Clock Glitch Attacks in the Presence of Heating

Barış Ege[1], Thomas Korak[2], Michael Hutter[2] and Lejla Batina[1]

[1] *Radboud University Nijmegen, ICIS – Digital Security Group, The Netherlands*

[2] *Graz University of Technology IAIK, Austria*

Previous Work

CLOCK GLITCHING

TEMPERATURE

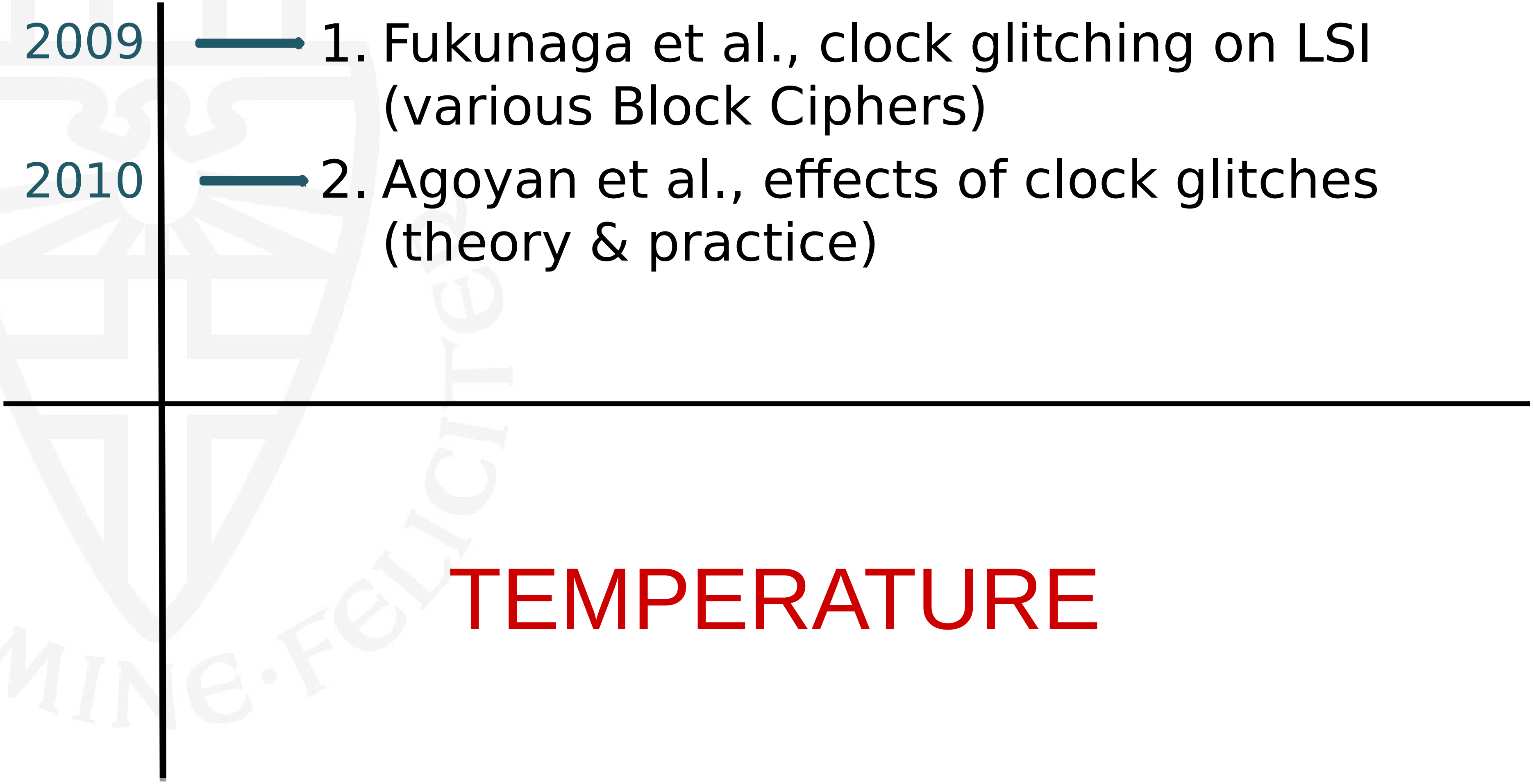
Previous Work

2009

1. Fukunaga et al., clock glitching on LSI (various Block Ciphers)

TEMPERATURE

Previous Work



2009

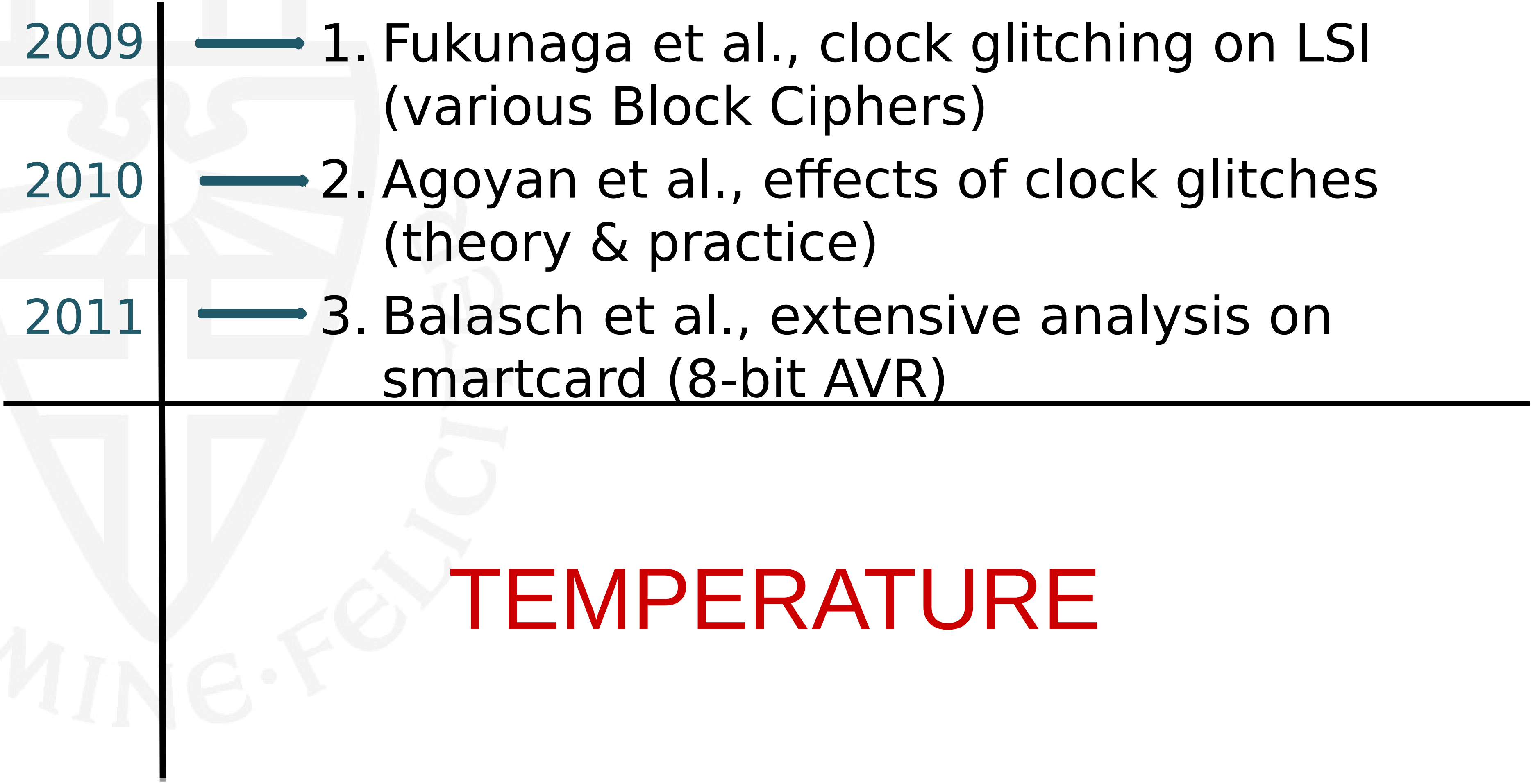
1. Fukunaga et al., clock glitching on LSI (various Block Ciphers)

