KU LEUVEN

Black-Box Characterization of The Effects of Laser Pulses on ATmega328P

Dilip S V Kumar, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede

CARDIS 2018

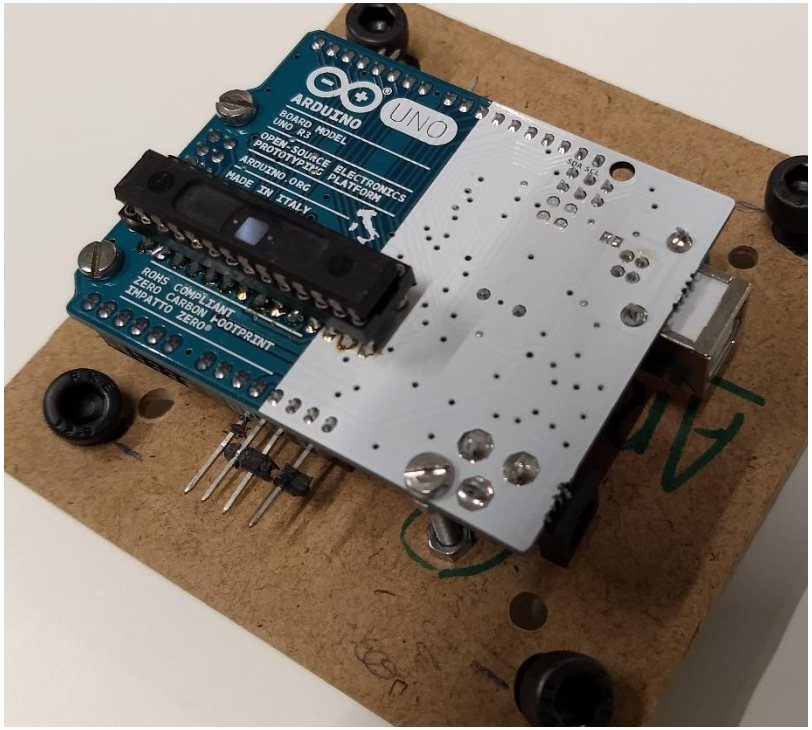
Introduction

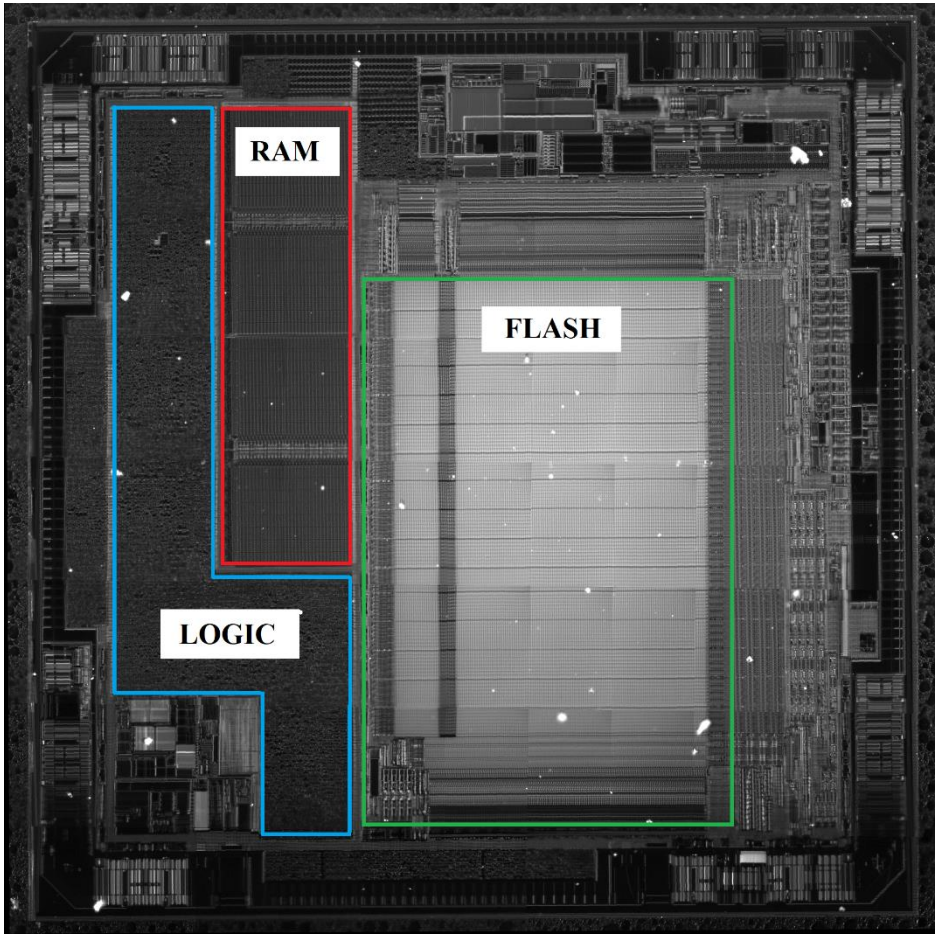
- Movitation :
  - Fault model descriptions for actual devices are rare
  - Assumed fault model for microcontroller is often instruction skip, while the reality is more complex

