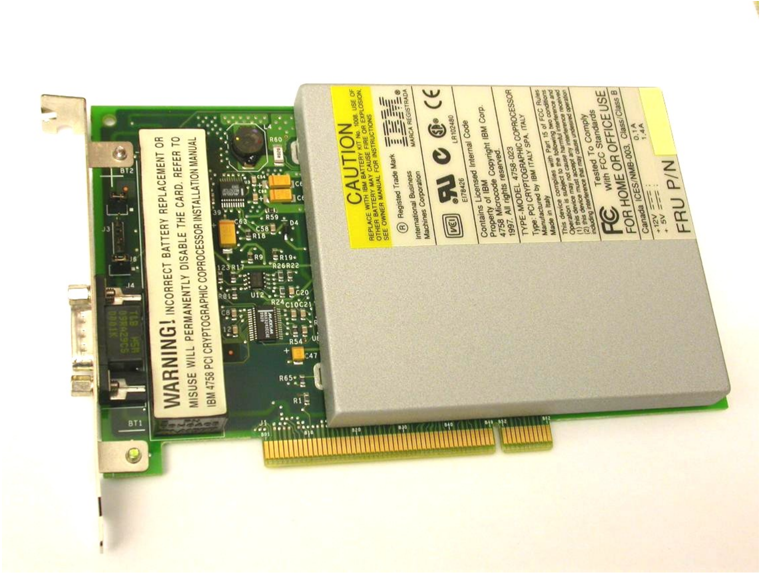
MOD



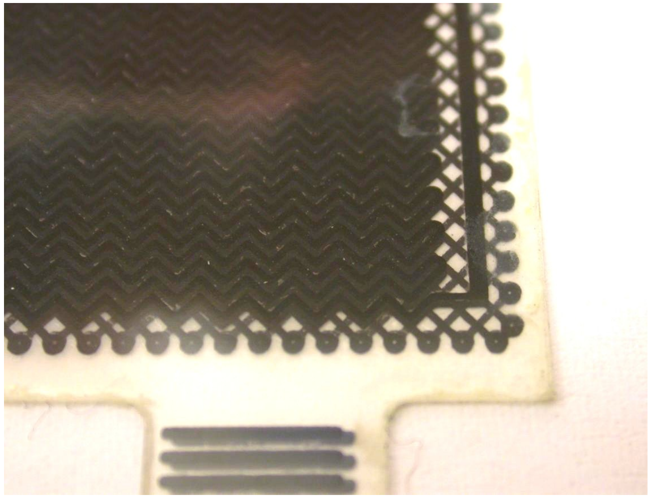
MODH

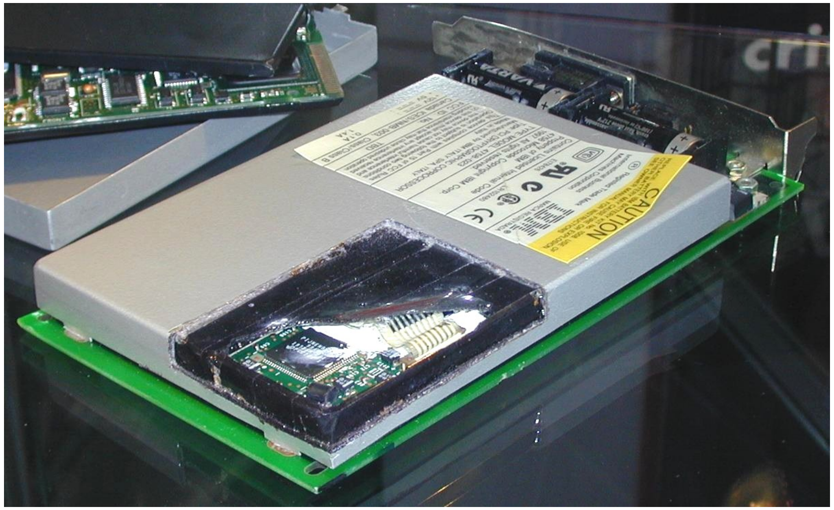
MODH

Tamper protection levels


WARNING! INCORRECT BATTERY REPLACEMENT OR
MISUSE WILL PERMANENTLY DISABLE THE CARD. REFER TO
IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR INSTALLATION MANUAL
CAUTION
IBM
FRU P/N

HIGH





Non-invasive attacks

- Non-penetrative to the attacked device: low-cost
  - observe and manipulate the device without physical harm to it
  - require only moderately sophisticated equipment and knowledge
  - normally do not leave tamper evidence of the attack
- Tools
  - IC soldering/desoldering station
  - digital multimeter, universal programmer and IC tester
  - power supplies, oscilloscope, logic analyser, signal generator
  - PC with data acquisition board, FPGA board, prototyping boards
- Types of non-invasive attacks: passive and active
  - side-channel attacks: timing, power and emission analysis
  - fault injection: glitching, bumping
  - data remanence
  - brute forcing

Invasive attacks

- Penetrative attacks: expensive to perform
  - require expensive equipment, knowledgeable attackers and time
  - almost unlimited capabilities to extract information from chips and understand their functionality
  - leave tamper evidence of the attack or even destroy the device
- Tools
  - IC soldering/desoldering station
  - simple chemical lab and high-resolution optical microscope
  - wire bonding machine, laser cutting system, microprobing station
  - oscilloscope, logic analyser, signal generator
  - scanning electron microscope and focused ion beam workstation
- Types of invasive attacks: passive and active
  - decapsulation, optical imaging, reverse engineering
  - microprobing and internal fault injection
  - chip modification

Semi-invasive attacks

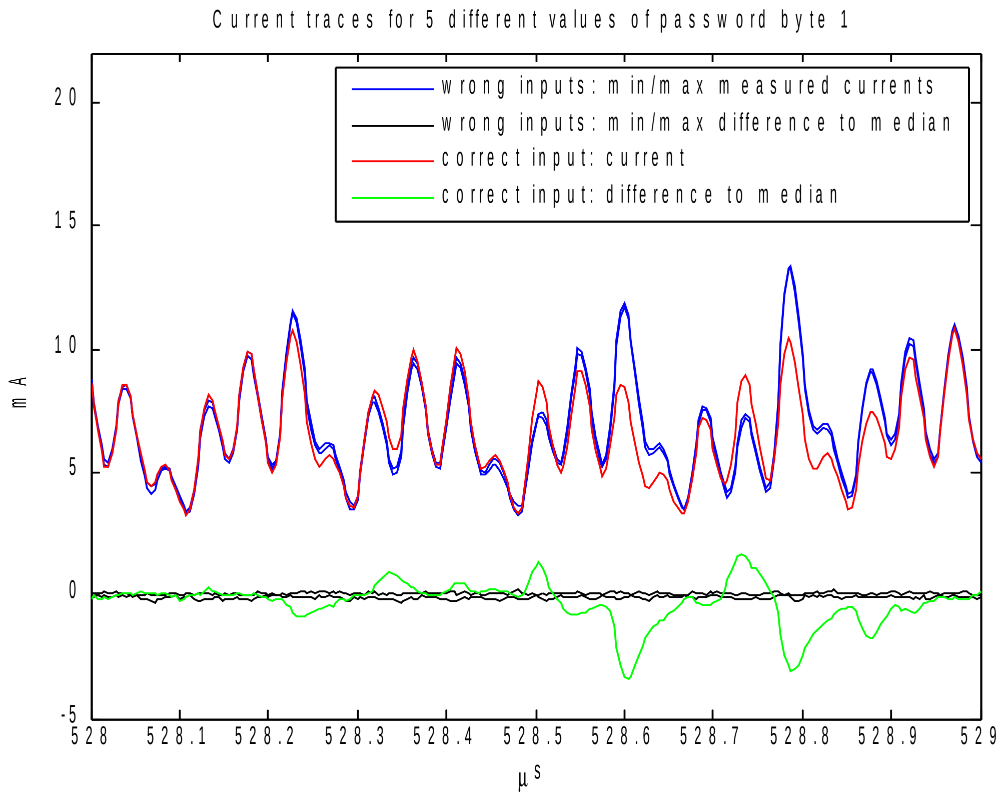
- Fill the gap between non-invasive and invasive attacks
  - less damaging to target device (decapsulation without penetration)
  - less expensive and easier to setup and repeat than invasive attacks
- Tools
  - IC soldering/desoldering station
  - simple chemical lab and high-resolution optical microscope
  - UV light sources, lasers and special microscopes (laser scan, IR)
  - oscilloscope, logic analyser, signal generator
  - PC with data acquisition board, FPGA board, prototyping boards
- Types of semi-invasive attacks: passive and active
  - imaging: optical and laser techniques
  - fault injection: UV attack, photon injection, local heating, masking
  - side-channel attacks: optical emission analysis, induced leakage

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
  - some knowledge in electrical engineering and signal processing
  - 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

Non-invasive attacks: power analysis

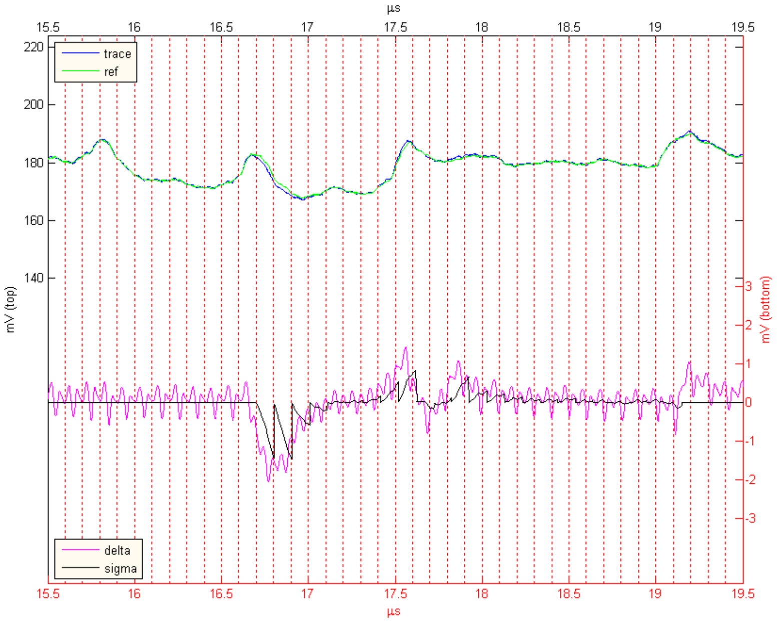
- Simple power analysis (SPA): difference in instruction flow
  - 8-byte password check in Freescale MC908AZ60A microcontroller
  - 1 byte at a time, 1 of 256 attempts leads to distinctive power trace
  - full password recovery in 2048 attempts (less than 10 minutes)

