Using Optical Emission Analysis for Estimating Contribution to Power Analysis

Dr Sergei Skorobogatov

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

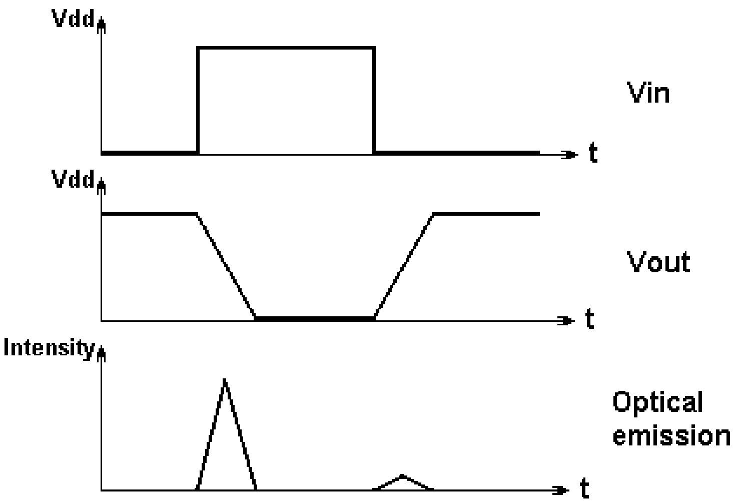
UNIVERSITY OF CAMBRIDGE
Computer Laboratory

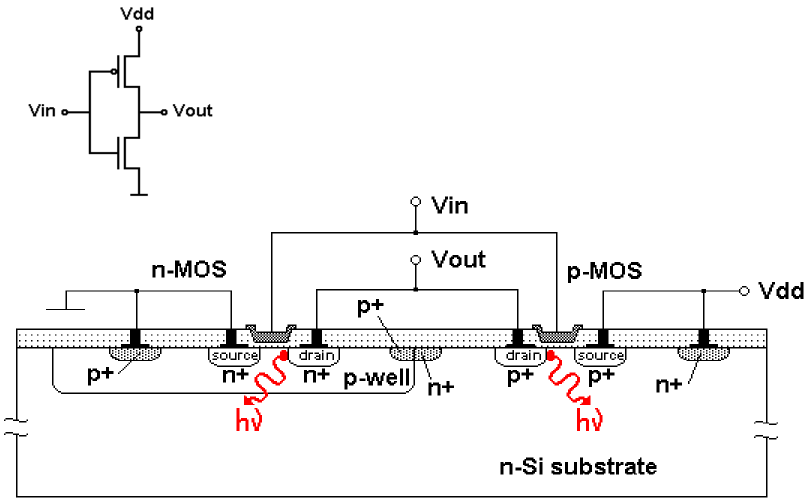
Introduction

- Power analysis attacks were introduced in 1999 (Kocher et al), and exploit well known fact that power consumption of a chip is correlated with its operation and processed data
- Semi-invasive attacks in a form of optical fault injection were introduced in 2002 (Skorobogatov et al), and use low-cost approach when a chip is attacked without establishing any physical contact to its internal components
- Optical emission analysis attacks were introduced in 2008 (Ferrigno et al), and exploit well known fact that photon emission of a chip is correlated with processed data
- The presented research shows how optical emission analysis attacks can be done at a low cost and how they can be used to improve protection against power analysis

Background

- Optical emission from CMOS circuits
  - known for over 40 years
  - actively used in failure analysis for over 20 years
- Can be used to compromise security in silicon chips
  - so far required expensive equipment and special chip preparation
  - was not considered as a threat, hence, no protection is in place





Background

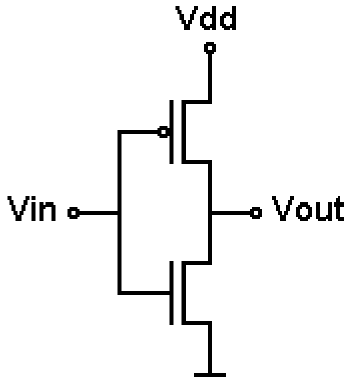
- Number of photons emitted per every switch

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

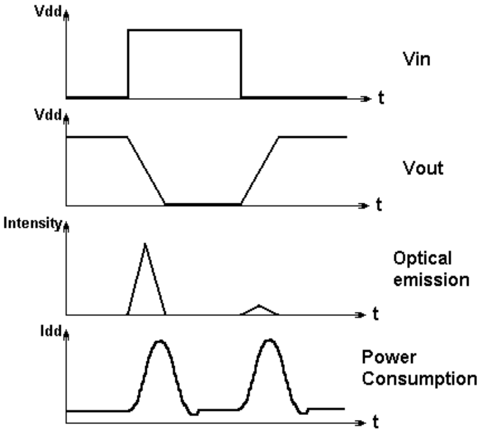
  S_e – spectral emission density, B – emission bandwidth,