- Aim: find fault model for ATmega328p microcontroller

- Atmega328p is built in a rather old technology but still widely used

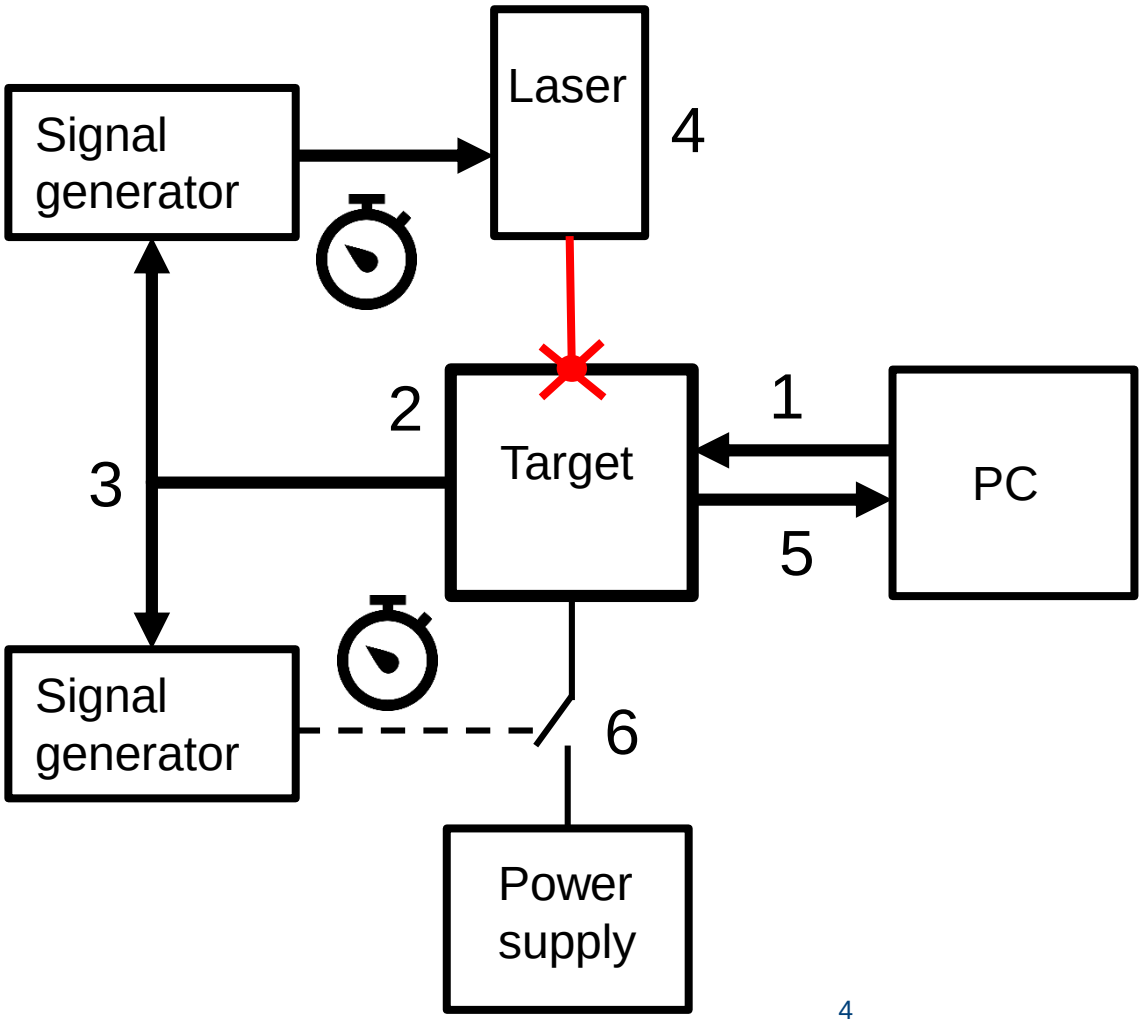
Atmega328P





KU LEUVEN

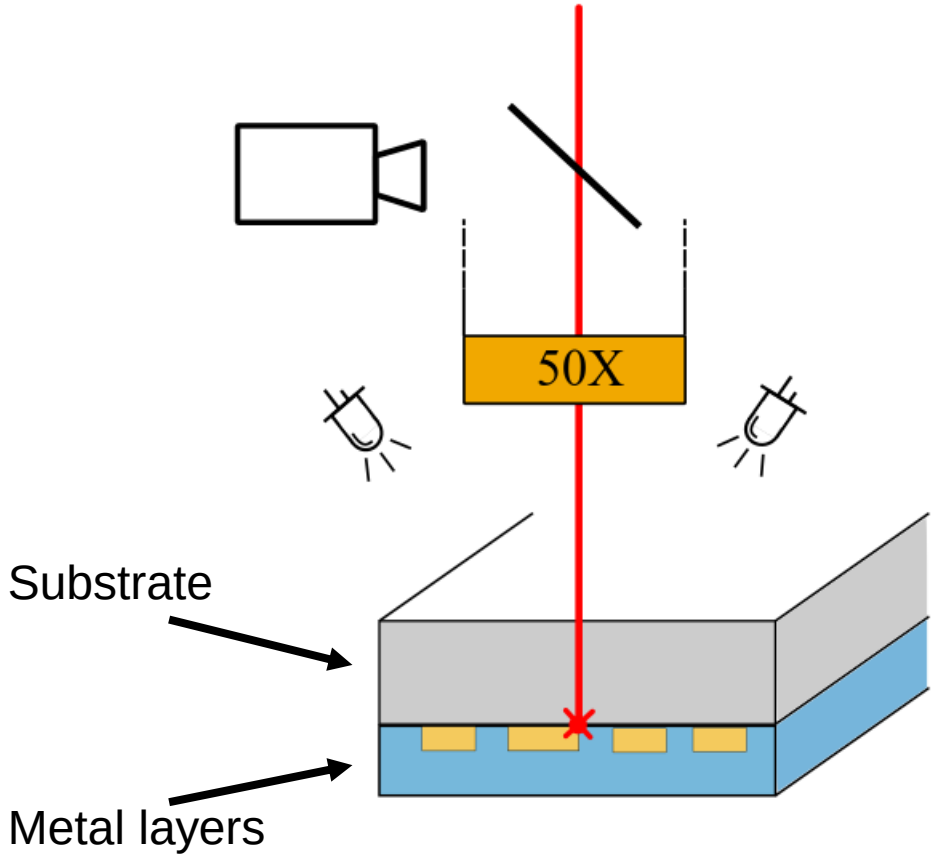
Fault injection setup



1. Start command
2. Execute target code
3. Send trigger
4. Enable laser FI
5. Send back result
6. Reset target

Laser setup

- Wavelength = 1064nm
- 50X magnification
- NIR lighting system
- XYZ stepper table, 0.1µm resolution
- Throug substrate fault injection
- CMOS NIR camera