2010

2. Agoyan et al., effects of clock glitches (theory & practice)

TEMPERATURE

Previous Work



2009

1. Fukunaga et al., clock glitching on LSI (various Block Ciphers)

2010

2. Agoyan et al., effects of clock glitches (theory & practice)

2011

3. Balasch et al., extensive analysis on smartcard (8-bit AVR)

TEMPERATURE

Previous Work

2009

1. Fukunaga et al., clock glitching on LSI (various Block Ciphers)

2010

2. Agoyan et al., effects of clock glitches (theory & practice)

2011

3. Balasch et al., extensive analysis on smartcard (8-bit AVR)

2002

4. Quisquater & Samyde, memory errors by extensive heating

Previous Work

2009 1. Fukunaga et al., clock glitching on LSI (various Block Ciphers)

2010 2. Agoyan et al., effects of clock glitches (theory & practice)

2011 3. Balasch et al., extensive analysis on smartcard (8-bit AVR)

2002 4. Quisquater & Samyde, memory errors by extensive heating

2003 5. Govindavajhala & Appel, memory errors by a 50W lamp

Previous Work

2009 → 1. Fukunaga et al., clock glitching on LSI (various Block Ciphers)

2010 → 2. Agoyan et al., effects of clock glitches (theory & practice)

2011 → 3. Balasch et al., extensive analysis on smartcard (8-bit AVR)

2002 → 4. Quisquater & Samyde, memory errors by extensive heating

2003 → 5. Govindavajhala & Appel, memory errors by a 50W lamp

2013 → 6. Hutter & Schmidt, temperature attack on RSA (temp. > 125°)

What's to come?

What's to come?

- Increased Temp. —> new faults

What's to come?

- Increased Temp. —> new faults
- Increased Temp. —> increased time frame

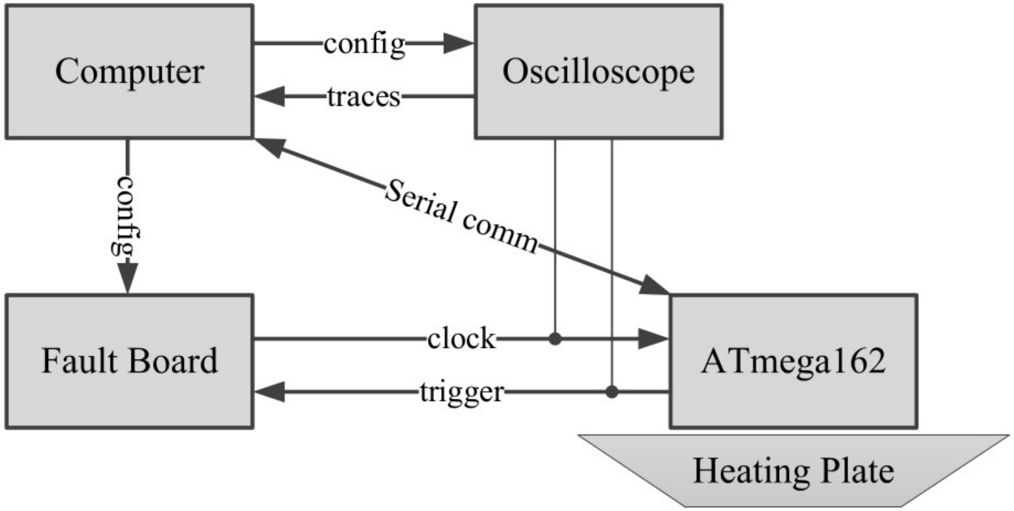
What's to come?

- Increased Temp. —> new faults
- Increased Temp. —> increased time frame
- Insert new instructions to program flow
  - Repeat instructions within the program flow