  L_H – hot-carrier region length, I_d – drain current, q – e^- charge,

  v_s – carrier saturated velocity, T_s – transition time

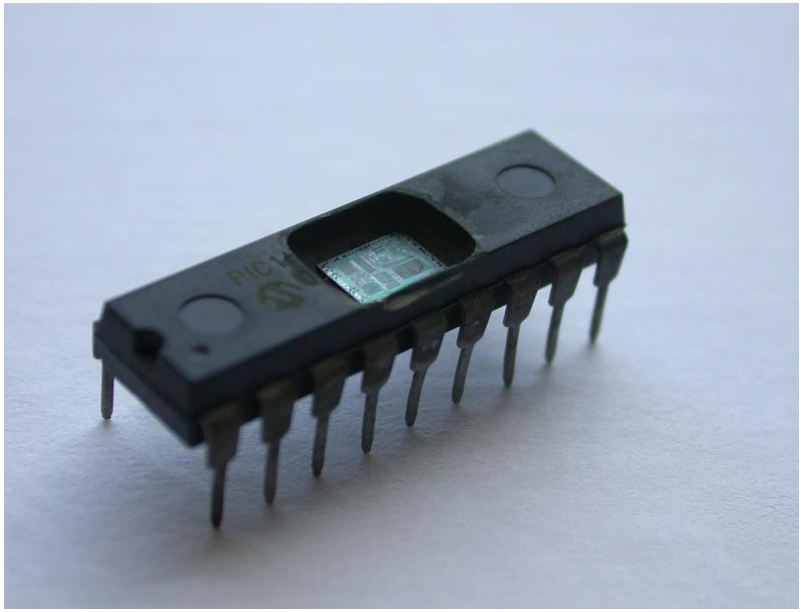


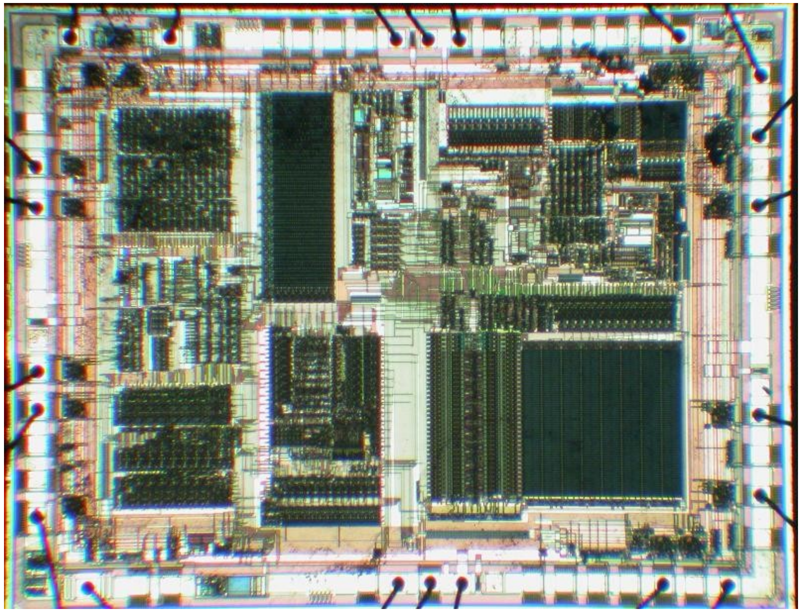
- Only 5~10% of photons can reach the sensor (direction and losses)
- Existing analysis techniques
  - picosecond imaging circuit analysis (PICA) uses photomultiplier arrays
  - photon emission microscopy (PEM) uses special IR cameras
- Correlation between photon emission and power consumption



Experimental setup

- Sample preparation (PIC16F628)
- Locating Flash, EEPROM, SRAM, CPU
- Choosing PMT, APD and CCD sensors