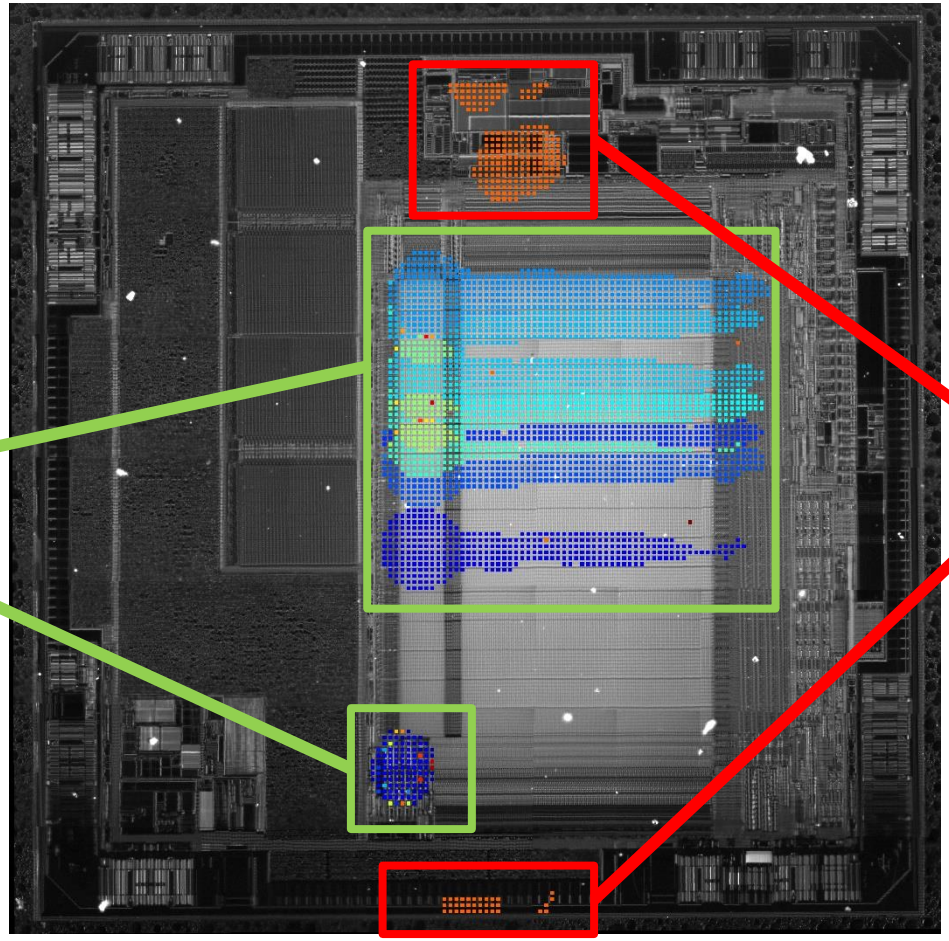
KU LEUVEN

Characterization strategy

Cycle	Instruction
1	sbi 0X0B, 7 // trigger
2	nop
3	nop
4	target
5	nop
6	nop

- ATMega328p has a two stage pipeline: fetch and execute
- Put the register file to a known state
- After laser pulse read out register file content
- After a laser pulse injection the microcontroller is always reset to a known state