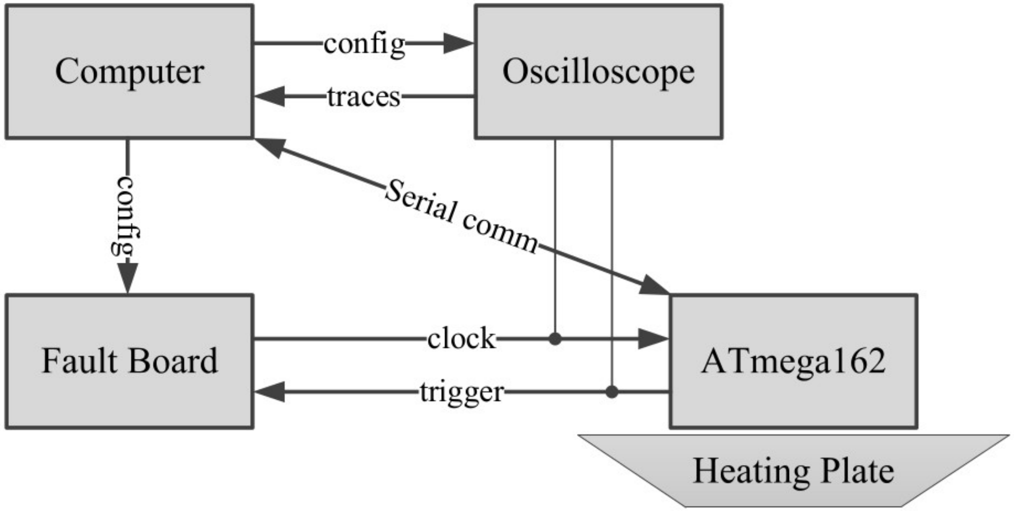
Outline

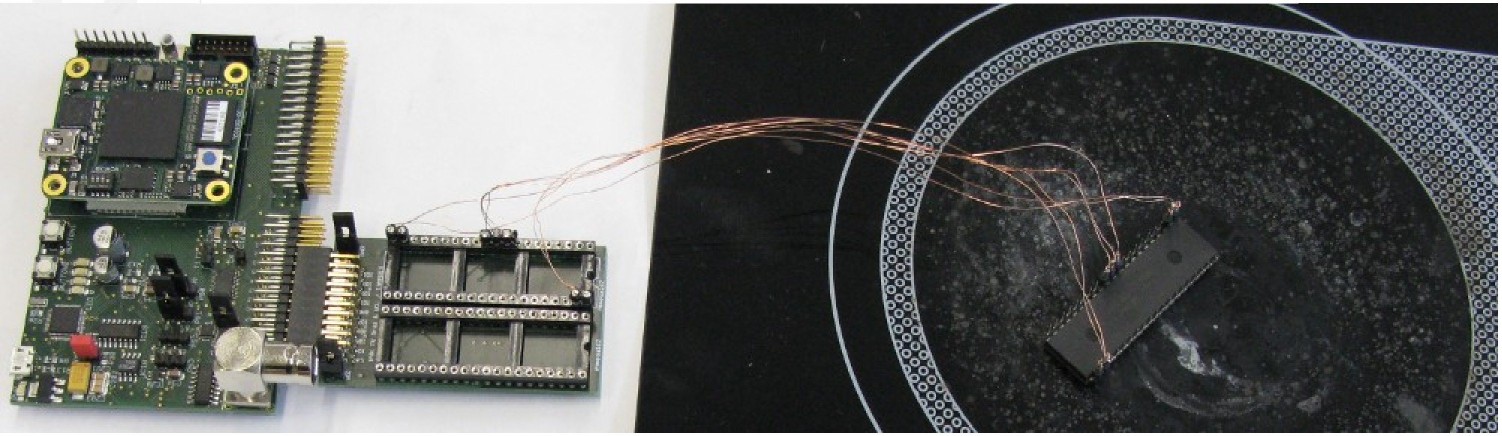
- Experimental setup
  - Glitch generation
  - Evaluation process
- Results
  - Types of faults generated
  - Effect of heat
- Summary

Experimental Setup



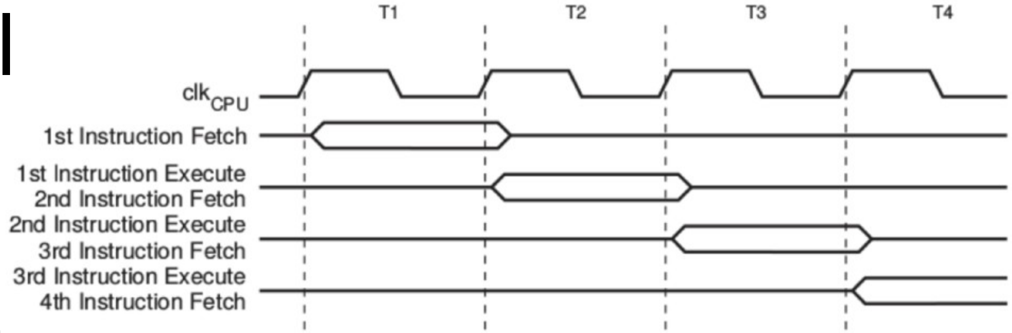
Experimental Setup





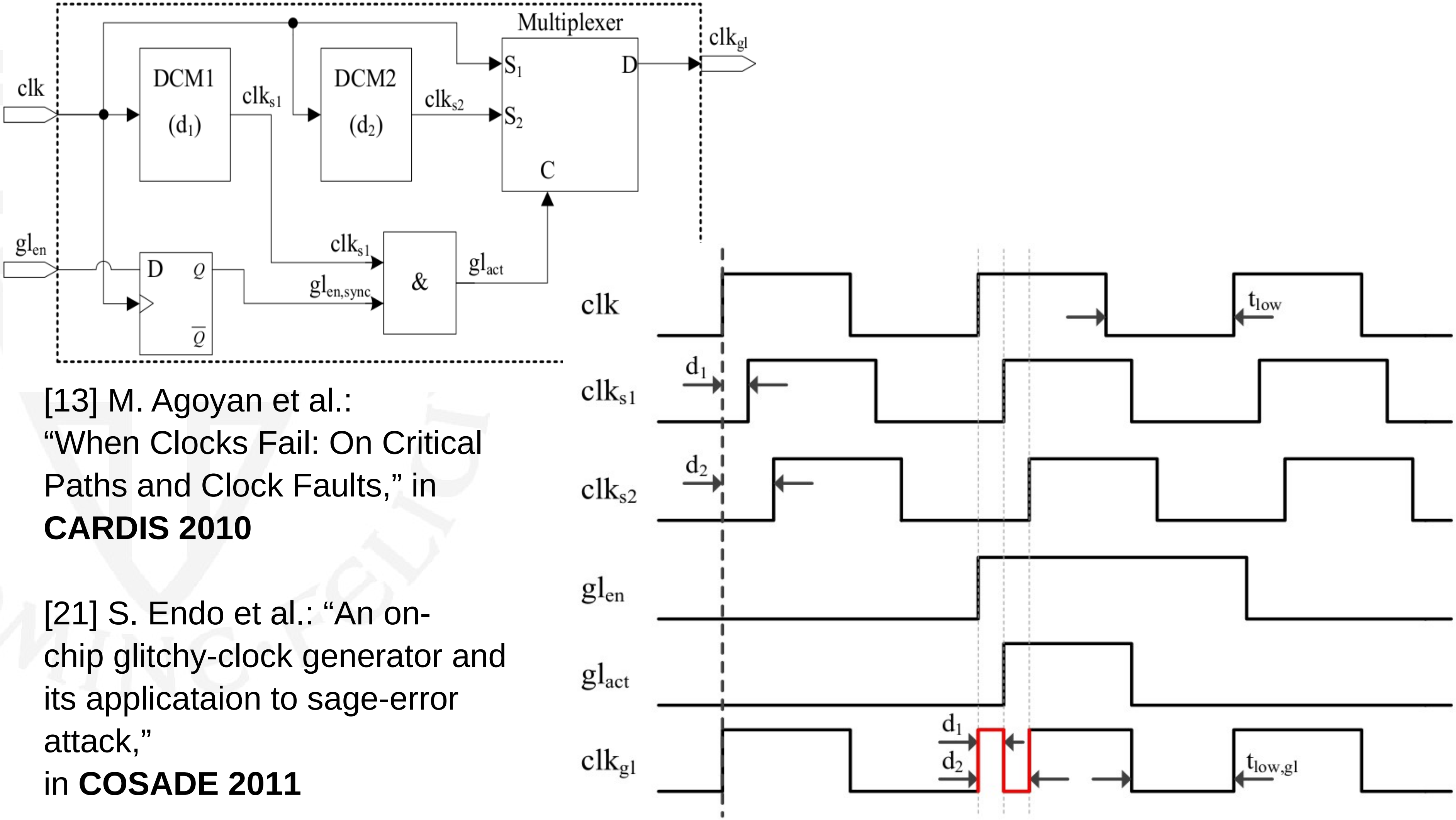
Target Microcontroller

- 8 – bit AVR
- 32 internal general purpose registers
- Up to 16 MHz with external clock