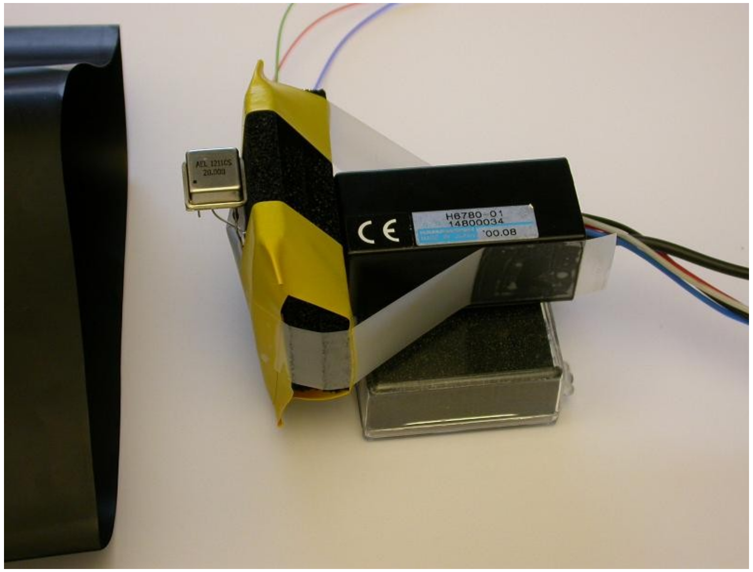
Experimental setup

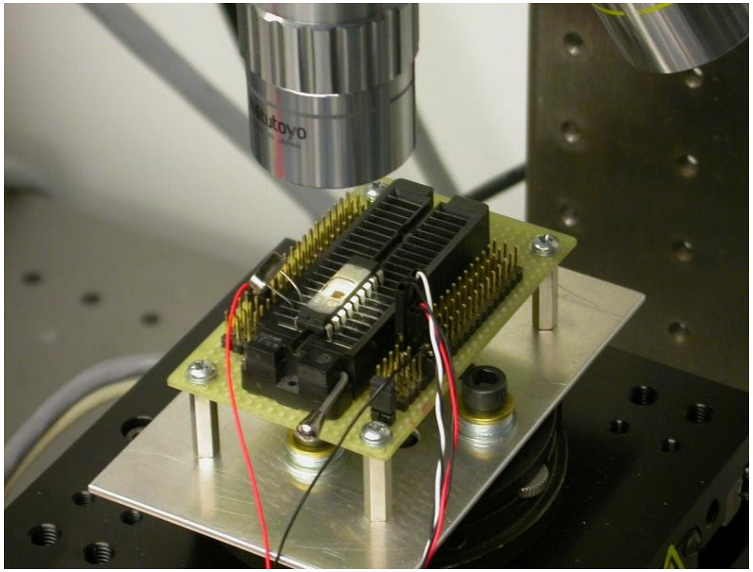
- Choosing PMT: low dark current
- Choosing APD: high quantum efficiency
- Choosing CCD: NIR sensitivity, low dark current

	Parameters				
Type of camera	***Wave-length, nm***	***QE at 900 nm***	***QE at 1000 nm***	***Dark current e^-/s***	***Time response***
Quantar Mepsicron II S25	180–940	1%	0%	0.005	50 ps
Hamamatsu C4880-21	200–1200	50%	20%	0.3	20 ms
Hamamatsu C4880-50	200–1100	30%	10%	0.01	20 ms
Hamamatsu H10330-25	850–1250	2%	2%	2000	900 ps
Hamamatsu H6780-01	250–850	<1%	0%	400	780 ps
Sensl PCDMini-0020	400–1100	2%	<1%	50	200 ps
Sony Super HAD CCD	300–1050	8%	1%	0.02	10 µs
Sony EXview HAD CCD	300–1100	12%	5%	0.02	10 µs

