Optical Fault Induction Attacks

Sergei Skorobogatov
Ross Anderson

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Semi-Invasive attacks

- Depackaging is required (access chip surface)

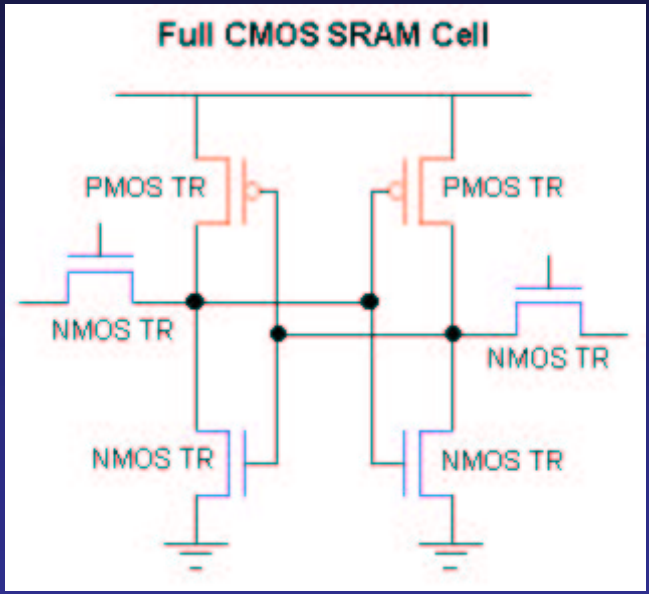
- No internal connections are required
  - No expensive FIB or Laser cutter techniques
  - No microprobing

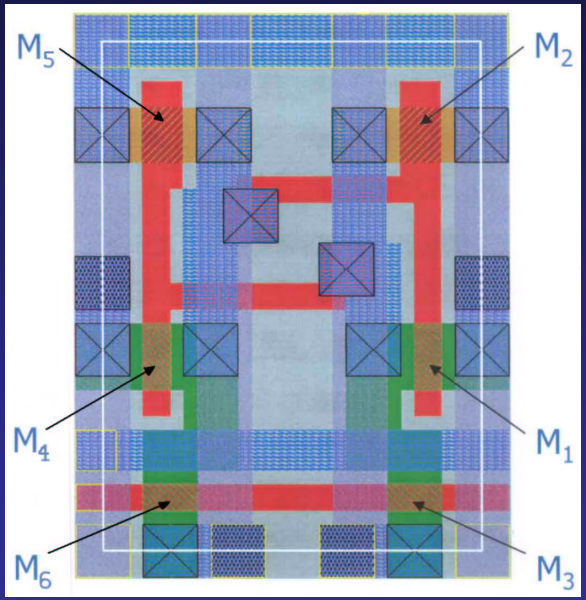
Examples of Semi-Invasive attacks

- UV light applied to a certain location
  - Erase EPROM/E²PROM/Flash (removing charge from floating gate)
- X-ray
  - Erase EPROM/E²PROM/Flash under top metal protection
  - Local ionization
- Laser light
  - Local ionization
- Local heating
- Electromagnetic fields