[*}http://www.atmel.com/Images/Atmel-2513-8-bit-AVR-Microntroller-ATmega162_Datasheet.pdf

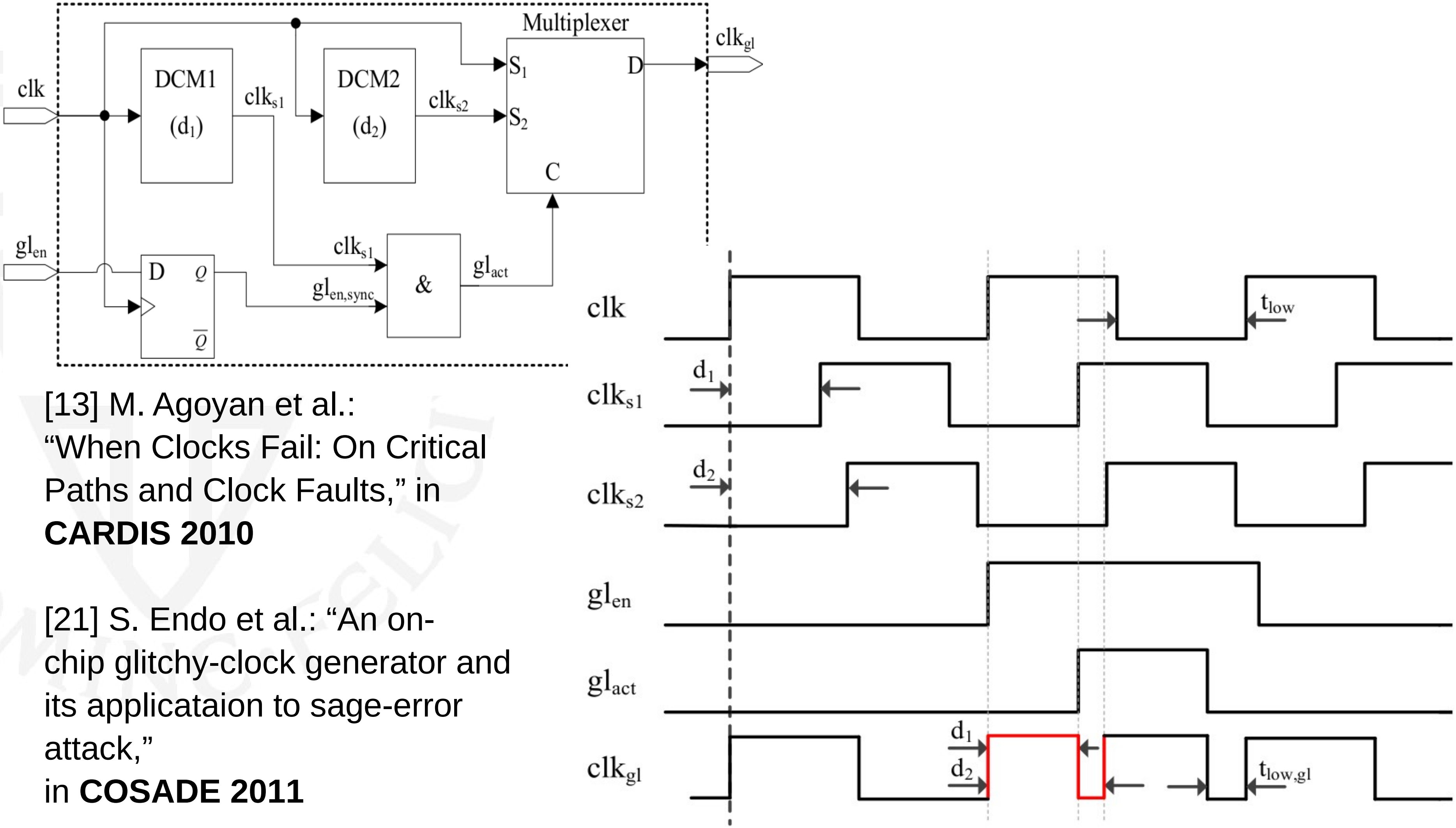
Glitch Generation



[13] M. Agoyan et al.:
“When Clocks Fail: On Critical Paths and Clock Faults,” in **CARDIS 2010**

[21] S. Endo et al.: “An on-chip glitchy-clock generator and its applicataion to sage-error attack,”
in **COSADE 2011**

Glitch Generation



[13] M. Agoyan et al.:
“When Clocks Fail: On Critical Paths and Clock Faults,” in
CARDIS 2010

[21] S. Endo et al.: “An on-chip glitchy-clock generator and its applicataion to sage-error attack,”
in **COSADE 2011**

Evaluation Process

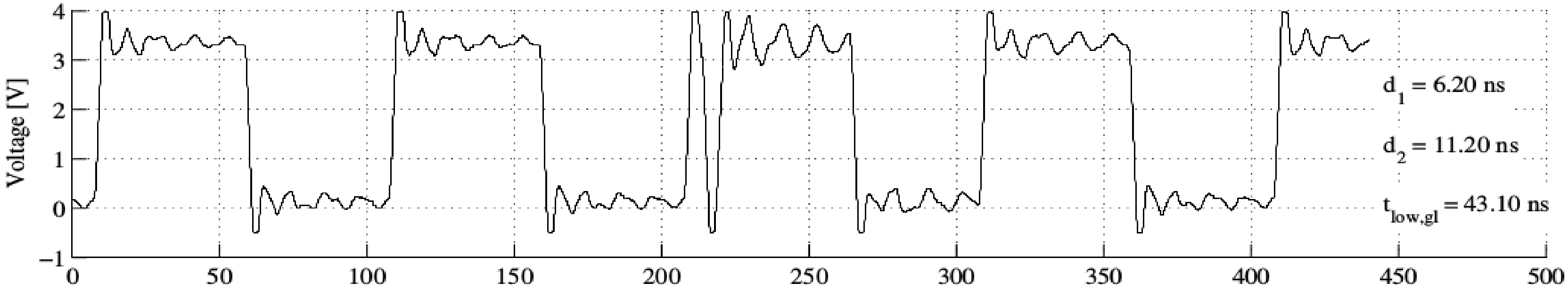
Evaluation Process

- Wrap '`Inst`' between '`NOP`' instructions
- Induce clock glitch at execution phase
- Read out entire register bank