Experimental setup

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





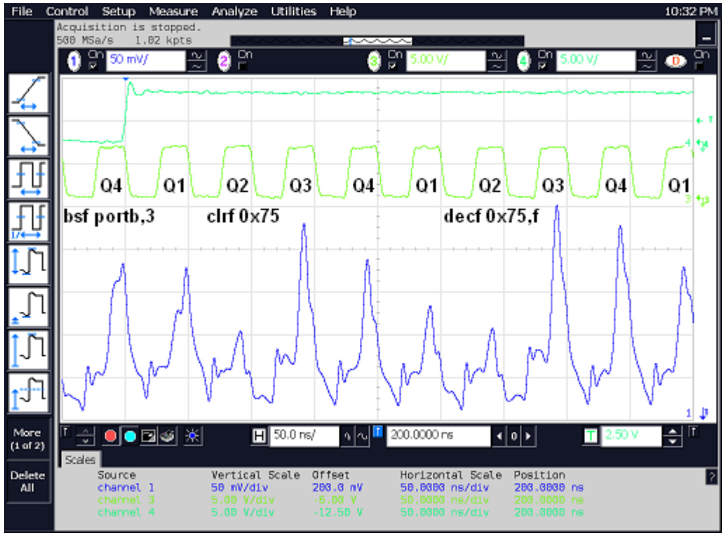
Results

- PIC16F628 was running at 20MHz clock (5 MIPS) with 6V power supply
  - PMT: H6780-01, 60' acquisition
  - SPA: 10Ω resistor, active probe
- PMT vs SPA
  - higher bandwidth
  - possible localisation
  - special hardware will suit better as oscilloscope is not designed for integration
- Test code:

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

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



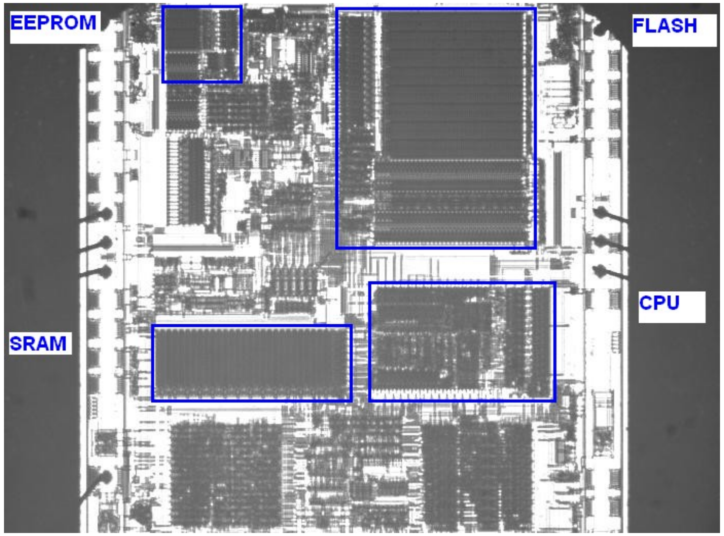
Acquisition is stopped.
500 MSa/s 1.02 kpts

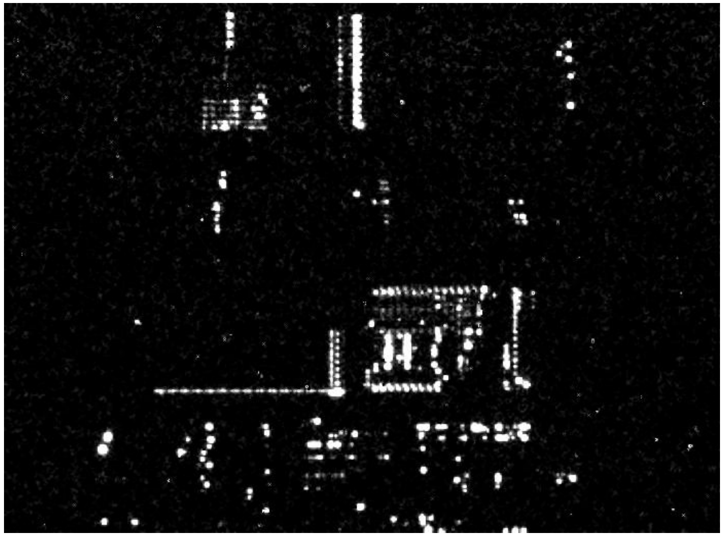
Source	Vertical Scale	Offset	Horizontal Scale	Position
channel 1	50 mV/div	200.0 mV	50.0000 ns/div	200.0000 ns
channel 3	5.00 V/div	-6.00 V	50.0000 ns/div	200.0000 ns
channel 4	5.00 V/div	-12.50 V	50.0000 ns/div	200.0000 ns

Results

- CCD
  - 2x objective lens
  - 30' integration time
  - continuous read of EEPROM and SRAM:

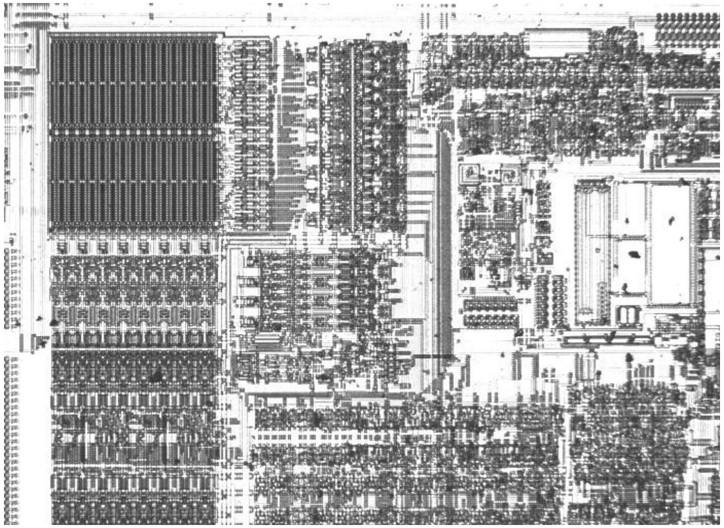
    ```
    incf EEADR,f
    bsf EECON1,RD
    movf EEDATA,w
    decf 0x75,f
    goto loop
    ```

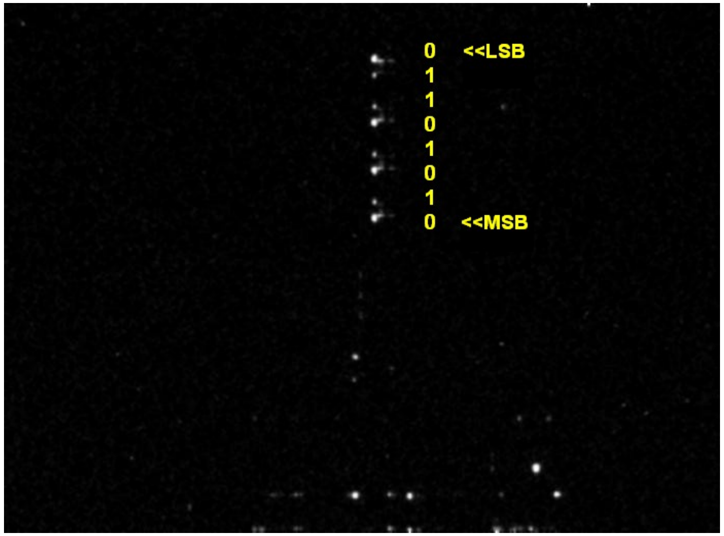




Results

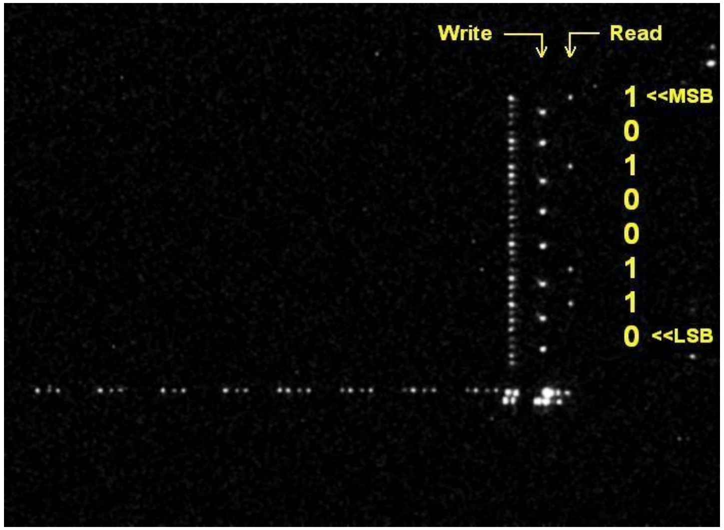
- EEPROM
  - 10x objective lens
  - 10' integration time
  - read 4 addresses in a loop
  - data: 56h, 56h, 56h, 00h
- Flash memory has similar structure and gives similar results