Full chip scan: muls r23,r27

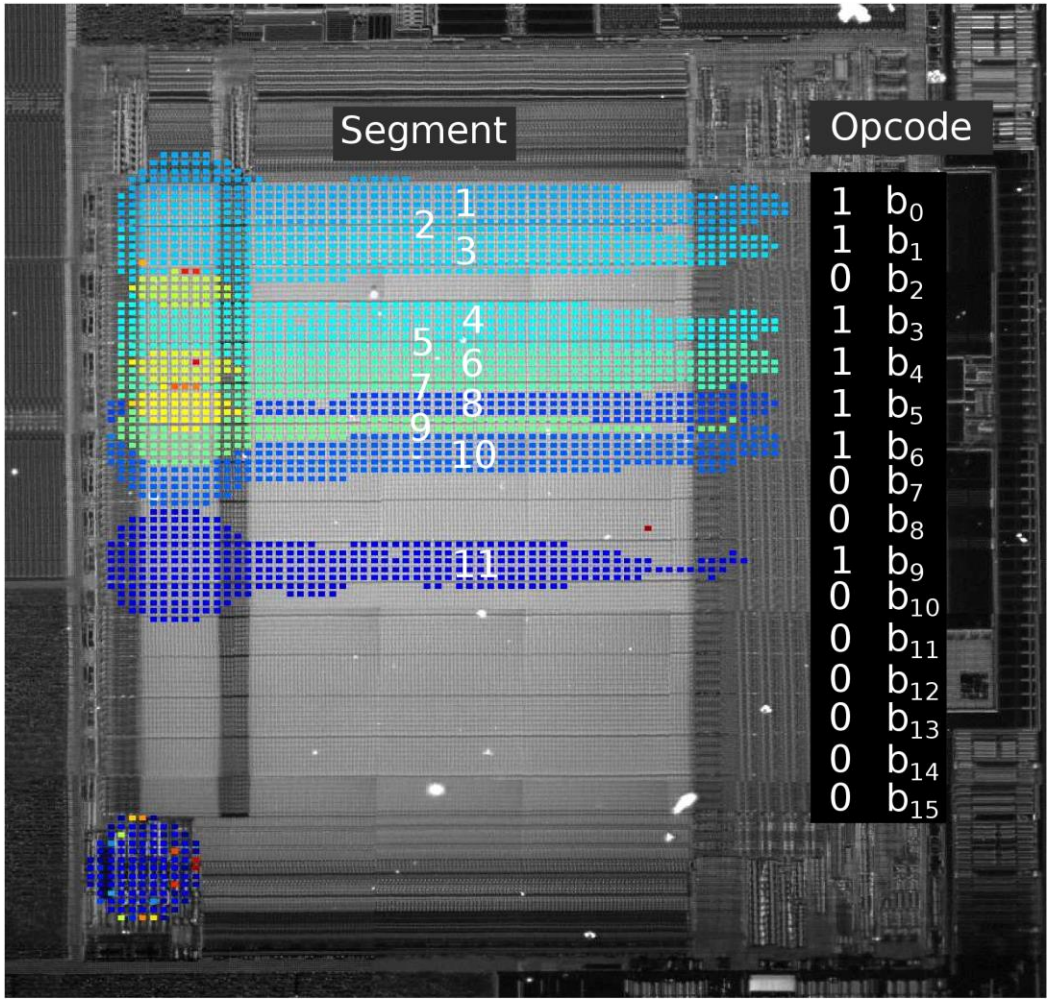


Exploitable faults

Device crashes

KU LEUVEN

Muls r23,r27

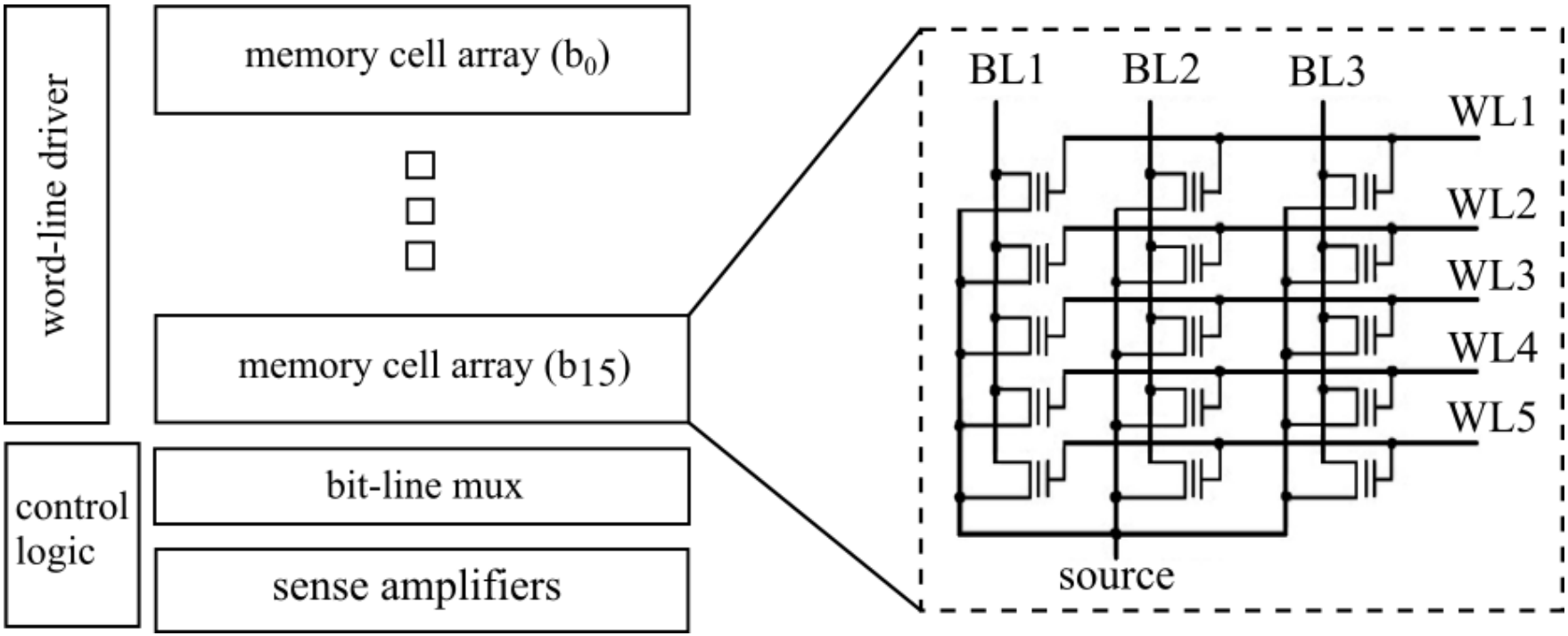


KU LEUVEN

Target instruction: muls r23,r27

Segment	Cycle	Instruction	Opcode(bin)	Bit(s) Reset
	i	nop	0000 0000 0000 0000	
	i+1	muls r23, r27	0000 0010 0111 1011	
1	i+1	muls r23, r26	0000 0010 0111 1010	b_0
2	i+1	muls r23, r24	0000 0010 0111 1000	b_0 & b_1
3	i+1	muls r23, r25	0000 0010 0111 1001	b_1
4	i+1	muls r23, r19	0000 0010 0111 0011	b_3
5	i+1	muls r22, r19	0000 0010 0110 0011	b_3 & b_4
6	i+1	muls r22, r27	0000 0010 0110 1011	b_4
7	i+1	muls r20, r27	0000 0010 0100 1011	b_4 & b_5
8	i+1	muls r21, r27	0000 0010 0101 1011	b_5
9	i+1	muls r17, r27	0000 0010 0001 1011	b_5 & b_6
10	i+1	muls r19, r27	0000 0010 0011 1011	b_6
11	i+1	nop*(Invalid)*	0000 0000 0111 1011	b_9