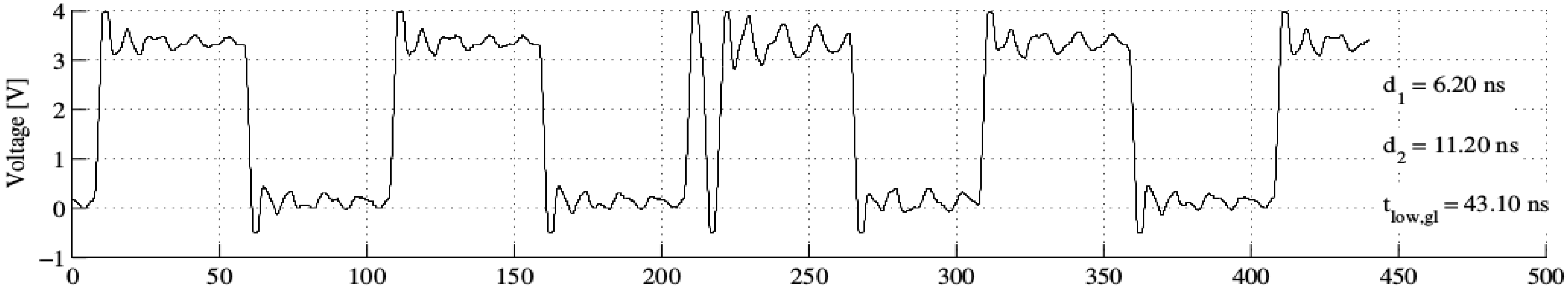
Evaluation Process

- Initialize registers with another known set
- Wrap '`Inst`' between '`NOP`' instructions
- Induce clock glitch at execution phase
- Read out entire register bank

Types of Faults – 1 (Inc.)

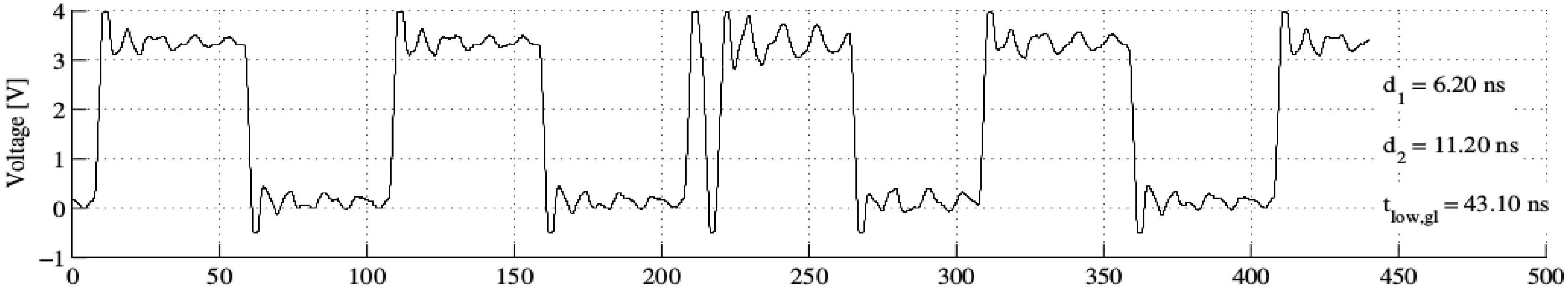


Types of Faults – 1 (Inc.)



```
reg_12 = 108
reg_13 = 109
reg_14 = 110
reg_15 = 111
reg_16 = 102
reg_17 = 0
reg_18 = 114
reg_19 = 115
reg_20 = 116
reg_21 = 117
```

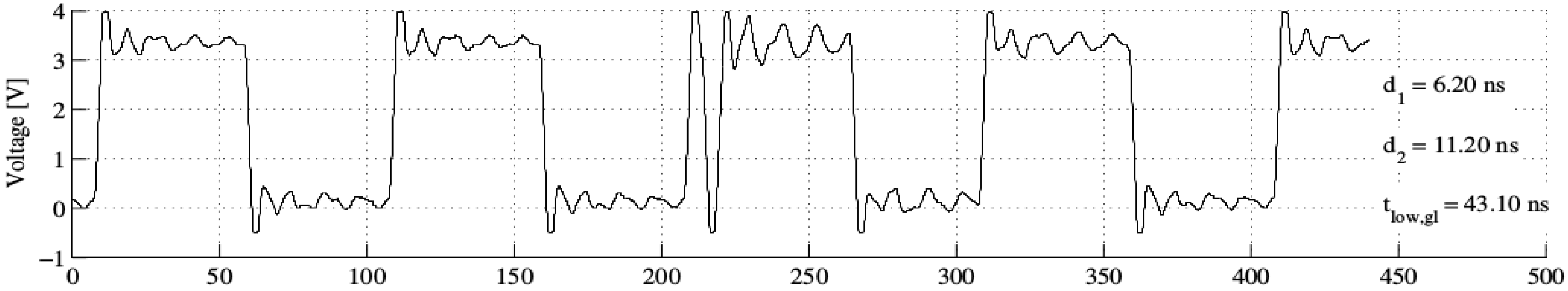
Types of Faults – 1 (Inc.)



```
reg_12 = 108
reg_13 = 109
reg_14 = 110
reg_15 = 111
reg_16 = 102
reg_17 = 0
reg_18 = 114
reg_19 = 115
reg_20 = 116
reg_21 = 117
```

```
reg_12 = 108
reg_13 = 109
reg_14 = 110
reg_15 = 111
reg_16 = 148
reg_17 = 0
reg_18 = 114
reg_19 = 115
reg_20 = 116
reg_21 = 117
```

Types of Faults – 1 (Inc.)



reg_12 = 108
reg_13 = 109
reg_14 = 110
reg_15 = 111
reg_16 = 102
reg_17 = 0
reg_18 = 114
reg_19 = 115
reg_20 = 116
reg_21 = 117