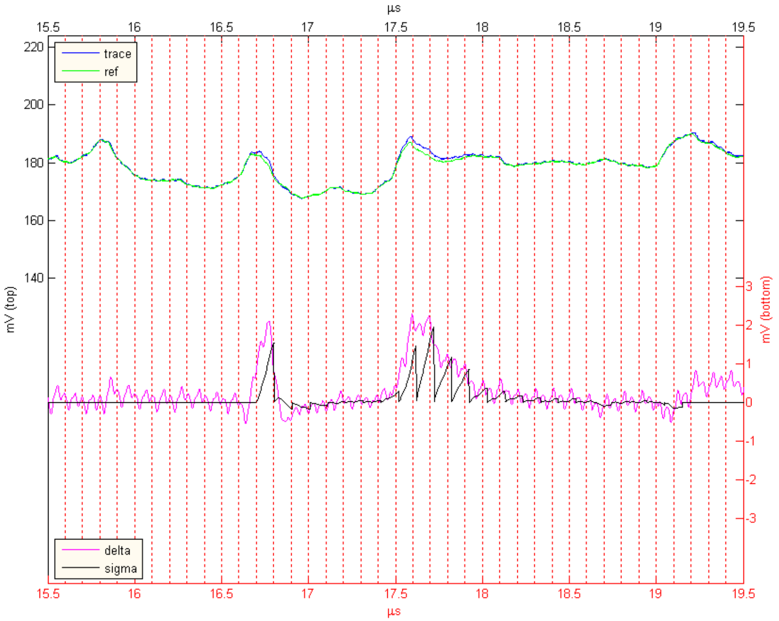


```
loop:   CBEQX #$FE, ptr3   ;check for end
        JSR sub_recv       ;receive byte
        CBEQ X+, ptr2      ;compare byte
        CLR adr_50         ;clear status
ptr1:   BRA loop           ;loop
ptr2:   BRA ptr1           ;time alignment
ptr3:   LDX #$FF           ;set address
        LDA adr_50         ;check status
        BEQ cont           ;skip flash enable
        STX , X            ;flash enable
cont:   … … …
```

Non-invasive attacks: power analysis

- Differential power analysis (DPA): correlation with secret
  - AES decryption in asynchronous ASIC (130 nm, 1.5V), 128-bit key
  - first round of decryption starts with XORing the input data with round key, the difference is only in the input data and the result
  - full key recovery in 256 attempts with each attempt requiring average of 4096 traces (~2 minutes per attempt, total 8 hours)



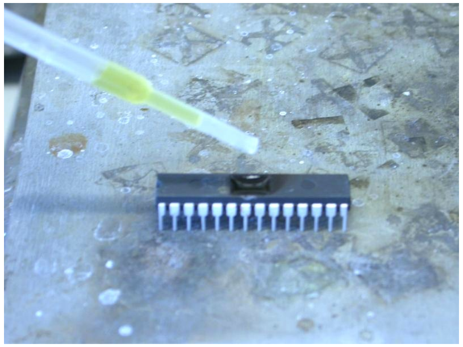
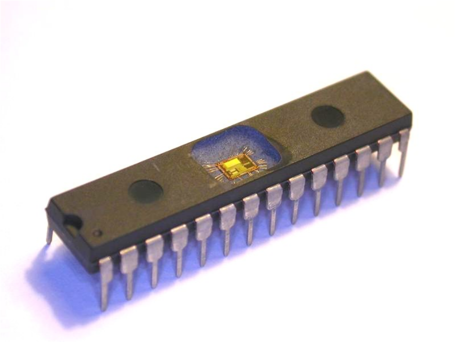
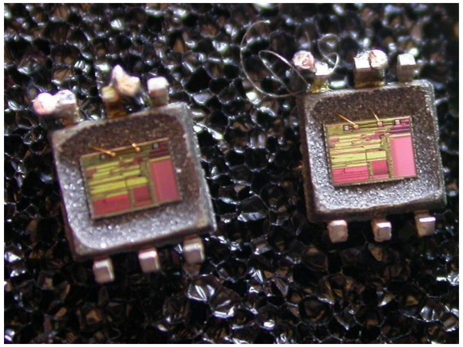
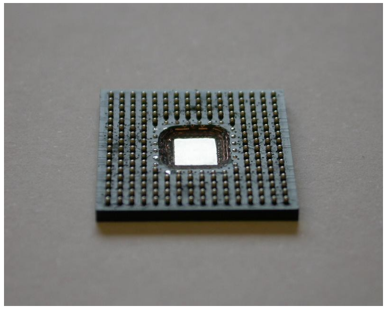
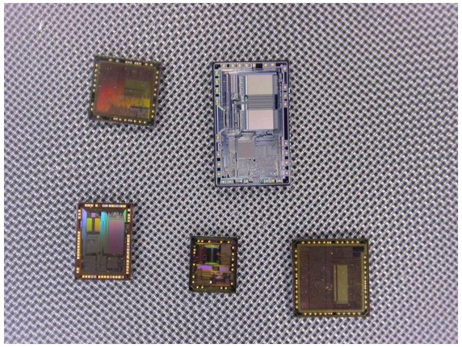
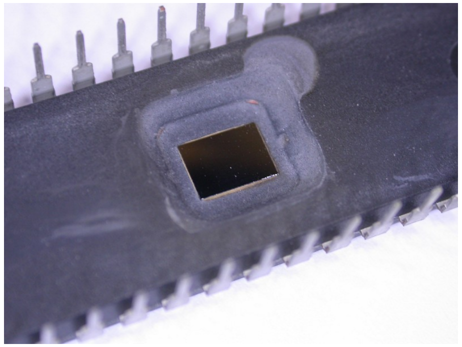
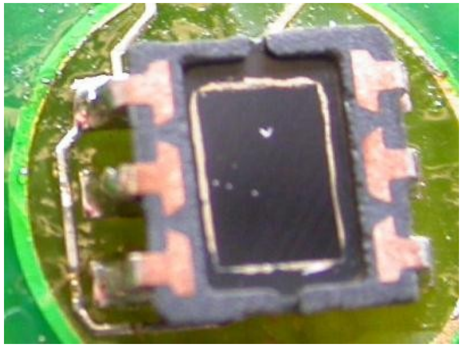


Non-invasive attacks: fault injection

- Glitch attacks
  - clock glitches
  - power supply glitches
  - corrupting data
- Security fuse verification in the Mask ROM bootloader of the Motorola MC68HC05B6 microcontroller
  - double frequency clock glitch causes incorrect instruction fetch
  - low-voltage power glitch results in corrupted EEPROM data read
- Today: glitch attacks became harder to exploit
  - effective countermeasures are in place: clock and supply monitors
  - internal clock sources, clock conditioning and PLL circuits
  - internal charge pumps and voltage regulators
  - checksums (CRC, SHA-1) and encryption
  - asynchronous design

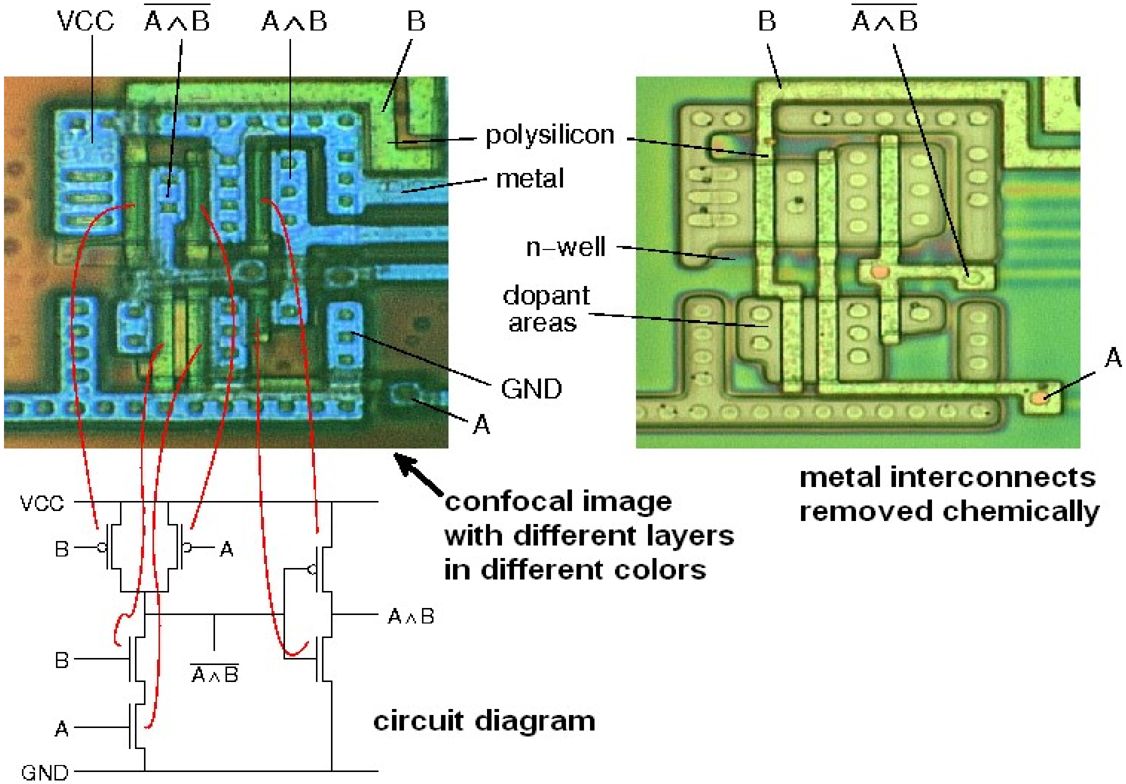
Invasive attacks: sample preparation

- Decapsulation
  - manual with fuming nitric acid (HNO_3) and acetone at 60ºC
  - automatic using mixture of HNO_3 and H_2SO_4
  - partial or full
  - from front side and from rear side (just mechanical milling)
- Challenging process for small and BGA packages

Invasive attacks: reverse engineering

- Reverse engineering – understanding the structure of a semiconductor device and its functions
  - optical, using a confocal microscope (for >0.5μm chips)
  - deprocessing is necessary for chips with smaller technology
  - very challenging task for modern chips with millions of gates



confocal image with different layers in different colors

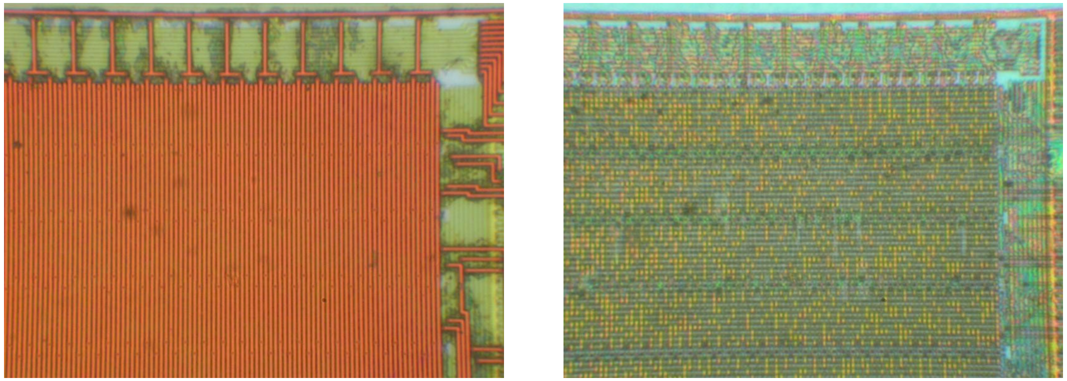
metal interconnects removed chemically

circuit diagram

Picture courtesy of Dr Markus Kuhn

Invasive attacks: reverse engineering

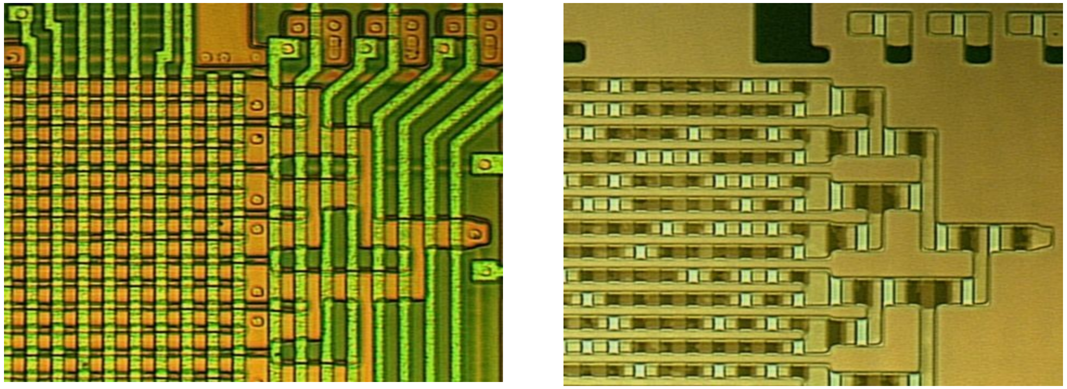
- Memory extraction from Mask ROMs
  - removing top metal layers for direct optical observation of data in NOR ROMs (bits programmed by presence of transistors)
  - for VTROM (ion implanted) used in many smartcards selective (dash) etchants are required to expose the ROM bits