Attack on Static RAM

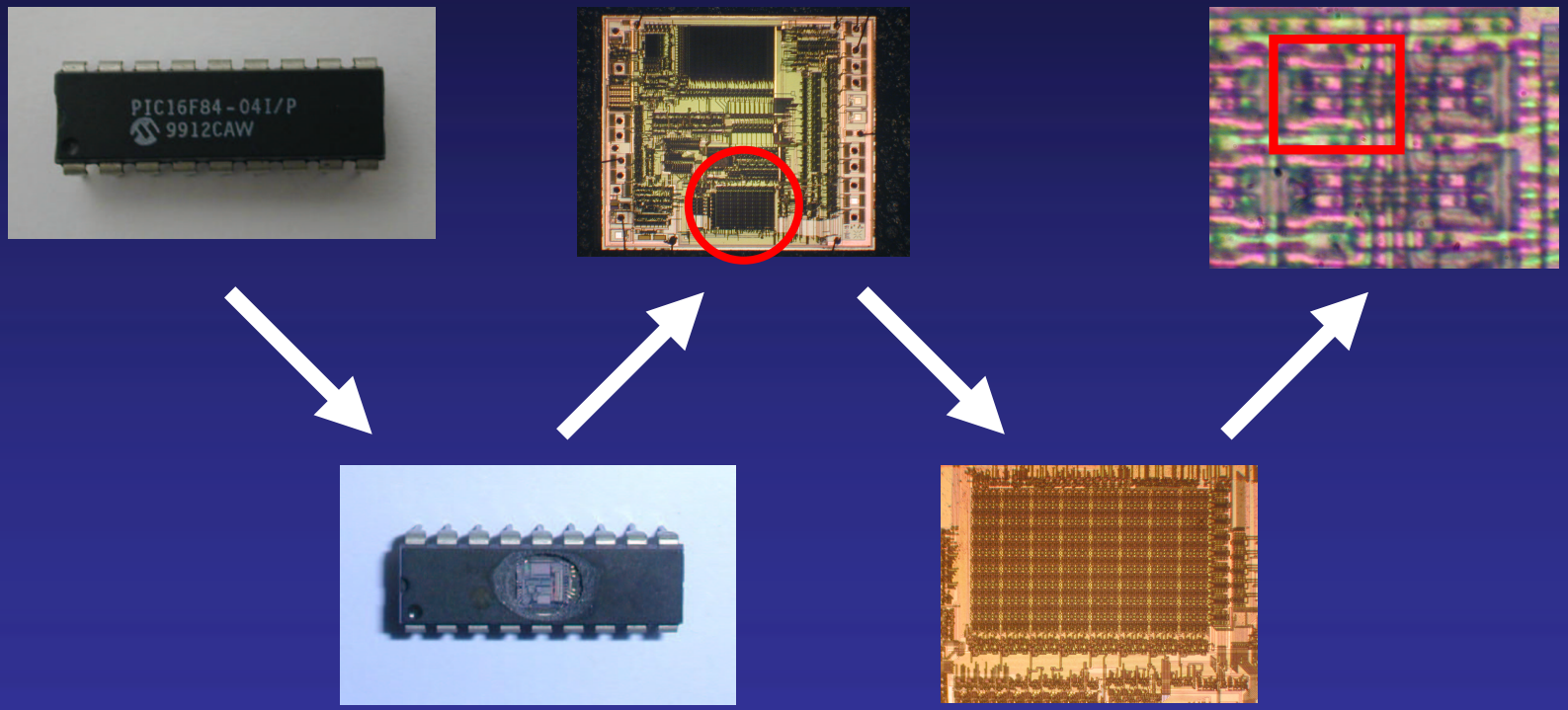
- Structure of CMOS SRAM cell





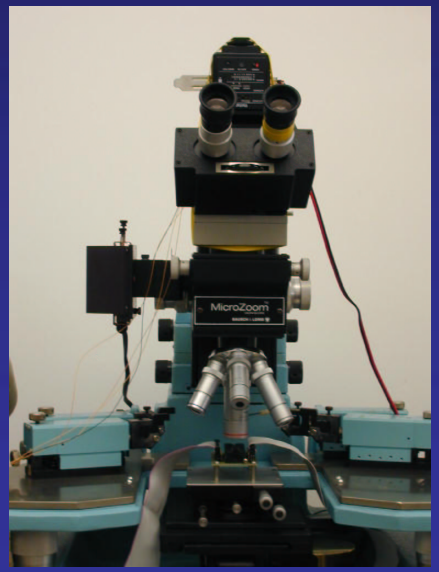
Attack on SRAM in PIC16F84

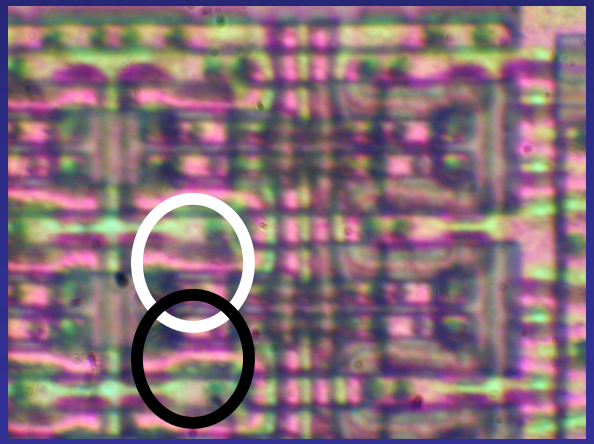
- Chip preparation



Attack on SRAM in PIC16F84

- Attack setup
  - Vivitar 550FD photoflash on microscope camera port
  - Magnification set to 1500x
  - Shielding the light with aluminum foil aperture
  - PIC16F84 programmed to monitor the SRAM





Results

- Allocation of memory bits

BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0

- Physical location of each memory address

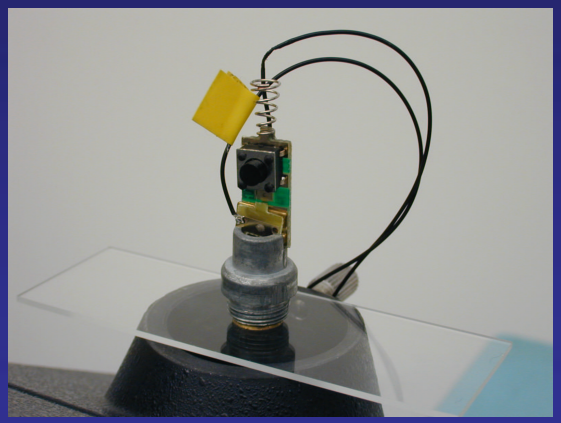
30h	34h	38h	3Ch	40h	44h	48h	4Ch	10h	14h	18h	1Ch	20h	24h	28h	2Ch	0Ch
31h	35h	39h	3Dh	41h	45h	49h	4Dh	11h	15h	19h	1Dh	21h	25h	29h	2Dh	0Dh
32h	36h	3Ah	3Eh	42h	46h	4Ah	4Eh	12h	16h	1Ah	1Eh	22h	26h	2Ah	2Eh	0Eh
33h	37h	3Bh	3Fh	43h	47h	4Bh	4Fh	13h	17h	1Bh	1Fh	23h	27h	2Bh	2Fh	0Fh

Implications on Smartcards

- Attack on RSA digital signature:
  $S = h(m)^d \pmod{pq}$
- Memory modification
- Glitch attacks on a particular register or area

Improvements to the attack equipment

- Replacing the photoflash with a laser pointer



- Motorized stage was required to align the chip

Countermeasures

- Top metal protection layers
  - X-rays
  - IR lasers from back side
- Self-timed dual-rail logic
  - Remove the clock to avoid clock glitch attacks
  - Be speed independent to tolerate power glitch attacks
  - Detect bad power glitches
  - Propagate *alarm* signals as part of the data:

code	meaning
00	clear
01	logic-0
10	logic-1
11	*alarm*

Conclusions

- Standard CMOS circuitry is extremely vulnerable to optical attacks
- Other memory technologies (EPROM, E^2PROM and Flash) can also be manipulated in various ways
- Top metal protection is not efficient
- Special circuit design is required to prevent optical attacks