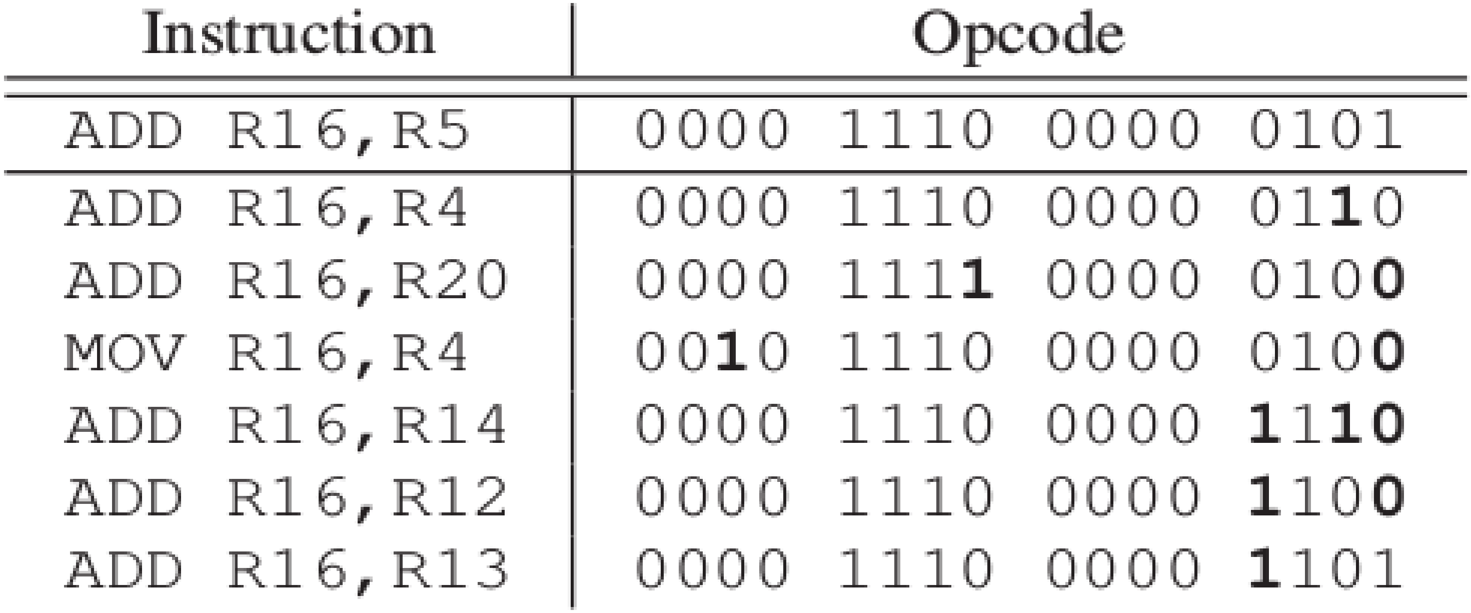
reg_12 = 108
reg_13 = 109
reg_14 = 110
reg_15 = 111
reg_16 = 148
reg_17 = 0
reg_18 = 114
reg_19 = 115
reg_20 = 116
reg_21 = 117

reg_14 = 110
reg_15 = 111
reg_16 = 112
reg_17 = 113
reg_18 = 102
reg_19 = 99
reg_20 = 116
reg_21 = 117
reg_22 = 118
reg_23 = 119

Types of Faults – 2 (Mod.)

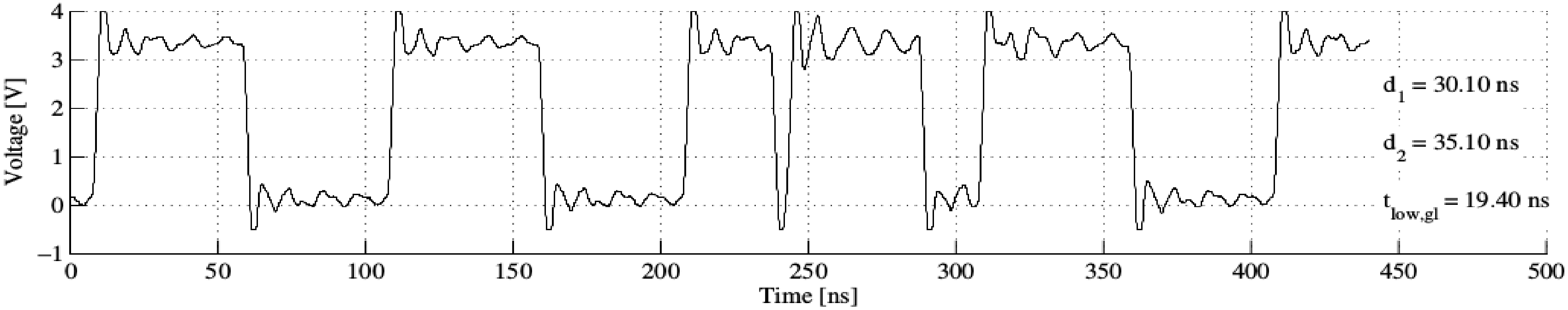
- Modified instructions similar to the ones observed by Balasch et al. in FDTC'11 [6]

- Note! Glitch is induced in execution phase unlike [6]



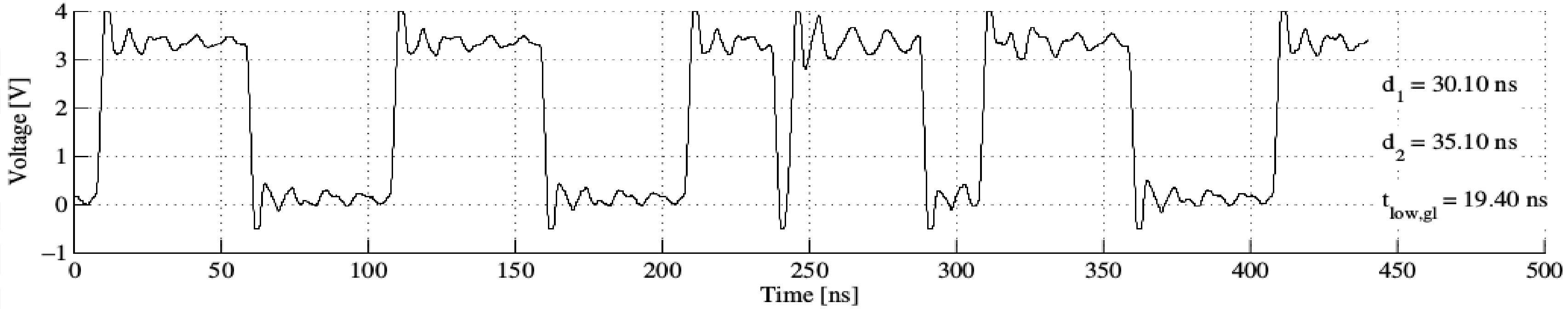
Instruction	Opcode
ADD R16,R5	0000 1110 0000 0101
ADD R16,R4	0000 1110 0000 01**1**0
ADD R16,R20	0000 111**1** 0000 010**0**
MOV R16,R4	00**1**0 1110 0000 010**0**
ADD R16,R14	0000 1110 0000 **1**110
ADD R16,R12	0000 1110 0000 **1**10**0**
ADD R16,R13	0000 1110 0000 **1**101