NEC µPD78F9116

microcontroller

0.35 µm



Motorola MC68HC05SC27

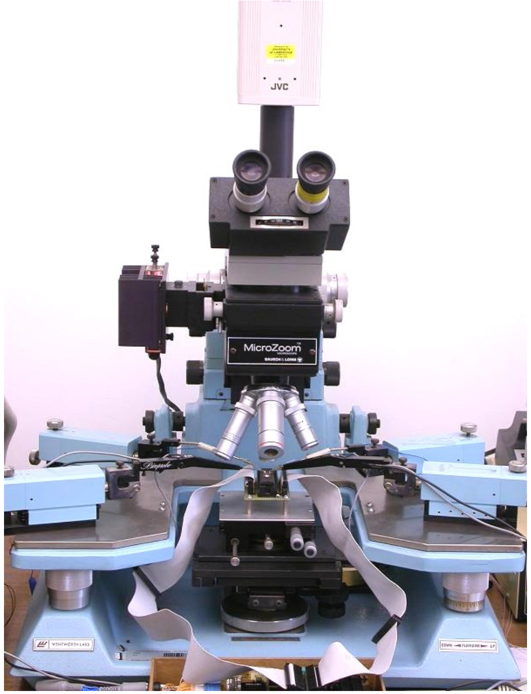
smartcard

1.0 µm

Picture courtesy of Dr Markus Kuhn

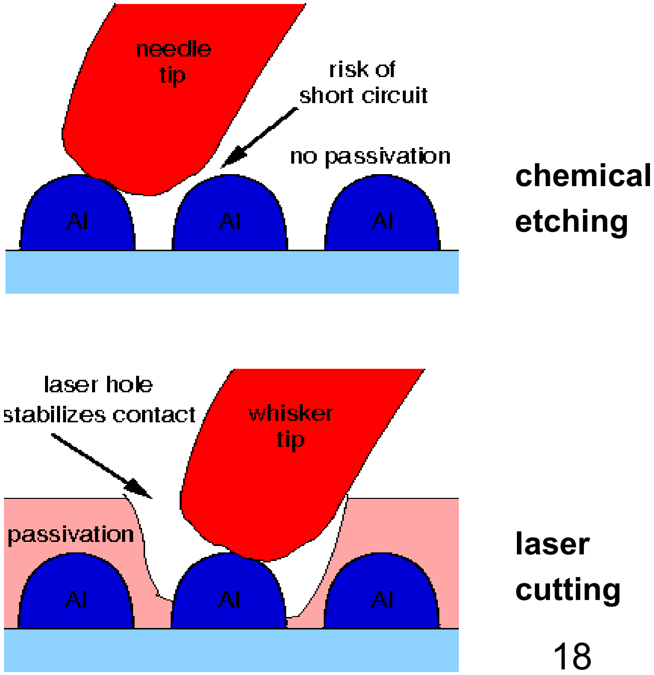
Invasive attacks: microprobing

- 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
  - laser cutter can be used to remove passivation and cut metal wires
  - limited use for 0.35µm and smaller chips



probing station

laser cutter

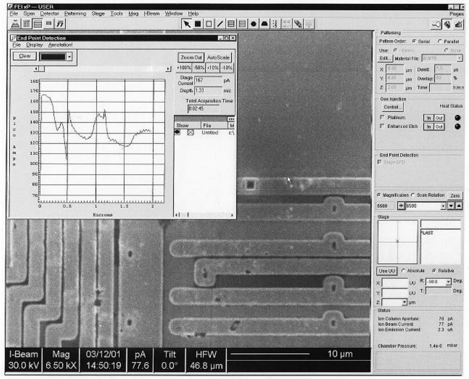


Picture courtesy of Dr Markus Kuhn

Invasive attacks: chip modification

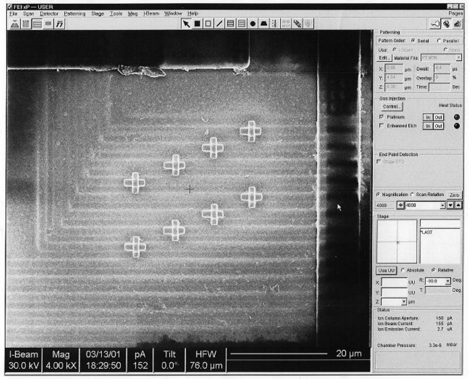
- Focused Ion Beam (FIB) workstation
  - chip-level surgery with 10 nm precision
  - etching with high aspect ratio
  - platinum and SiO_2 deposition

Picture courtesy of Semiresearch Ltd


FEI xP — USER
File Scan Detector Patterning Stage Tools Mag I-Beam Window Help
End Point Detection
Patterning
Status

I-Beam	Mag	03/12/01	pA	Tilt	HFW	10 µm
30.0 kV	6.50 kX	14:50:19	77.6	0.0°	46.8 µm	

etching passivation and metal

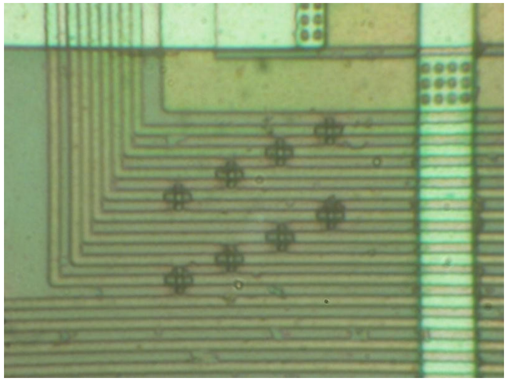

FEI xP — USER
File Scan Detector Patterning Stage Tools Mag I-Beam Window Help
Patterning
Status

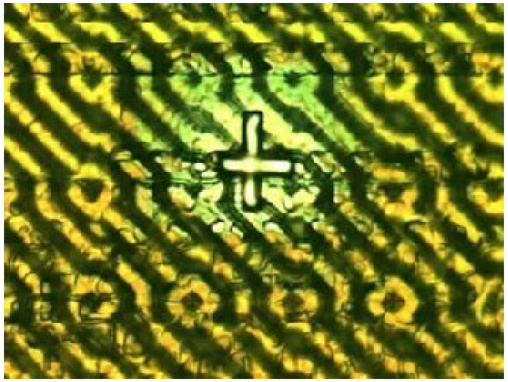
I-Beam	Mag	03/13/01	pA	Tilt	HFW	20 µm
30.0 kV	4.00 kX	18:29:50	152	0.0°	76.0 µm	

deposit platinum

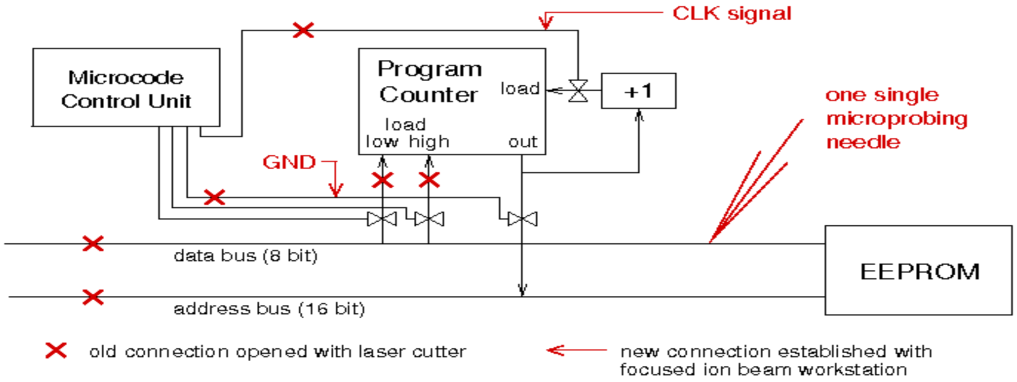
Invasive attacks: chip modification

- Today: Focused Ion Beam workstation
  - chip-level surgery with 10nm precision
  - create probing points inside smartcard chips, read the memory
  - modern FIBs allow backside access, but require special chip preparation techniques to reduce the thickness of silicon





Picture: Oliver Kömmerling

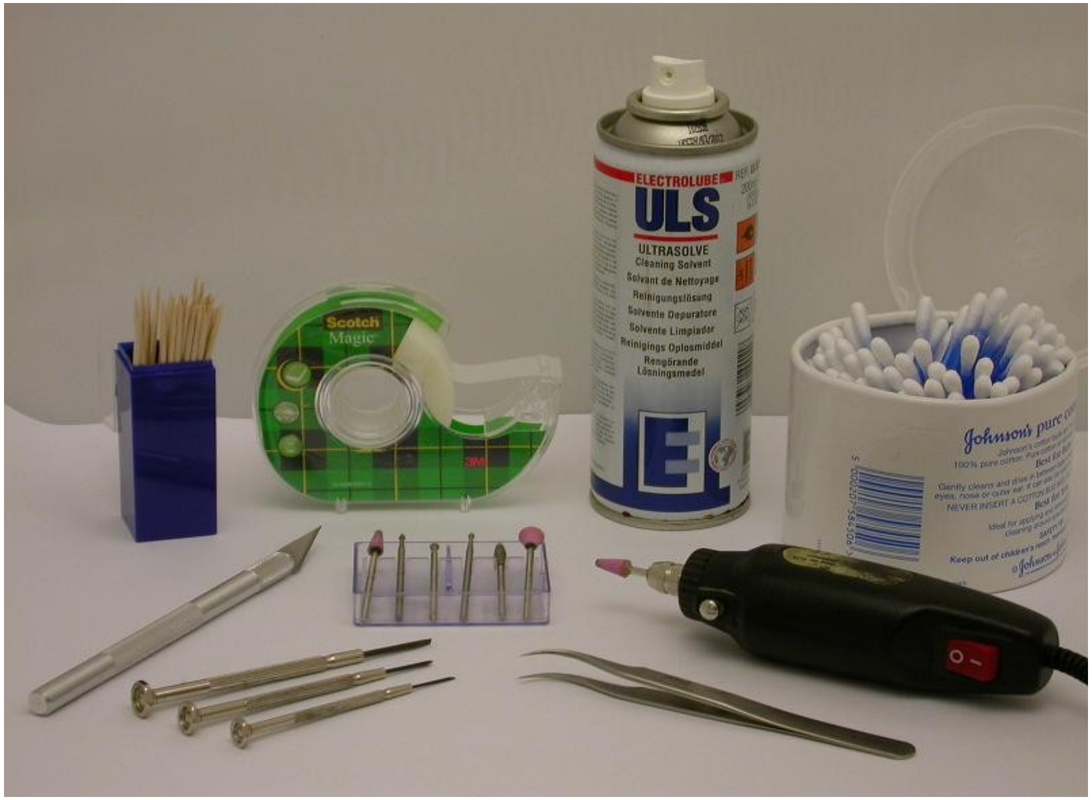


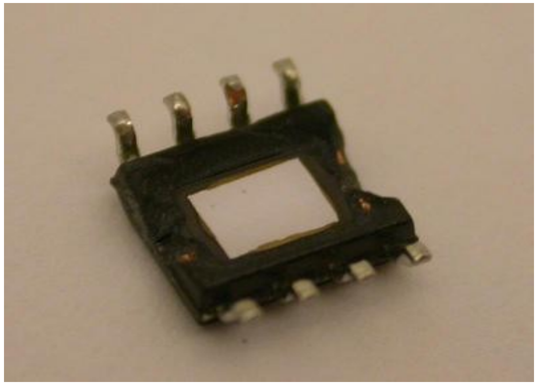
CLK signal
Microcode Control Unit
Program Counter
load
+1
load
low high
out
GND
one single microprobing needle
data bus (8 bit)
address bus (16 bit)
EEPROM
old connection opened with laser cutter
new connection established with focused ion beam workstation