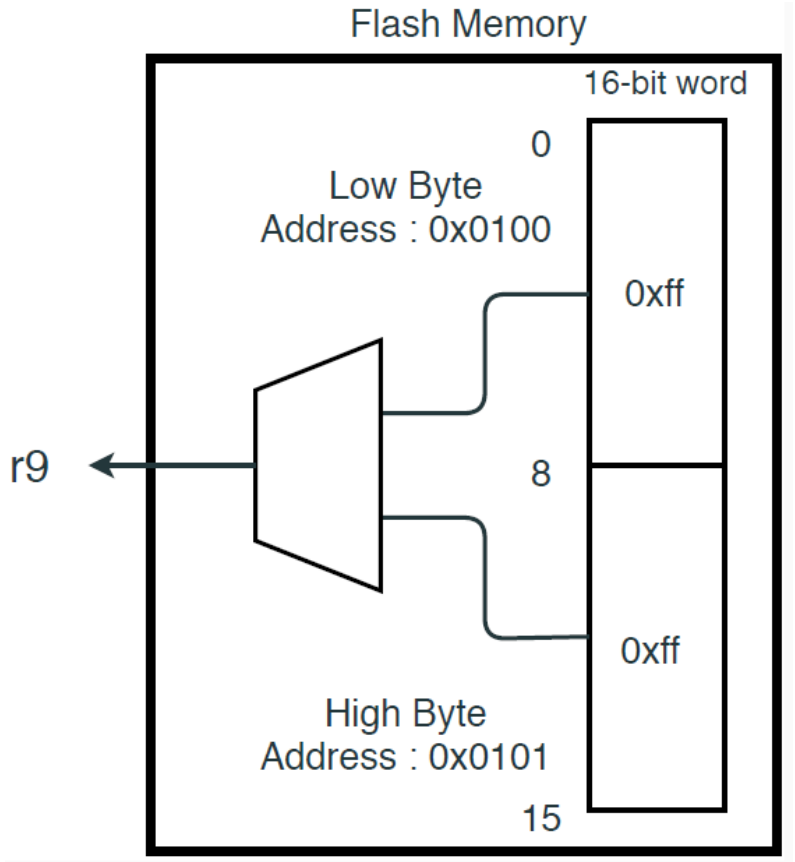
Flash memory structure



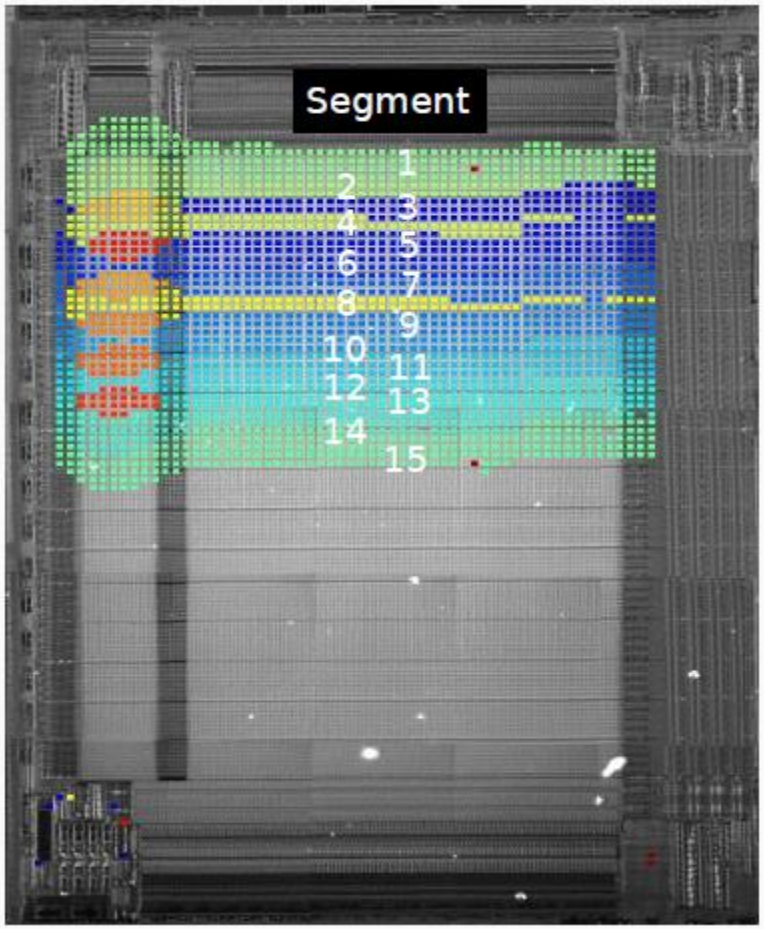
Loading data from program memory

Instruction: lpm r9, Z

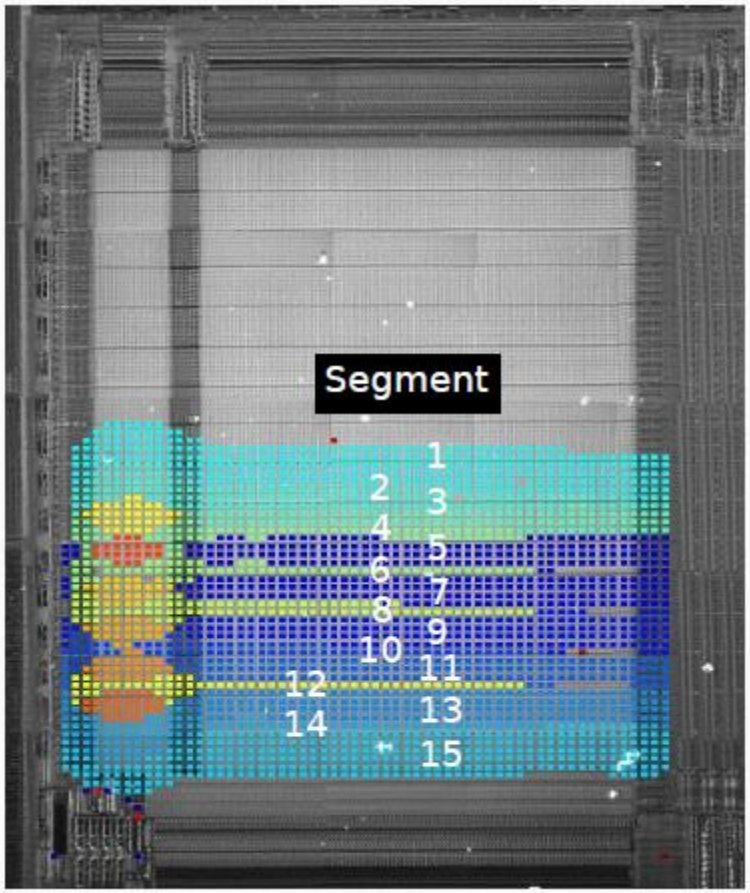
- Flash memory stores 16-bit words
- Z pointer is a byte address