Types of Faults – 3 (Repeat)



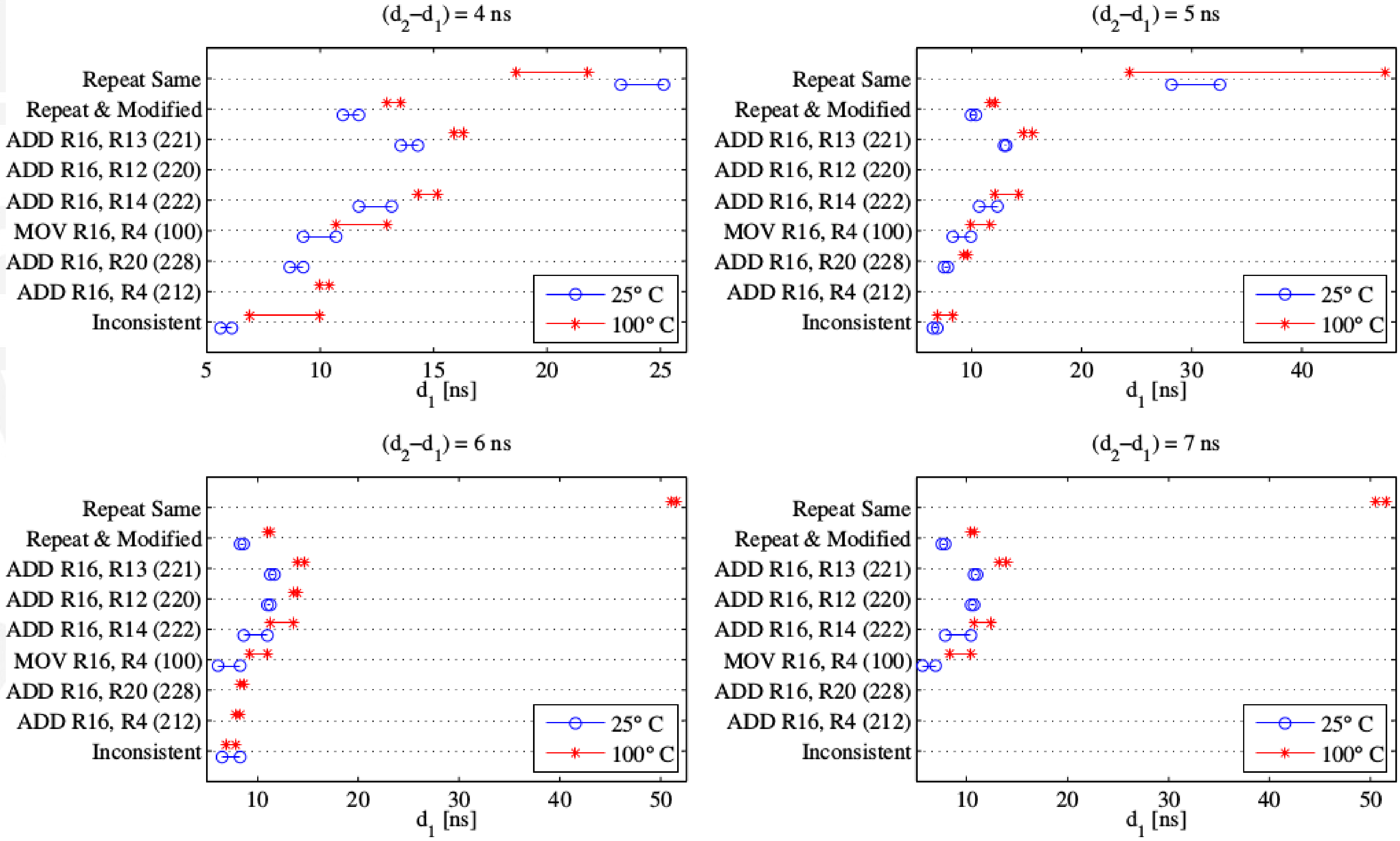
Program Counter	Instruction	Value of `R16`
n-1	`NOP`	112
n	`ADD R16, R5`	213
n+1	`ADD R16, R21`	74
n+2	`CLR R4`	74
n+3	`LDI R18, 0xFF`	74
n+4	`NOP`	74
n+5	`NOP`	74

Types of Faults – 4 (Repeat)