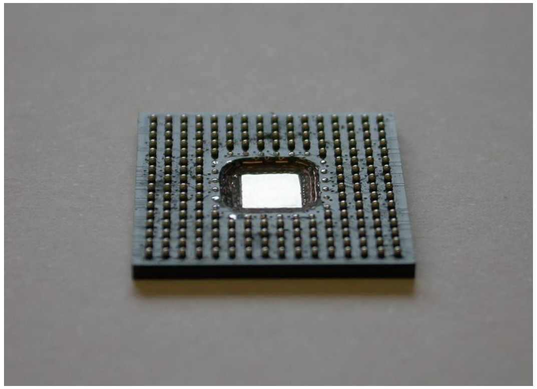
Picture courtesy of Dr Markus Kuhn

Semi-invasive attacks: 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

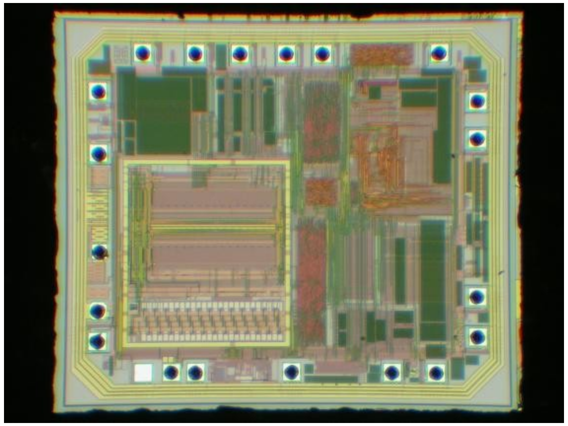


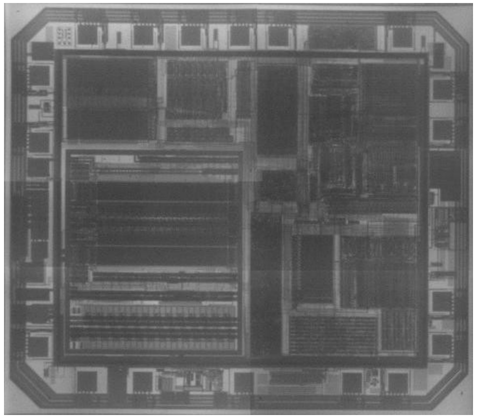




Semi-invasive attacks: imaging

- Backside infrared imaging using IR-sensitive cameras
  - Mask ROM extraction without chemical etching
- Main option for 0.35μm and smaller chips
  - multiple metal wires do not block the optical path

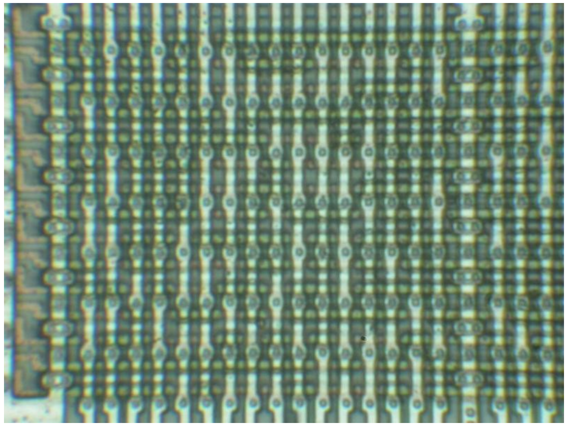


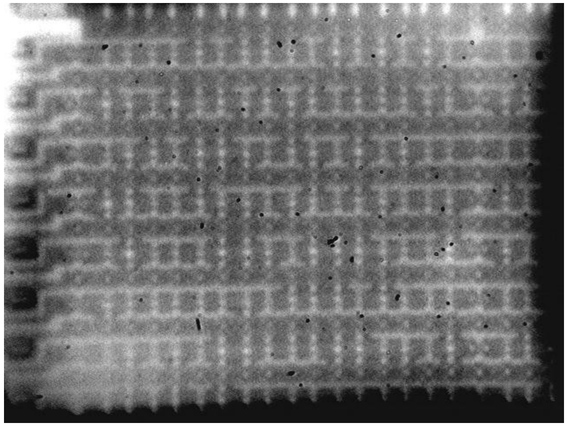


Texas Instruments MSP430F112

microcontroller

0.35 μm





Mask ROM in

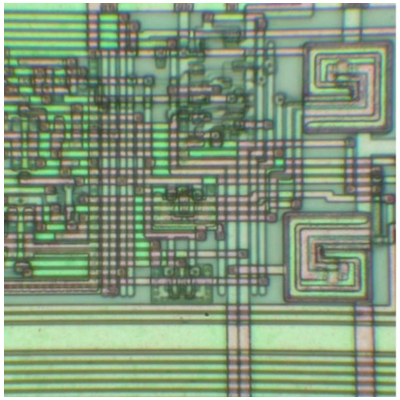
Motorola MC68HC705P6A

microcontroller

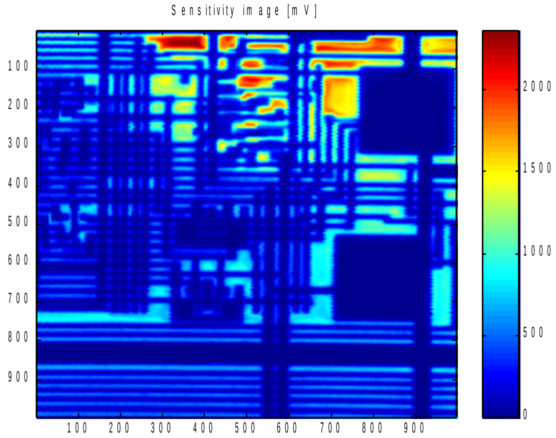
1.2 μm

Semi-invasive attacks: laser imaging

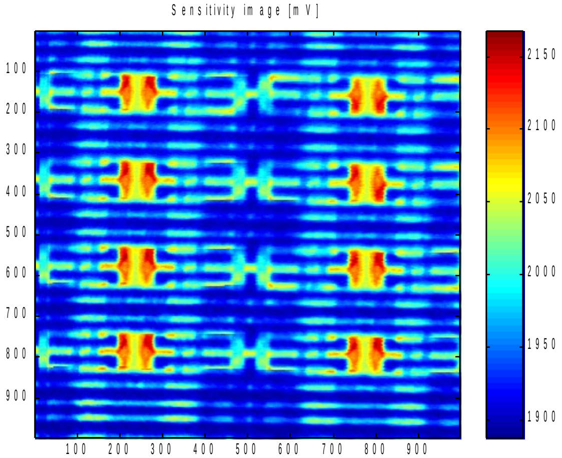
- OBIC imaging techniques – active photon probing
  - photons ionize IC’s regions, which results in a photocurrent flow
  - used for localisation of active areas
- LIVA imaging – active photon probing on powered up chip
  - photon-induced photocurrent is dependable on the transistor state
  - reading logic state of CMOS transistors inside a powered-up chip
- Requires backside approach for 0.35µm and smaller chips
  - multiple metal wires do not block the optical path



optical image of fuse



OBIC laser image of fuse

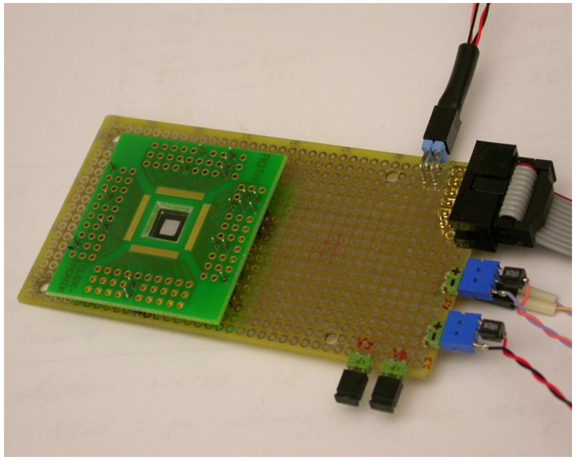


LIVA laser image of SRAM

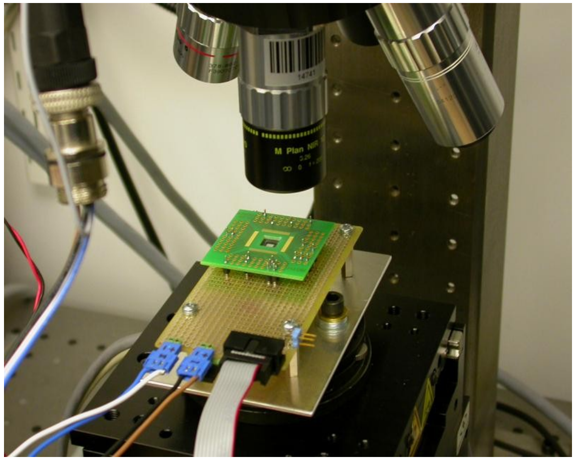
Microchip PIC16F84A microcontroller

Semi-invasive attacks: fault injection

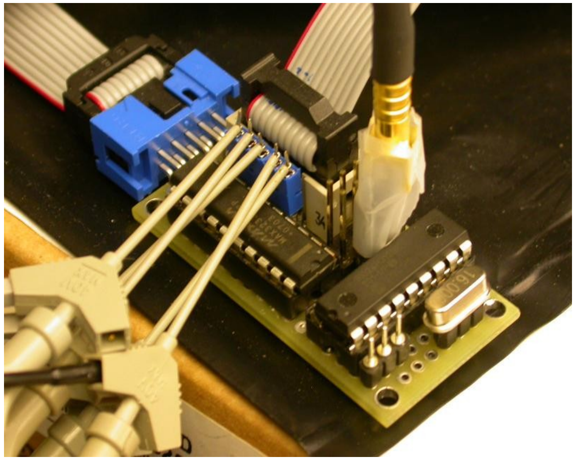
- Optical fault injection attack
  - using laser attached to microscope to inject fault into chip operation
  - chip is decapsulated and placed on a test board under microscope
  - red laser (635nm) for front approach and IR (1065nm) for backside
  - control board is used to operate the chip and trigger the laser pulse
- Tested on chips down to 90nm and proved its effectiveness
  - requires backside approach for modern chips due to metal layers
  - cannot be scaled down to individual transistor, but still effective