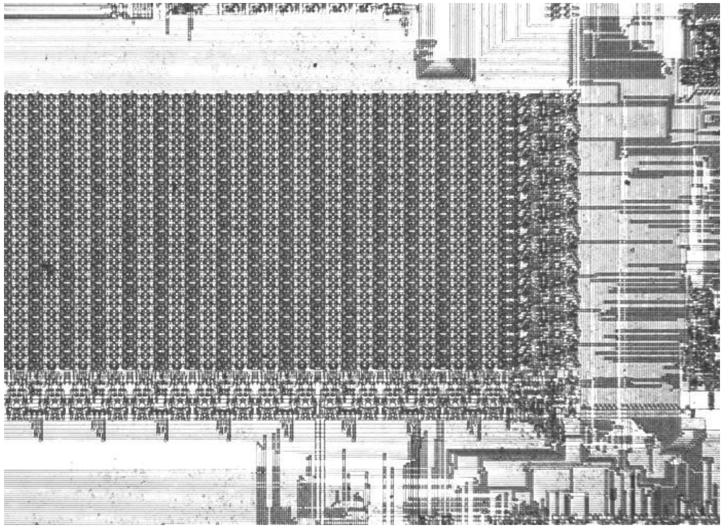


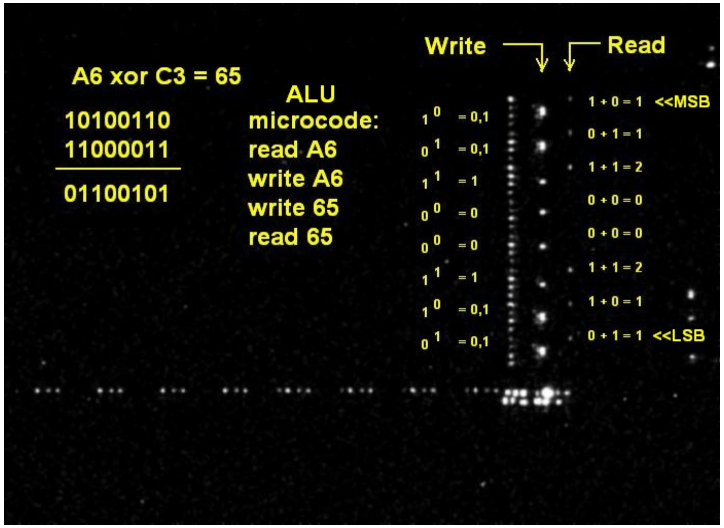


Results

- SRAM
  - 10x objective lens
  - 10' integration time
  - read A6h: movf 0x75,w
  - write W=A6h: movwf 0x75
  - XOR W=C3h, (0x74)=A6h, xorwf 0x74,f







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 require longer integration time
- Backside approach
  - silicon is transparent to light wavelengths above 1000 nm
  - lower spatial resolution
  - longer integration time due to higher losses in silicon and optics
  - higher magnification lenses give better result
  - use of NIR optics improves result (expensive)
  - substrate thinning might be useful for faster analysis (expensive)
  - increase of the power supply voltage boosts the optical emission

Limitations and improvements

- Increasing the power supply voltage:

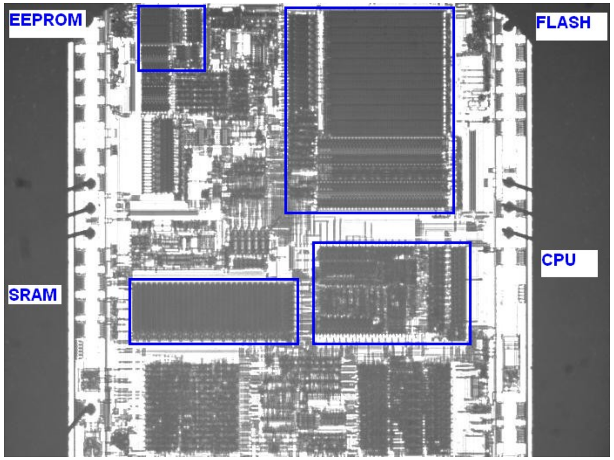
every 10% increase boosts the emission by 40~120%

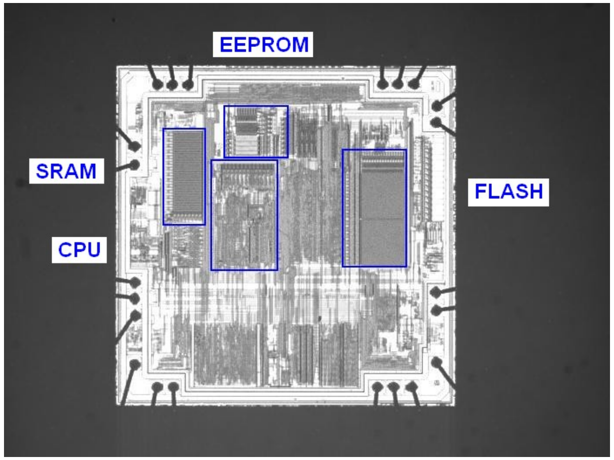
	Power Supply Voltage					
PIC16F628	*3.5 V*	*4.0 V*	*4.5 V*	*5.0 V*	*5.5 V*	*6.0 V*
Photometry results	1046	1286	2427	8400	23292	43026