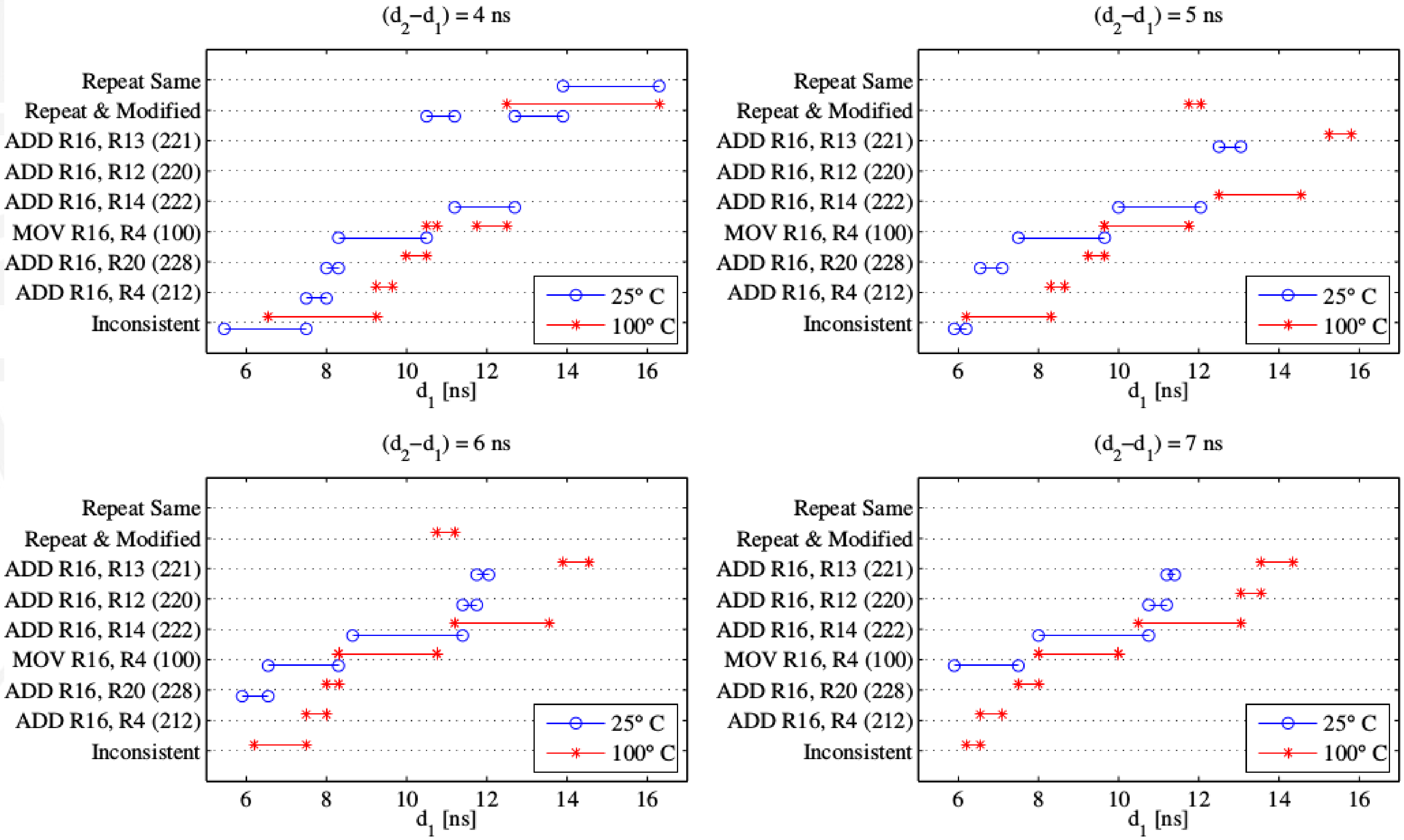


Program Counter	Instruction	Value of `R16`
n-1	`NOP`	112
n	`ADD R16, R5`	213
n	`ADD R16, R5`	58
n+1	`ADD R16, R21`	175
n+2	`CLR R4`	175
n+3	`LDI R18, 0xFF`	175
n+4	`NOP`	175

Results (10 MHz)



Results (20 MHz)



Summary

- First work investigating combined glitch and thermo attacks
  - Performed experiments on an 8-bit AVR
- Some types of faults are easier to induce due to increased time frame with heat

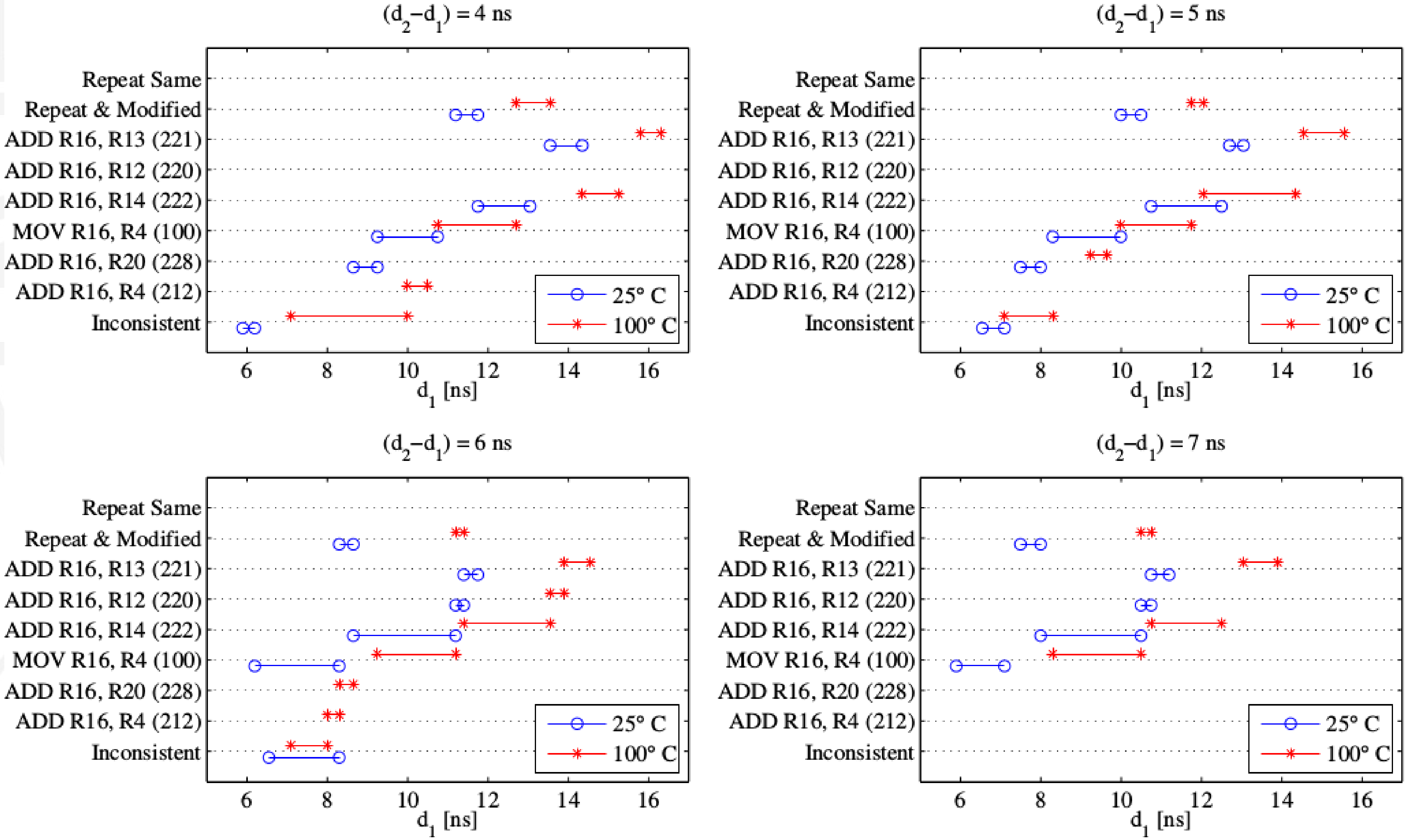
Thank you!

Questions?

Barış Ege
Digital Security Group (ICIS)

Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands
✉ *B.Ege@cs.ru.nl* 🏠 *www.cs.ru.nl/B.Ege*

Appendix – A


(d_2–d_1) = 4 ns
(d_2–d_1) = 5 ns
(d_2–d_1) = 6 ns
(d_2–d_1) = 7 ns
Repeat Same
Repeat & Modified
ADD R16, R13 (221)
ADD R16, R12 (220)
ADD R16, R14 (222)
MOV R16, R4 (100)
ADD R16, R20 (228)
ADD R16, R4 (212)
Inconsistent
6
8
10
12
14
16
d_1 [ns]
25° C
100° C