test board



test setup

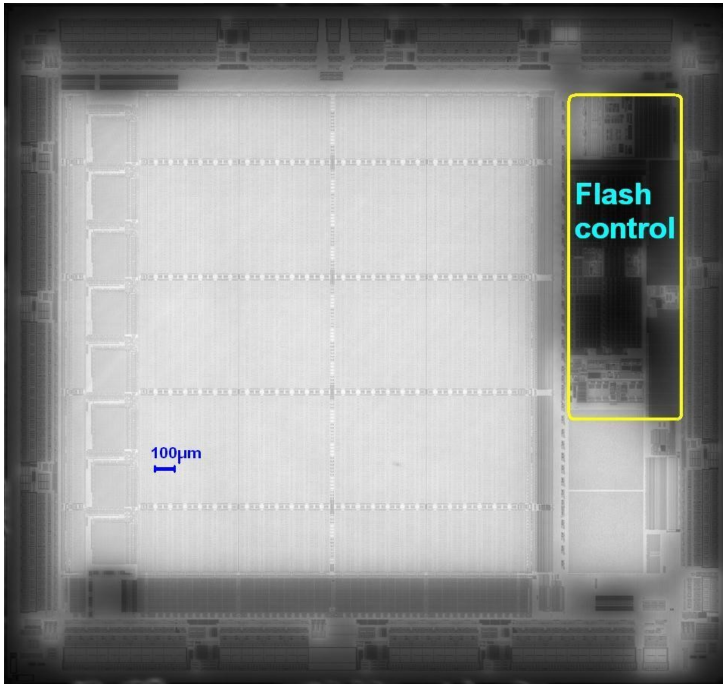


control board

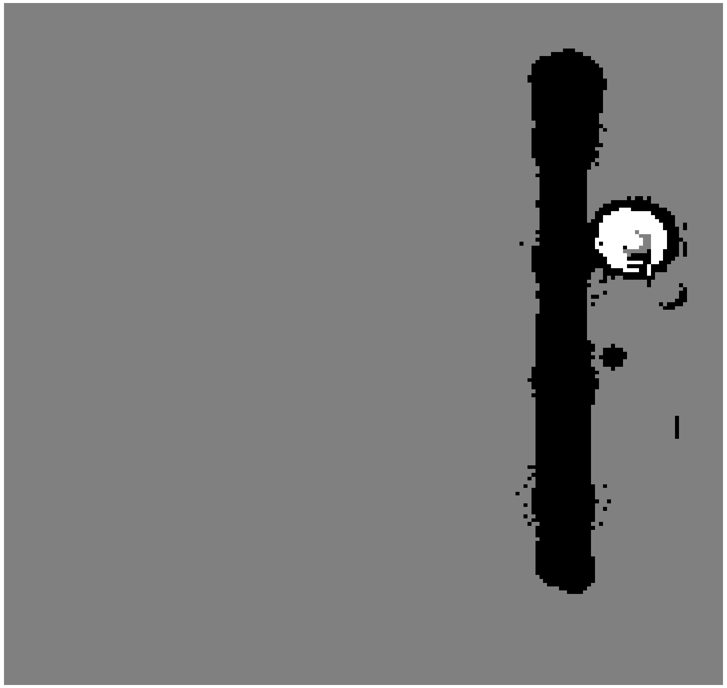
Semi-invasive attacks: fault injection

- Actel secure FPGA (A3P250, 130nm) with JTAG interface
  - possibility of attack proposed in 2002 and demonstrated in 2010
- Locating Flash and active areas is easy via laser scanning
- Sensitive locations were found with exhaustive search

  20µm grid: black – data corrupted, white – matching predicted data



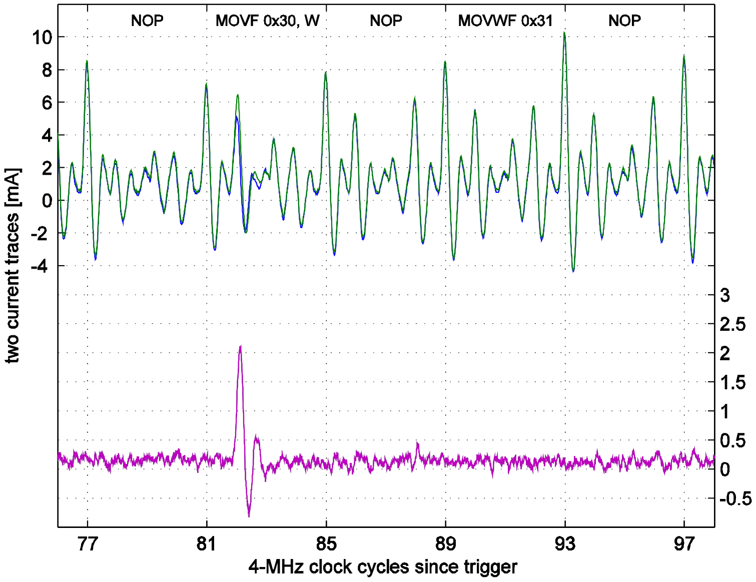
backside laser scanning image



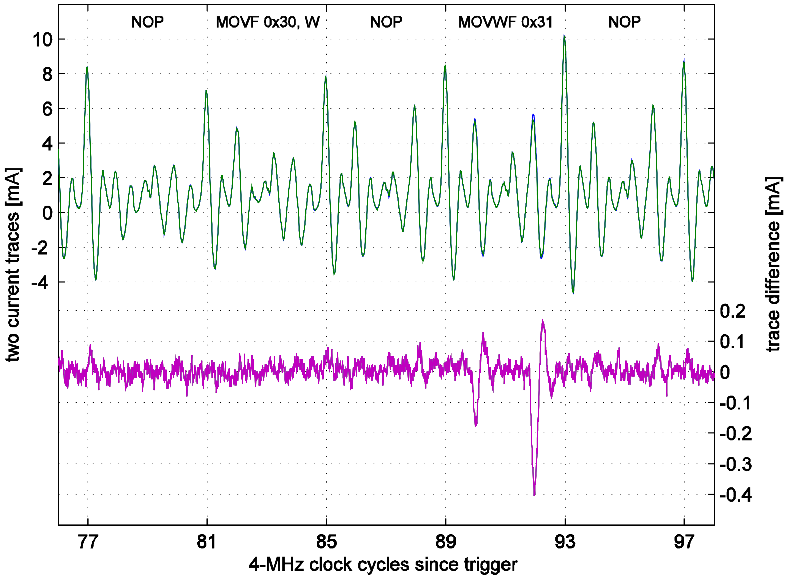
fault injection sensitive locations

Semi-invasive attacks: side-channel

- Optically enhanced position-locked power analysis
  - combining power analysis setup with laser microscope setup
  - memory read: non-destructive analysis of active locations: ‘0’ or ‘1’
  - memory write: non-destructive analysis of active locations and performed operation: ‘0→0’, ‘0→1’, ‘1→0’ or ‘1→1’
- Only backside approach for 0.35μm and smaller chips



memory read difference with laser

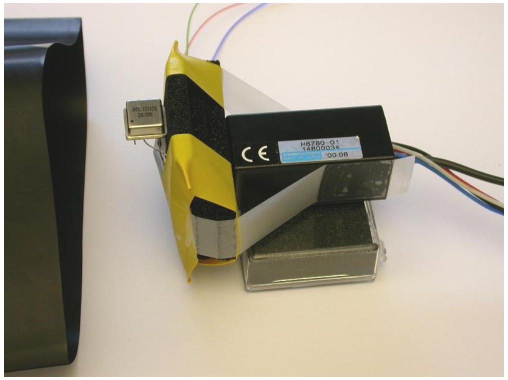


memory write difference with laser

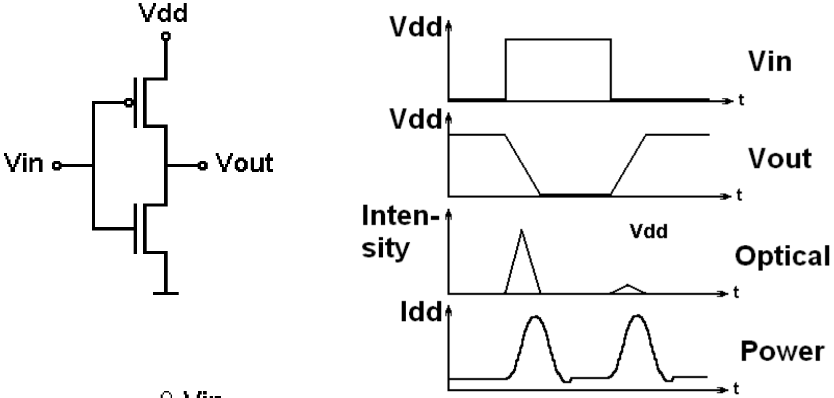
Semi-invasive attacks: side-channel

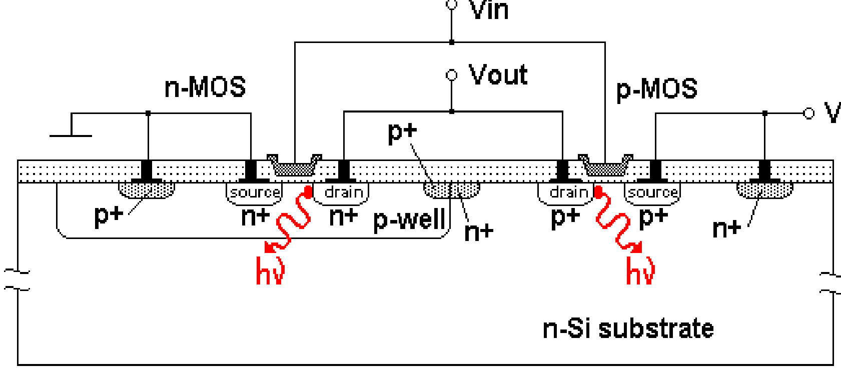
- Optical emission analysis
  - transistors emit photons when they switch
  - 10^{-2} to 10^{-4} photons per switch with peak in IR region (900-1200nm)
  - comes from area close to drain and mainly from NMOS transistor
  - optical emission can be detected with PMT and CCD cameras

CCD setup



PMT setup





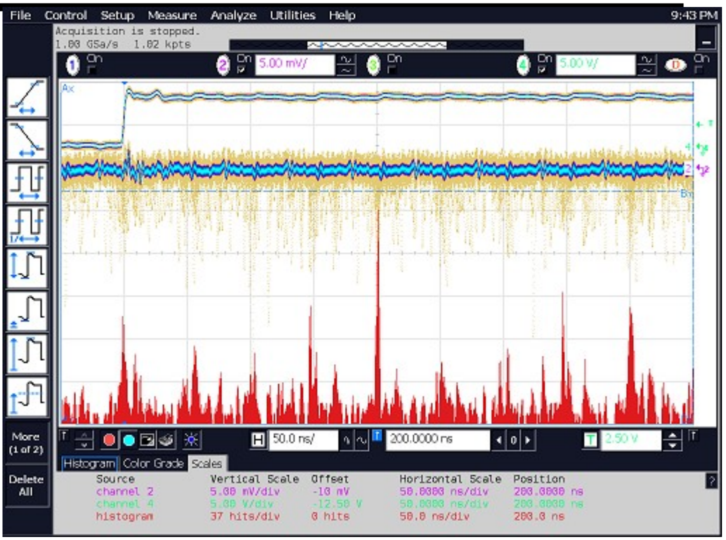
cross section

Semi-invasive optical emission 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:

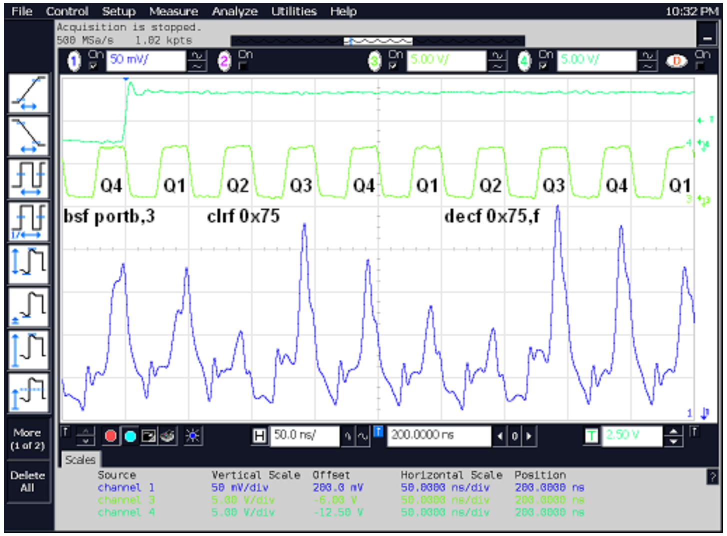
```
bsf portb,3
clrf 0x75
decf 0x75,f
bcf portb,3
goto loop
```