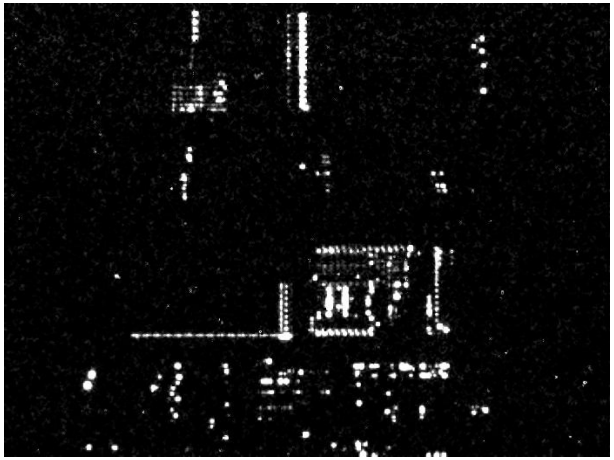
	Power Supply Voltage					
130nm ASIC	*1.5 V*	*1.6 V*	*1.8 V*	*2.0 V*	*2.2 V*	*2.5 V*
Photometry results	889	1194	1953	5270	9536	23270

Limitations and improvements

- 16F628 vs 16F628A: 0.9 µm and 0.5 µm, higher density with CMP technology leads to ~80% loss in intensity