Loading data from program memory

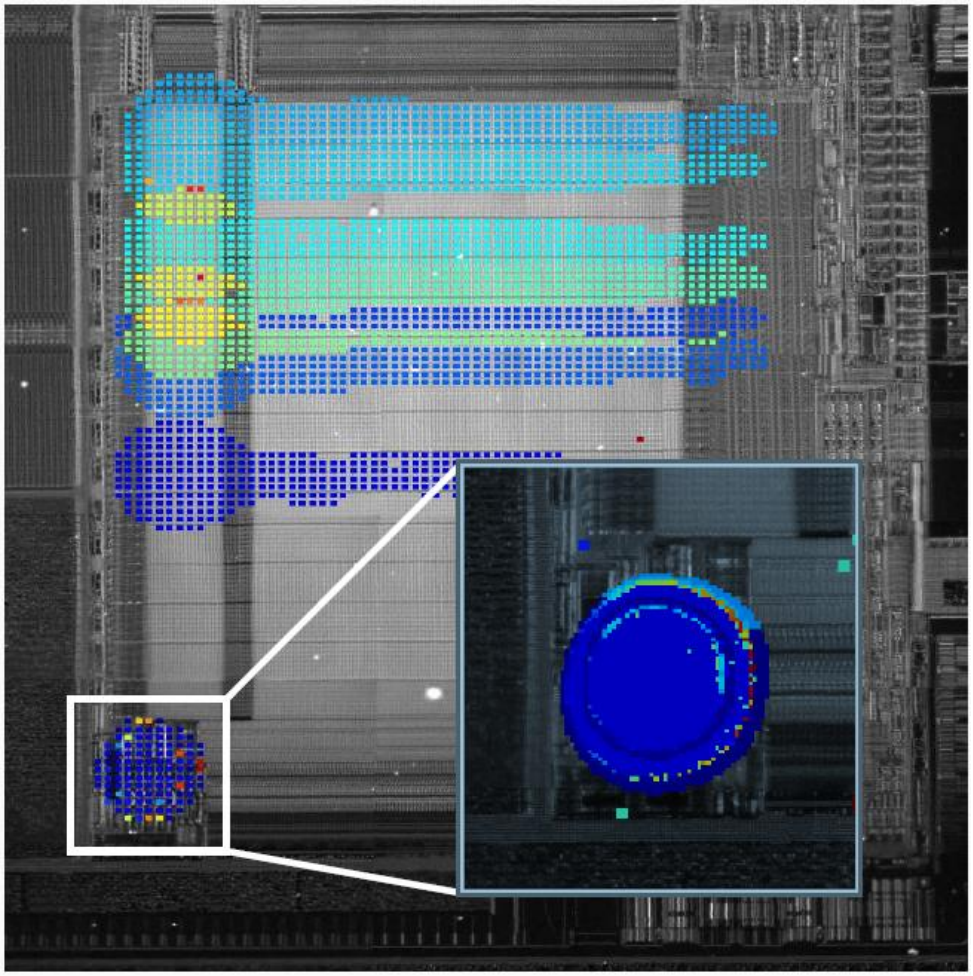


Z = 0x0100



Z = 0x0101

Second sensitive region

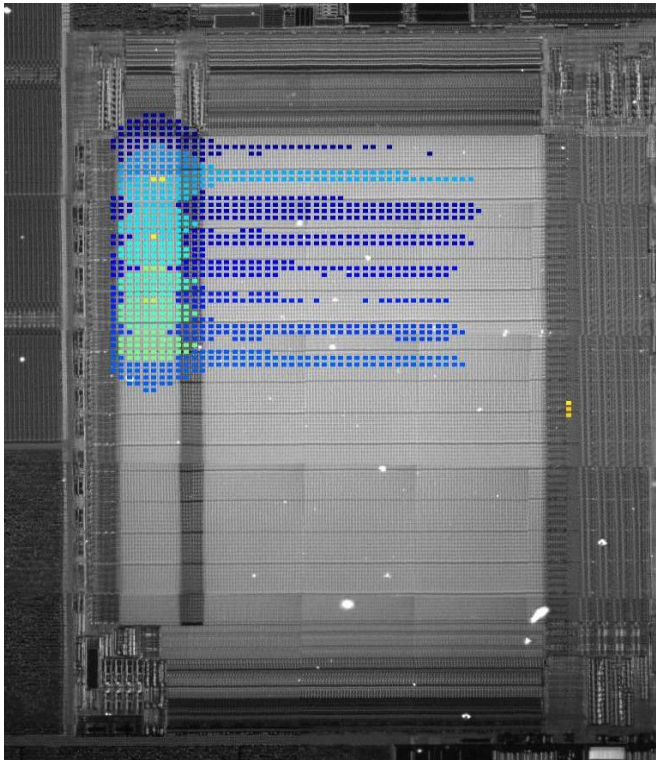


- nop
- muls r16, r16
- and r0, r16
- or r0, r18
- or r0, r16

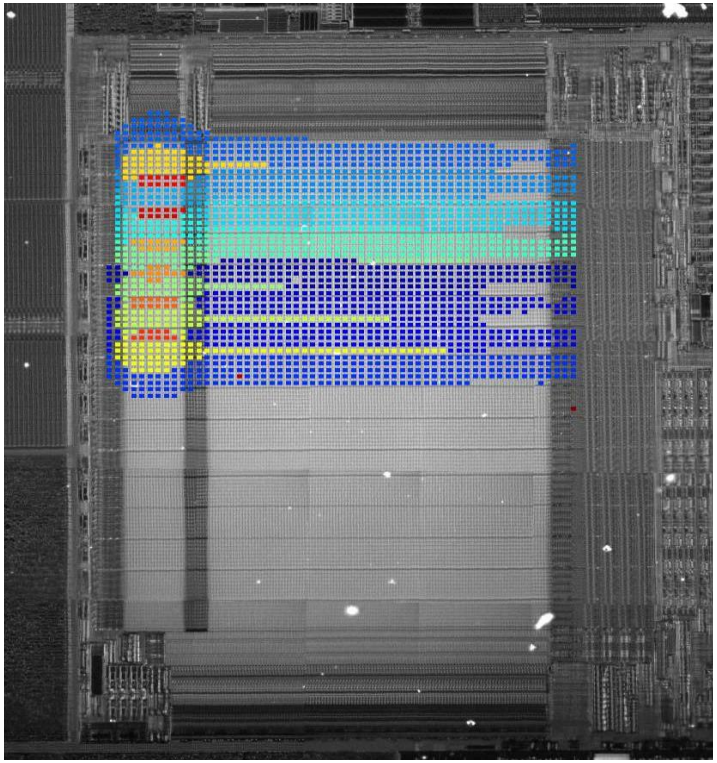
Influence laser parameters

Laser energy = pulse duration X laser power

70ns X 0.6W



70ns X 1.2W



Fault exploitation

- Fault model = stuck at 0 faults for data read out from flash memory
- No permanent faults

Program flow faults:

BRNE 1111 01kk kkkk k001
BREQ 1111 00kk kkkk k001

Data faults:

Fault loading of S-box values ➡ classical DFA

Conclusion

- Able to fault data and instructions loaded from flash memory
- The induced faults are deterministic
- An in depth knowledge of the fault model can lead to powerfull attacks

Questions?

KU LEUVEN