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



Acquisition is stopped.
1.00 GSa/s 1.02 kpts

Source	Vertical Scale	Offset	Horizontal Scale	Position
channel 2	5.00 mV/div	-10 mV	50.0000 ns/div	200.0000 ns
channel 4	5.00 V/div	-12.50 V	50.0000 ns/div	200.0000 ns
histogram	37 hits/div	0 hits	50.0 ns/div	200.0 ns

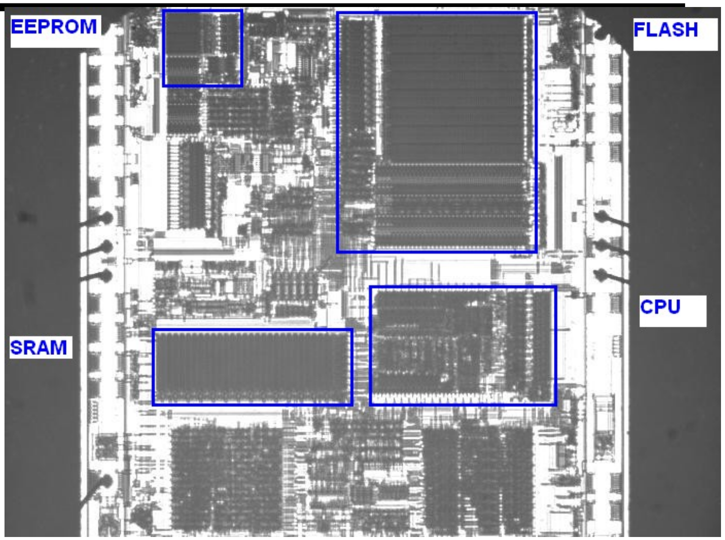


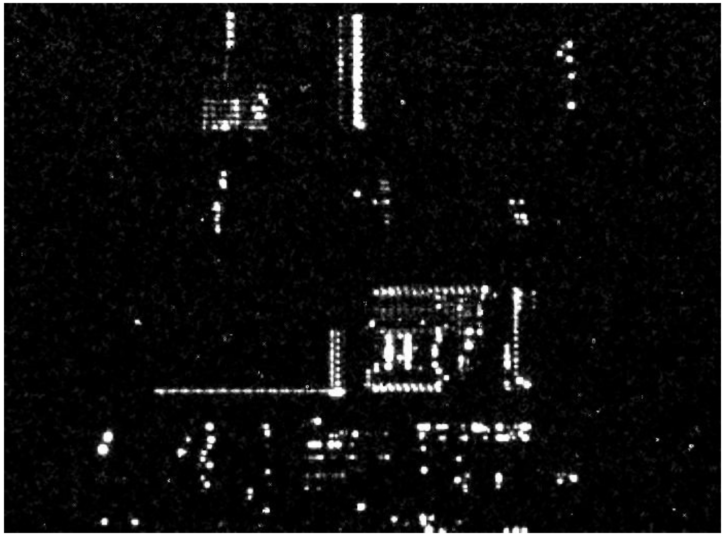
Acquisition is stopped.
500 MSa/s 1.02 kpts

Source	Vertical Scale	Offset	Horizontal Scale	Position
channel 1	50 mV/div	200.0 mV	50.0000 ns/div	200.0000 ns
channel 3	5.00 V/div	-6.00 V	50.0000 ns/div	200.0000 ns
channel 4	5.00 V/div	-12.50 V	50.0000 ns/div	200.0000 ns

Semi-invasive optical emission 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