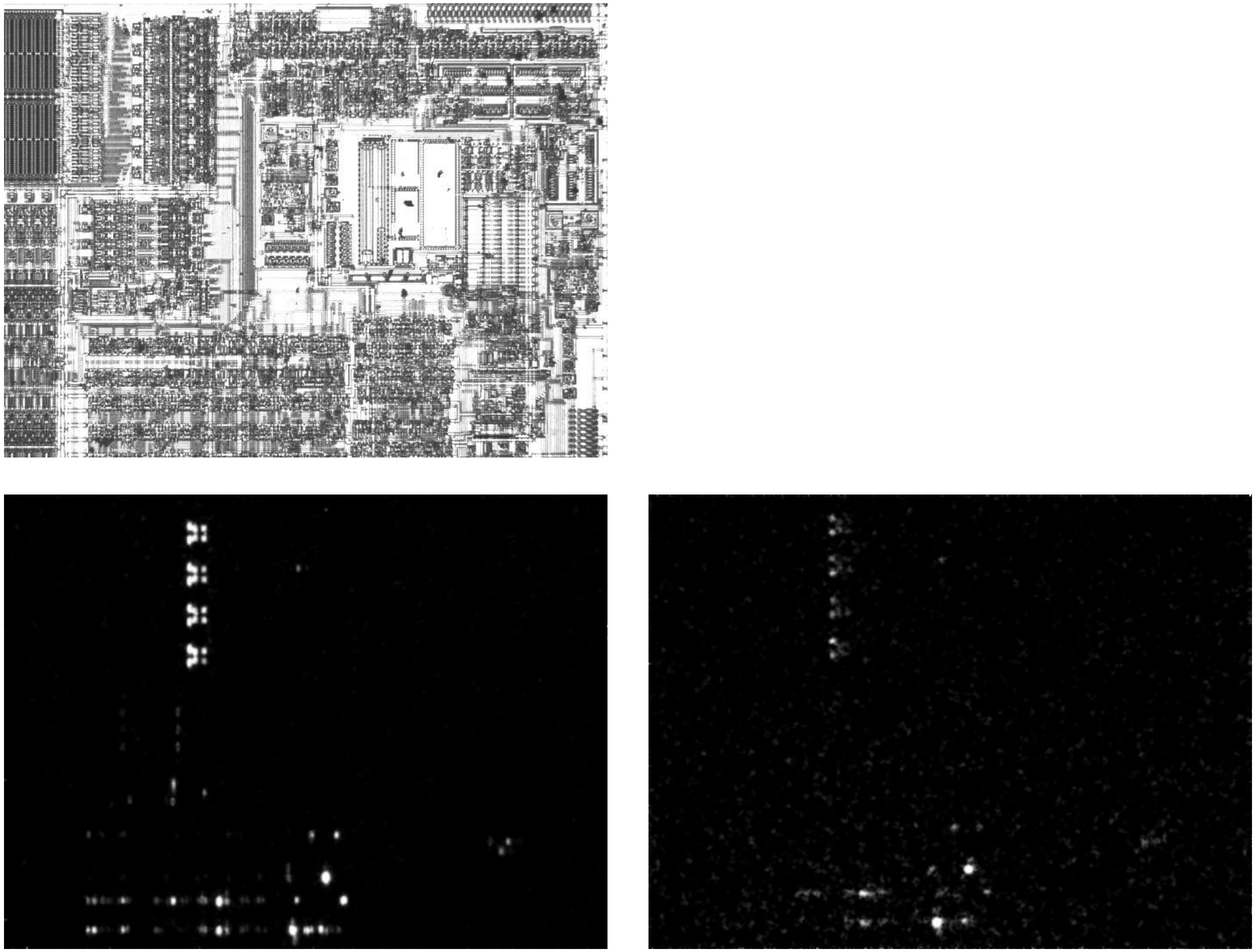






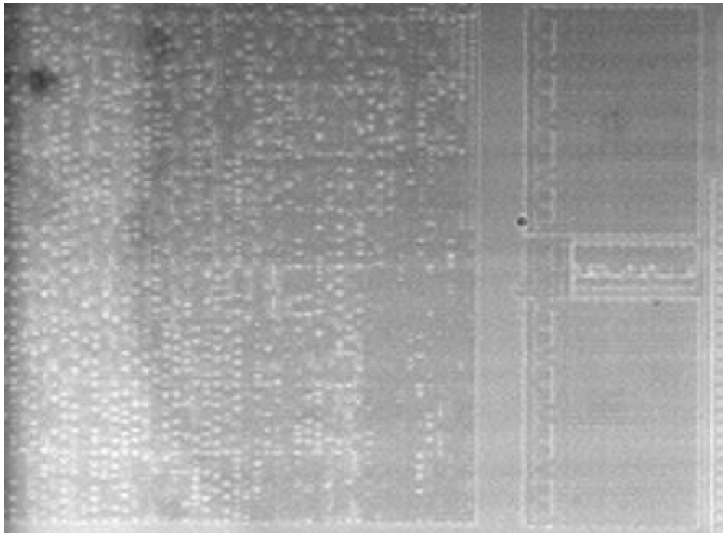
Limitations and improvements

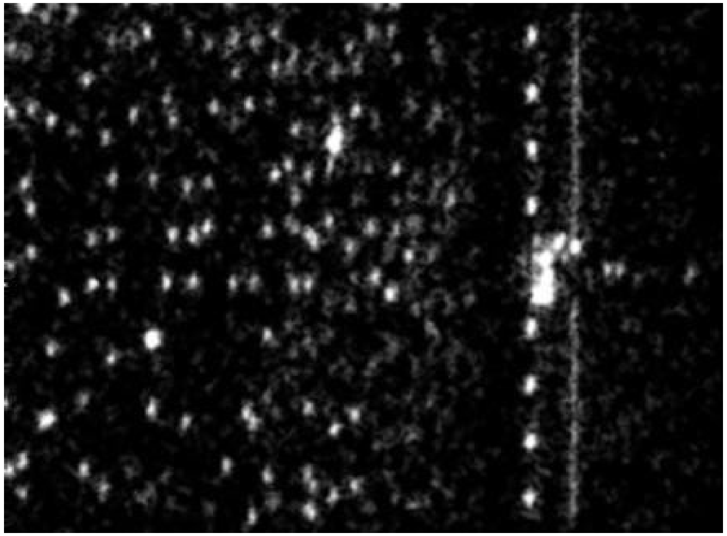
- PIC16F628: EEPROM area from front and rear sides after 30' of integration with standard 10x objective lens



Limitations and improvements

- Backside approach
  - 0.13 µm ASIC with SRAM
  - Vcc increased from 1.5 V to 2.0 V (6x boost of emission)
  - 20x NIR objective
  - 60' integration time





Countermeasures

- Use of modern chips with multiple metal layers forces an attacker to use backside approach and results in longer time required for the attack
- Metal shielding over sensitive areas can help but cannot prevent backside analysis
- Encryption and redundancy check make analysis harder
- Asynchronous circuits could make the attack more problematic as data analysis requires a single byte to be present at a specific time

Conclusions

- Optical emission analysis can be carried out at a relatively low cost using hobbyist astronomical CCD cameras
- PMT offers high bandwidth and acquired data have correlation with power analysis results
- Results of optical emission analysis can be used for finding weak spots in protection against power analysis attacks
- Optical emission analysis offers possibility for partial reverse engineering of chips including data analysis
- Backside approach can help in modern chips, but has lower spatial resolution and requires longer integration time
- Increase of the power supply voltage boosts the optical emission and considerably reduces time of analysis
- Lack of protection against optical side-channel attacks in modern chips might lead to possible vulnerabilities