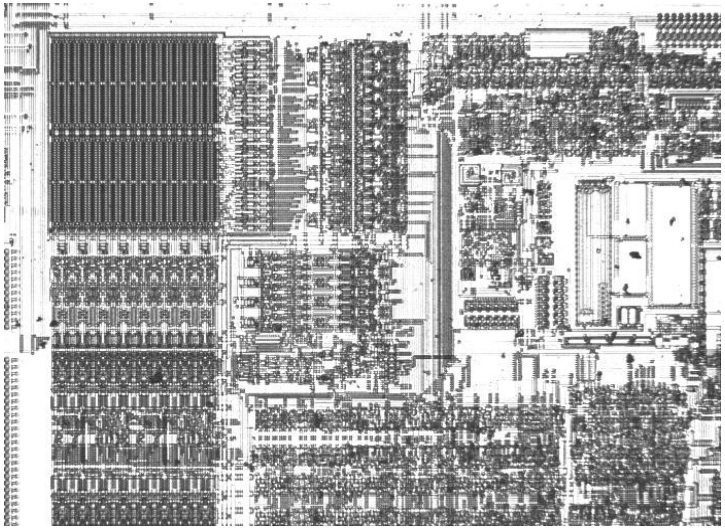


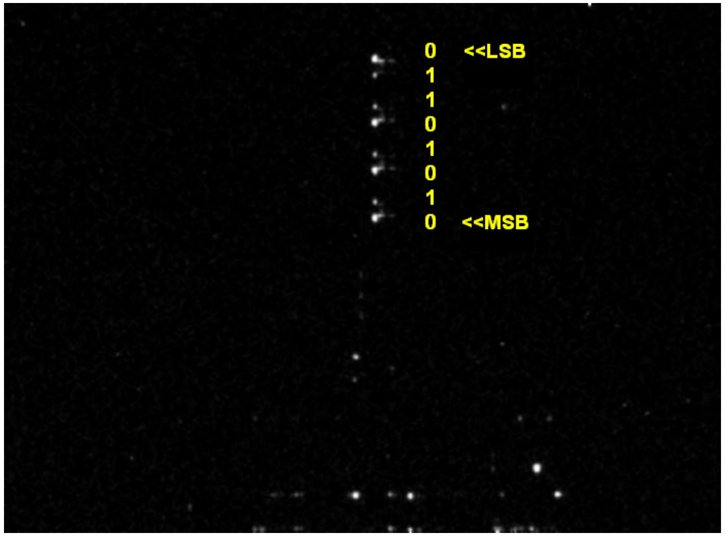
Semi-invasive optical emission results

- 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
```

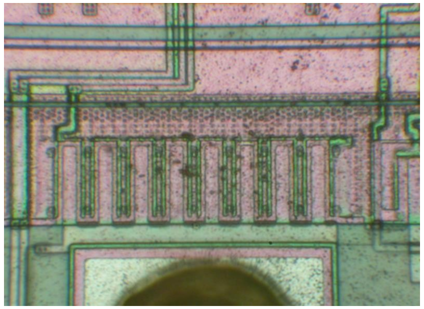
- Flash memory has similar structure and gives similar result
  - data extraction is complicated by the fact that program code is executed from the flash memory



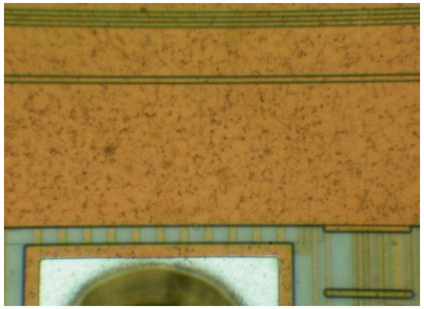


Defence technologies: tamper protection

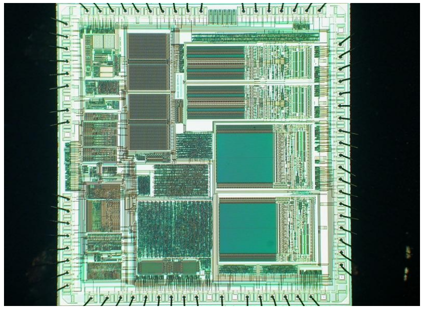
- Help comes from chip fabrication technology
  - planarisation as a part of modern chip fabrication process (0.5 μm or smaller feature size)
  - moving away from building blocks which are easily identifiable and have easily traceable data paths
  - glue logic design makes reverse engineering much harder
  - multiple metal layers block any direct access
  - small size of transistors makes attacks less feasible
  - chips operate at higher frequency and consume less power
  - smaller and BGA packages scare off many attackers



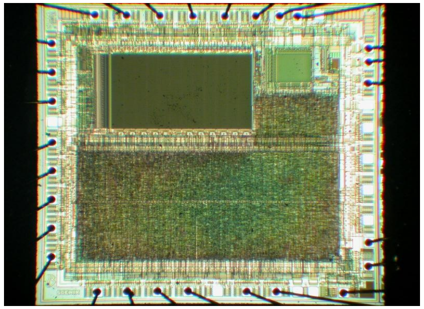
0.9μm



0.5μm



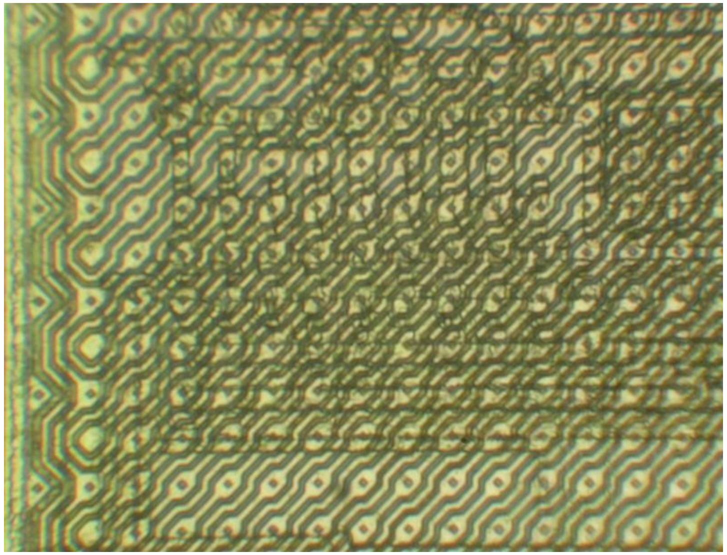
MC68HC908AZ60A microcontroller



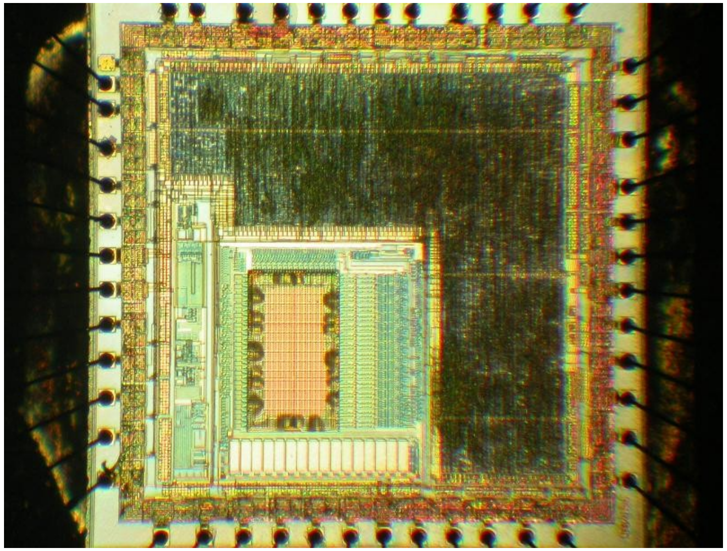
Scenix SX28 microcontroller

Defence technologies: tamper protection

- Additional protections
  - top metal layers with sensors
  - 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 custom secure chip

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?

What goes wrong: where is the key?

- Flash memory prevails
  - usually stores IP, sensitive data, passwords and encryption keys
  - widely used in microcontrollers, smartcards and some FPGAs
  - non-volatile (live at power-up) and reprogrammable, it can be OTP
  - low-power (longer battery life)
- How secure is Flash memory storage?
  - used in smartcards and secure memory chips, so it has to be secure
  - used in secure CPLDs and FPGAs and believed to be highly secure
  - used in secure FPGAs by Actel, marketed as “virtually unbreakable”
- Vulnerabilities of Flash memory found during my research
  - power glitching influence on data read from memory (Web2000)
  - optical fault injection changes data values (CHES2002)
  - laser scanning techniques reveal memory contents (PhD2004)
  - data remanence allows recovery of erased data (CHES2005)
  - optical emission analysis allows direct data recovery (FDTC2009)

Defence technologies: how it fails

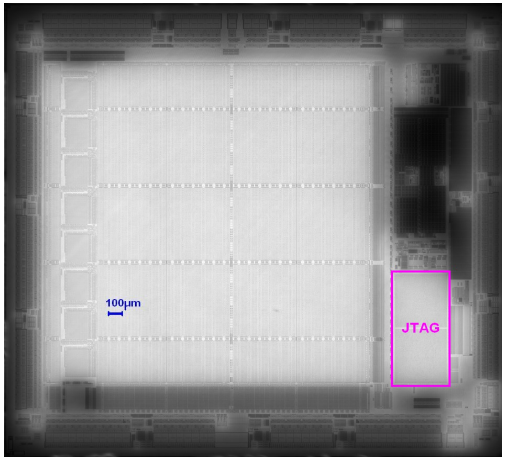
- Microchip PIC microcontroller: software attack on security
  - security fuse can be reset without erasing the code/data memory
- Atmel AVR microcontroller: glitch attack on security fuse
  - security fuse can be reset without erasing the code/data memory
- Hitachi smartcard: information leakage on a products CD
  - full datasheet on the smartcard was placed by mistake on user CD
- Xilinx secure CPLD: programming software bug
  - security fuse incorrectly programmed resulting in no protection
- Dallas SHA-1 secure memory: factory initialisation bug
  - security features were not activated resulting in easy access to key
- Actel secure FPGA: programming software bug
  - Flash FPGA devices were always programmed with 00..00 passkey
- Other possible ways of security failures
  - insiders, datasheets of similar products, development tools, patents

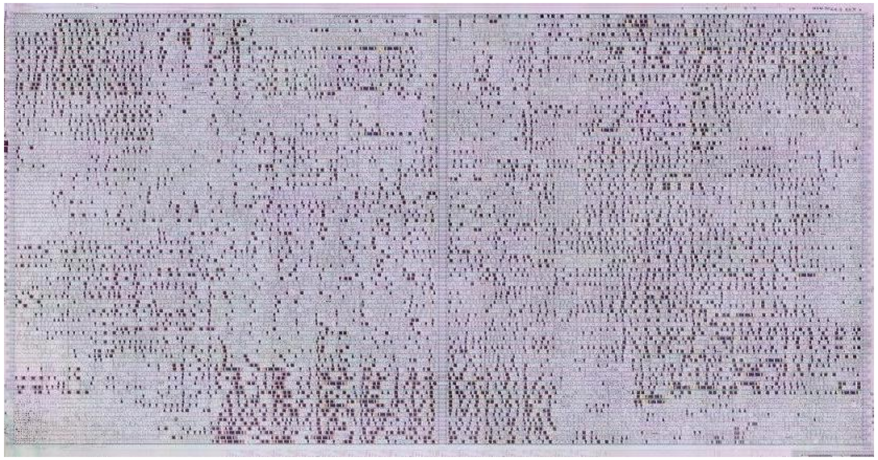
Attacking real secure chip

- Non-invasive attack on Actel® ProASIC3® Flash FPGA
  - *“unique in being reprogrammable and highly resistant to both invasive and noninvasive attacks”*
  - *“on-board security mechanisms prevent access to the programming information from noninvasive attacks”*
  - *“special security keys are hidden throughout the fabric of the device, preventing internal probing and overwriting. They are located such that they cannot be accessed or bypassed without destroying the rest of the device, making both invasive and more subtle noninvasive attacks ineffective”*
  - other security measures: voltage monitors, internal charge pumps, asynchronous internal clock and lack of information about JTAG
- Attack challenge: bypass multiple security protection
  - gain low-level control over the internal Flash hardware control logic and interfere with read sense amplifiers to influence V_{TH}-V_{REF}

Ways to approach

- Ask Actel if the chip has any backdoors or special features
  - even under the most strict NDA Actel would not admit the device has any backdoor access, even if there were such
- Straightforward invasive reverse engineering (40k gates)
  - open up the chip and remove layer by layer using deprocessing technique
  - take high-resolution digital photos and combine them into the layout map
  - create transistor level netlist of the device and convert it into gates level
  - organise gates into functional units and groups
  - simulate the whole system and find hidden functions and bugs
  - 6 to 12 months to extract the design with 300k to 2M GBP cost
  - 3 to 12 months to analyse the data



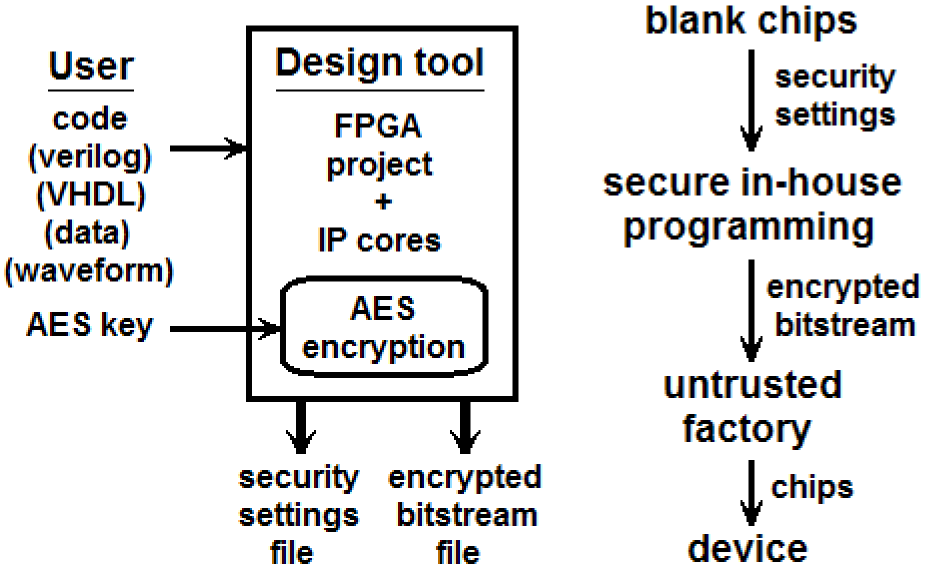


Affordable ways to approach

- Do a bit of research
- Google it for code examples, disclosed information, patents
  - programming files with security settings
  - hint on V_{TH} compensation for RT devices
- Use development tools to generate programming files, use them and eavesdrop on JTAG communication; it is simpler
  - STAPL high-level language is used which is self-explanatory
- Company website and distributors for clues on the security
  - release notes and product descriptions mention *"dual-key security"*
  - *"board with a dual-key M1AFS600 device"*
- Why is the **'dual-key security'** is not mentioned in any Actel datasheets, press releases and white papers???

Secure AES-128 update in Actel FPGA

- Designed to prevent IP theft, cloning and overbuilding
- A3P600 vs M1A3P600 (ProASIC3 FPGA family)
  - if certain vendor IP cores are used (Cortex-M1) – no user protection
  - user AES DMK is used for Actel IP core protection (DMK = M1 key)



User

code (verilog) (VHDL) (data) (waveform)

AES key

Design tool

FPGA project + IP cores

AES encryption

security settings file

encrypted bitstream file

blank chips

security settings

secure in-house programming

encrypted bitstream

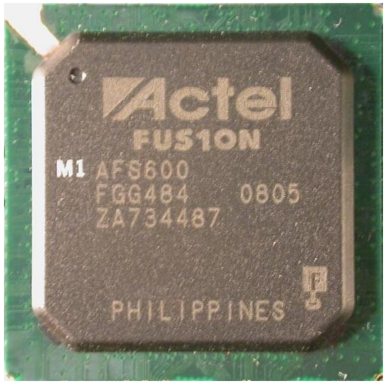
untrusted factory

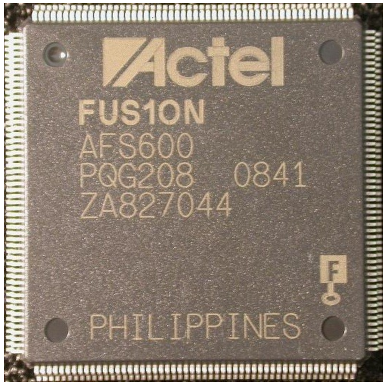
chips

device

Dual-key security in Actel FPGA

- What problem does the dual-key security solve?
  - IP cores loyalty control without compromising user security
  - *“The system enables application development with the ARM Cortex-M1 and/or with your own optional AES key (owing to dual-key feature) in mixed-signal M1-enabled Fusion devices”*
- AFS600 vs M1AFS600 (Fusion mixed-signal FPGA family)
  - user AES DMK protects user's IP and 2nd key is for the vendor IP
  - when protection for both user IP and vendor IP are required then AES Key = H(user key, vendor key), H – secure hash function
  - in M1AFS600 the 2nd key = M1 key, what is the 2nd key in AFS600?





How the AES key can be attacked?

- Invasive attacks (expensive)
  - partial reverse engineering followed by microprobing
- Semi-invasive attacks (affordable)
  - optical fault injection attack (Skorobogatov, Anderson CHES2002)
  - optical emission analysis (Skorobogatov FDTC2009)
- 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 (clocks, pumps, acquisition)
- What can be done if AES key is known
  - decrypt bitstream configuration and clone the design
  - decrypt internal Flash ROM configuration
  - authenticate the device and gain access to reconfiguration features

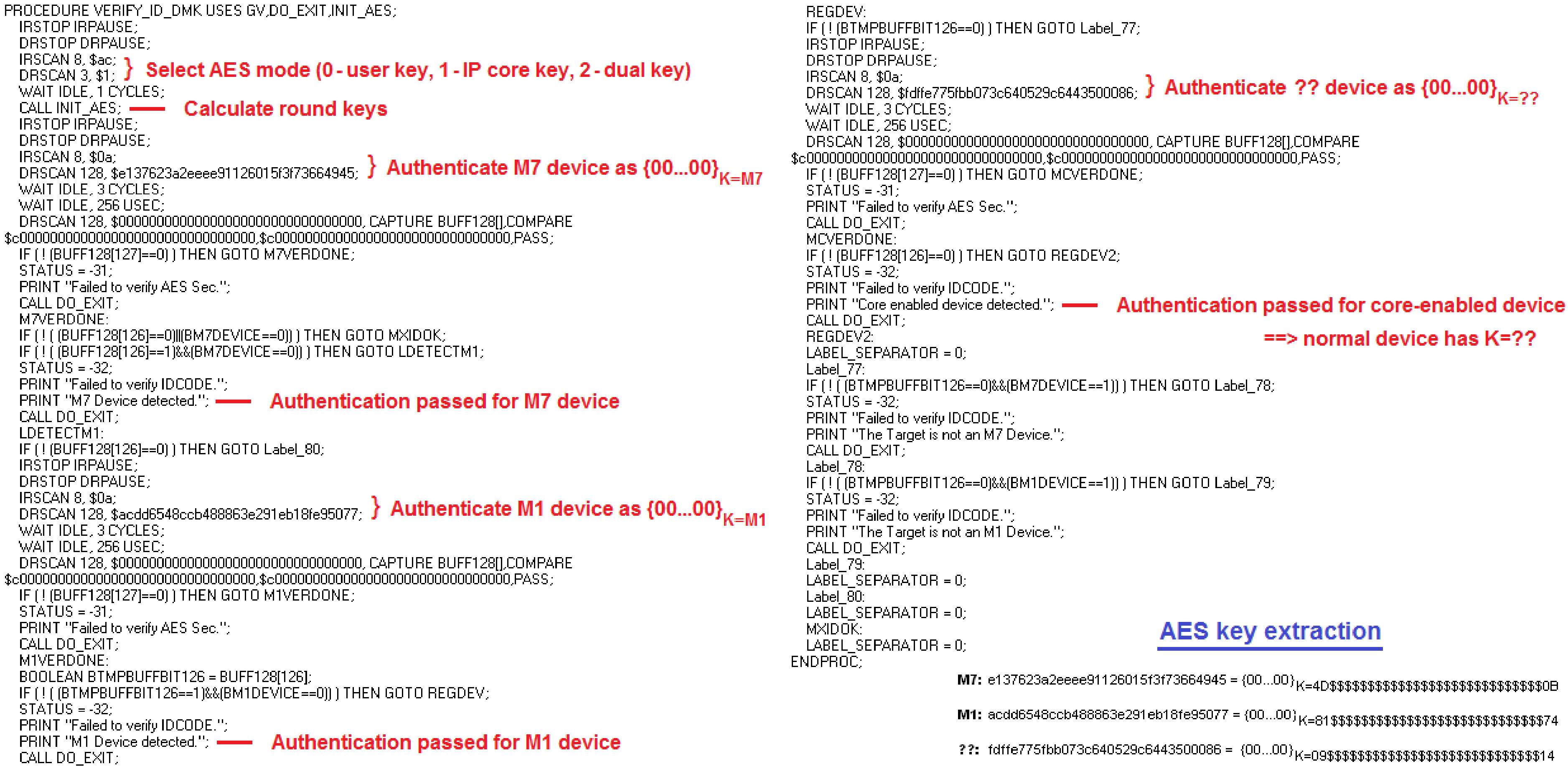
How long does it take to get the AES key?

- 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 Espial tester using breakthrough approach to power analysis technique from QVL

Quest for the factory secret master key

- Reverse engineering of the STAPL file for M1AFS600

  source: Google search that revealed Cortex-M1 Fusion Kit soft CD



```
PROCEDURE VERIFY_ID_DMK USES GV,DO_EXIT,INIT_AES;
   IRSTOP IRPAUSE;
   DRSTOP DRPAUSE;
   IRSCAN 8, $ac;
   DRSCAN 3, $1;
```

} Select AES mode (0 - user key, 1 - IP core key, 2 - dual key)

```
   WAIT IDLE, 1 CYCLES;
   CALL INIT_AES;
```

Calculate round keys

```
   IRSTOP IRPAUSE;
   DRSTOP DRPAUSE;
   IRSCAN 8, $0a;
   DRSCAN 128, $e137623a2eeee91126015f3f73664945;
```

} Authenticate M7 device as $\{00...00\}_{K=M7}$

```
   WAIT IDLE, 3 CYCLES;
   WAIT IDLE, 256 USEC;
   DRSCAN 128, $00000000000000000000000000000000, CAPTURE BUFF128[],COMPARE
$c0000000000000000000000000000000,$c0000000000000000000000000000000,PASS;
   IF ( ! (BUFF128[127]==0) ) THEN GOTO M7VERDONE;
   STATUS = -31;
   PRINT "Failed to verify AES Sec.";
   CALL DO_EXIT;
   M7VERDONE:
   IF ( ! ( (BUFF128[126]==0)||(BM7DEVICE==0)) ) THEN GOTO MXIDOK;
   IF ( ! ( (BUFF128[126]==1)&&(BM7DEVICE==0)) ) THEN GOTO LDETECTM1;
   STATUS = -32;
   PRINT "Failed to verify IDCODE.";
   PRINT "M7 Device detected.";
```

Authentication passed for M7 device

```
   CALL DO_EXIT;
   LDETECTM1:
   IF ( ! (BUFF128[126]==0) ) THEN GOTO Label_80;
   IRSTOP IRPAUSE;
   DRSTOP DRPAUSE;
   IRSCAN 8, $0a;
   DRSCAN 128, $acdd6548ccb488863e291eb18fe95077;
```

} Authenticate M1 device as $\{00...00\}_{K=M1}$

```
   WAIT IDLE, 3 CYCLES;
   WAIT IDLE, 256 USEC;
   DRSCAN 128, $00000000000000000000000000000000, CAPTURE BUFF128[],COMPARE
$c0000000000000000000000000000000,$c0000000000000000000000000000000,PASS;
   IF ( ! (BUFF128[127]==0) ) THEN GOTO M1VERDONE;
   STATUS = -31;
   PRINT "Failed to verify AES Sec.";
   CALL DO_EXIT;
   M1VERDONE:
   BOOLEAN BTMPBUFFBIT126 = BUFF128[126];
   IF ( ! ( (BTMPBUFFBIT126==1)&&(BM1DEVICE==0)) ) THEN GOTO REGDEV;
   STATUS = -32;
   PRINT "Failed to verify IDCODE.";
   PRINT "M1 Device detected.";
```

Authentication passed for M1 device

```
   CALL DO_EXIT;
   REGDEV:
   IF ( ! (BTMPBUFFBIT126==0) ) THEN GOTO Label_77;
   IRSTOP IRPAUSE;
   DRSTOP DRPAUSE;
   IRSCAN 8, $0a;
   DRSCAN 128, $fdffe775fbb073c640529c6443500086;
```

} Authenticate ?? device as $\{00...00\}_{K=??}$

```
   WAIT IDLE, 3 CYCLES;
   WAIT IDLE, 256 USEC;
   DRSCAN 128, $00000000000000000000000000000000, CAPTURE BUFF128[],COMPARE
$c0000000000000000000000000000000,$c0000000000000000000000000000000,PASS;
   IF ( ! (BUFF128[127]==0) ) THEN GOTO MCVERDONE;
   STATUS = -31;
   PRINT "Failed to verify AES Sec.";
   CALL DO_EXIT;
   MCVERDONE:
   IF ( ! (BUFF128[126]==0) ) THEN GOTO REGDEV2;
   STATUS = -32;
   PRINT "Failed to verify IDCODE.";
   PRINT "Core enabled device detected.";
```

Authentication passed for core-enabled device

==> normal device has K=??

```
   CALL DO_EXIT;
   REGDEV2:
   LABEL_SEPARATOR = 0;
   Label_77:
   IF ( ! ( (BTMPBUFFBIT126==0)&&(BM7DEVICE==1)) ) THEN GOTO Label_78;
   STATUS = -32;
   PRINT "Failed to verify IDCODE.";
   PRINT "The Target is not an M7 Device.";
   CALL DO_EXIT;
   Label_78:
   IF ( ! ( (BTMPBUFFBIT126==0)&&(BM1DEVICE==1)) ) THEN GOTO Label_79;
   STATUS = -32;
   PRINT "Failed to verify IDCODE.";
   PRINT "The Target is not an M1 Device.";
   CALL DO_EXIT;
   Label_79:
   LABEL_SEPARATOR = 0;
   Label_80:
   LABEL_SEPARATOR = 0;
   MXIDOK:
   LABEL_SEPARATOR = 0;
ENDPROC;
```

AES key extraction

M7: e137623a2eeee91126015f3f73664945 = $\{00...00\}_{K=4D\$0B}$

M1: acdd6548ccb488863e291eb18fe95077 = $\{00...00\}_{K=81\$74}$

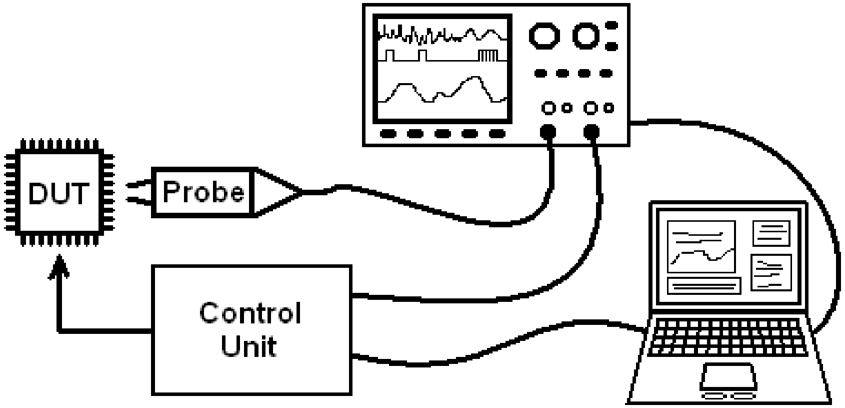
??: fdffe775fbb073c640529c6443500086 = $\{00...00\}_{K=09\$14}$

Results

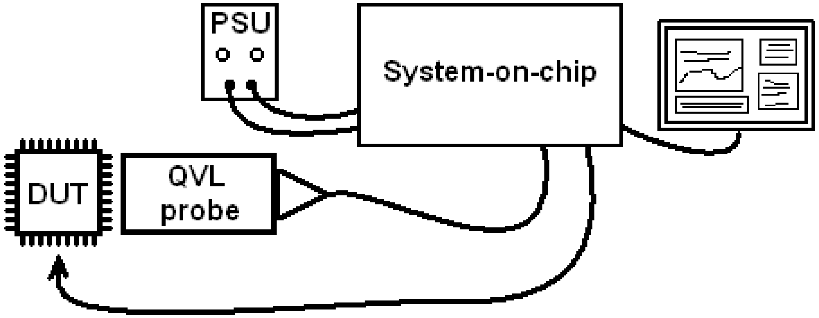
- What can be done if the factory secret master key is known?
  - turn some ROM areas into reprogrammable Flash areas
  - reprogram low-level features
  - access shadow areas
  - access hidden JTAG registers
  - find the JTAG registers responsible for controlling read sense amplifiers, such that V_{REF} can be adjusted
- Actel's big security mistake
  - all Actel 3rd generation Flash FPGA devices (ProASIC3, ProASIC3L, ProASIC3 nano, Igloo, Igloo plus, Igloo nano, Fusion, SmartFusion) share the same factory secret master key
  - thanks to irresponsible corporate security strategy many Flash FPGA devices can now be manipulated
- Do we really have to go that long way to find the factory key?
  - YES, because it is somewhat million times harder to break the factory key than the AES key, thanks to side-channel leakages

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

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)?

Conclusion

- There is no such a thing as absolute protection
  - given enough time and resources any protection can be broken
- Attack technologies are constantly evolving
  - do not underestimate capabilities of the attackers
  - technical progress reduces cost of already known attacks
- Defence should be ahead of attack technologies
  - security hardware engineers must be familiar with existing attack technologies to develop adequate protection
  - many chips unavoidably have backdoors as a part of fabrication and testing process, but they must be made as secure as possible to prevent easy target
- Many vulnerabilities were found in various secure chips and more are to be found posing more challenges to hardware security engineers

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

References

- Slides
  - http://www.cl.cam.ac.uk/~sps32/NCL_2011.pdf
- Literature
  - http://www.cl.cam.ac.uk/~sps32/
  - http://www.cl.cam.ac.uk/~sps32/#Publications