Characterizing and Modeling Clock-Glitch Fault Injection

Amélie Marotta

Ronan Lashermes, Olivier Sentieys, Rachid Dafali, Guillaume Bouffard

amelie.marotta@inria.fr

Goals

→ Electromagnetic fault injection has an impact on clock signals [1]

→ TRAITOR, a many-fault injection tool, that uses clock glitches, recreates this impact

⇒ Which fault model apply to TRAITOR ?

[1] (Electromagnetic fault injection: the curse of flip-flops, Sébastien Ordas, Ludovic Guillaume-Sage, Philippe Maurine)

Goals

Fault model at:

Goals

Fault model at:

- microarchitecture level
  - $\rightarrow$ program execution

Goals

Fault model at:

- microarchitecture level
  → program execution

- register-transfer level
  → bit-flip, stuck-at-0 or -1

Goals

Fault model at:

- microarchitecture level
  → program execution

- register-transfer level
  → bit-flip, stuck-at-0 or -1

- physical level
  → logic gates, registers

Goals

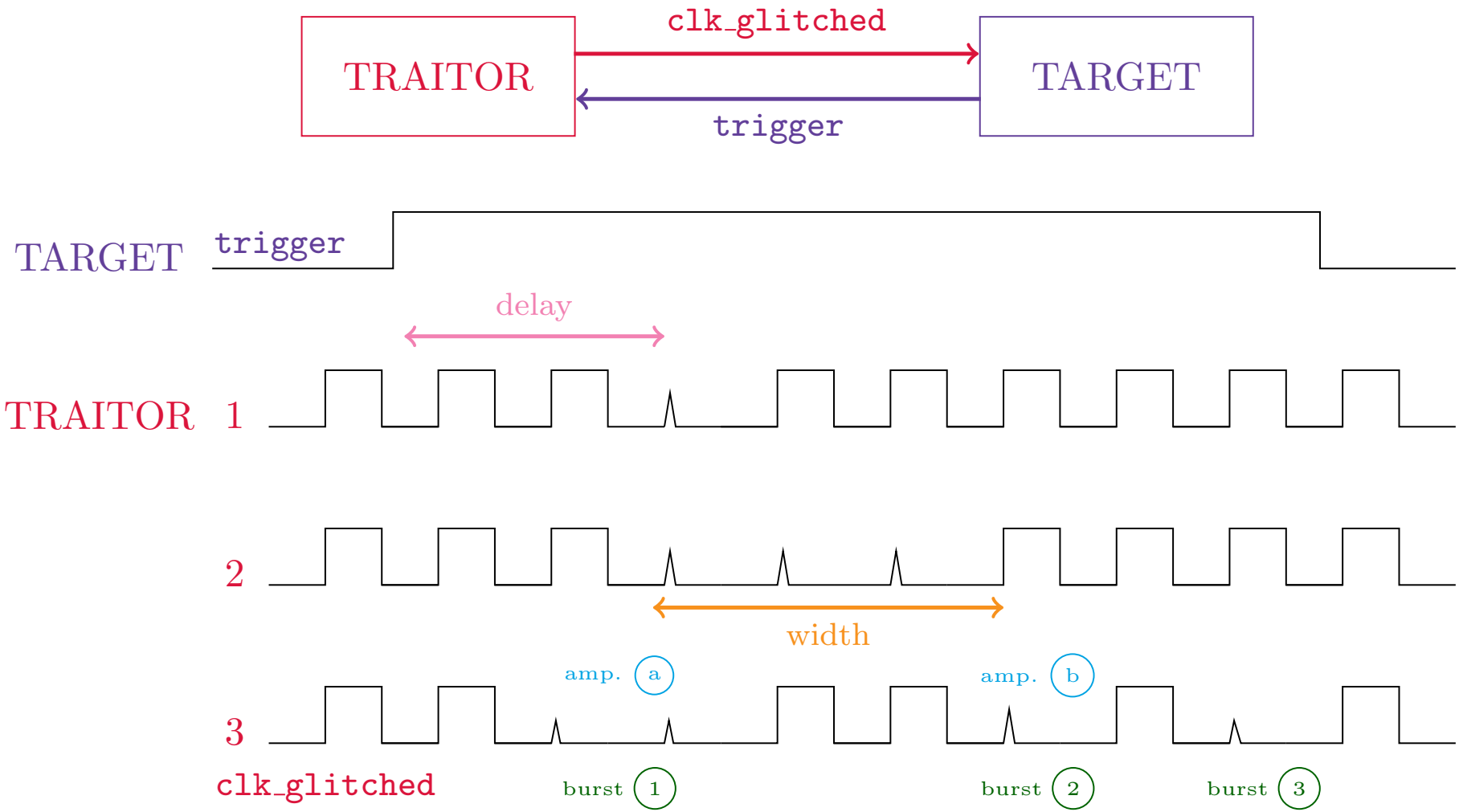
Fault model at:

- microarchitecture level
  → program execution

- register-transfer level
  → bit-flip, stuck-at-0 or -1

- physical level
  → logic gates, registers

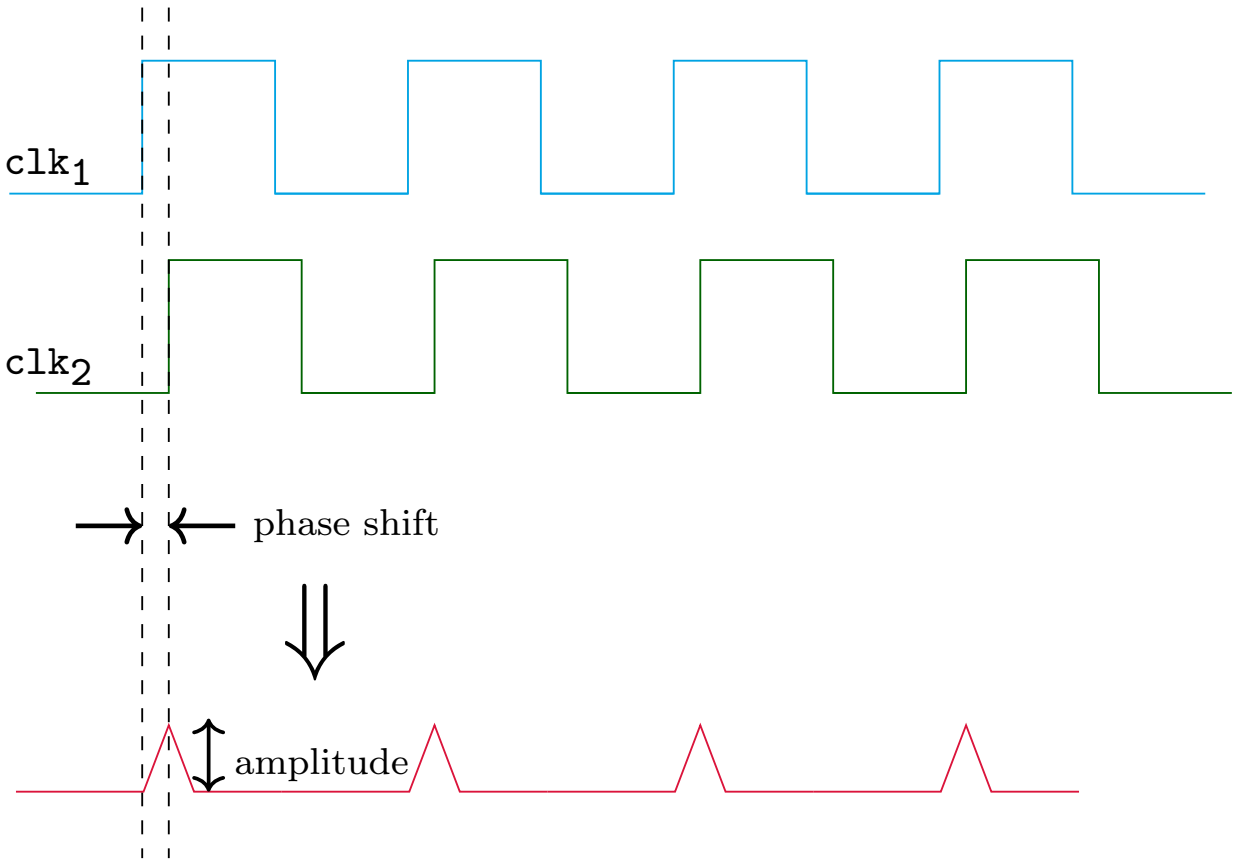
TRAITOR



TRAITOR: A Low-Cost Evaluation Platform for Multifault Injection. Ludovic Claudepierre, Pierre-Yves Péneau, Damien Hardy, Erven Rohou.

TRAITOR

Generation of `clk_glitched`:



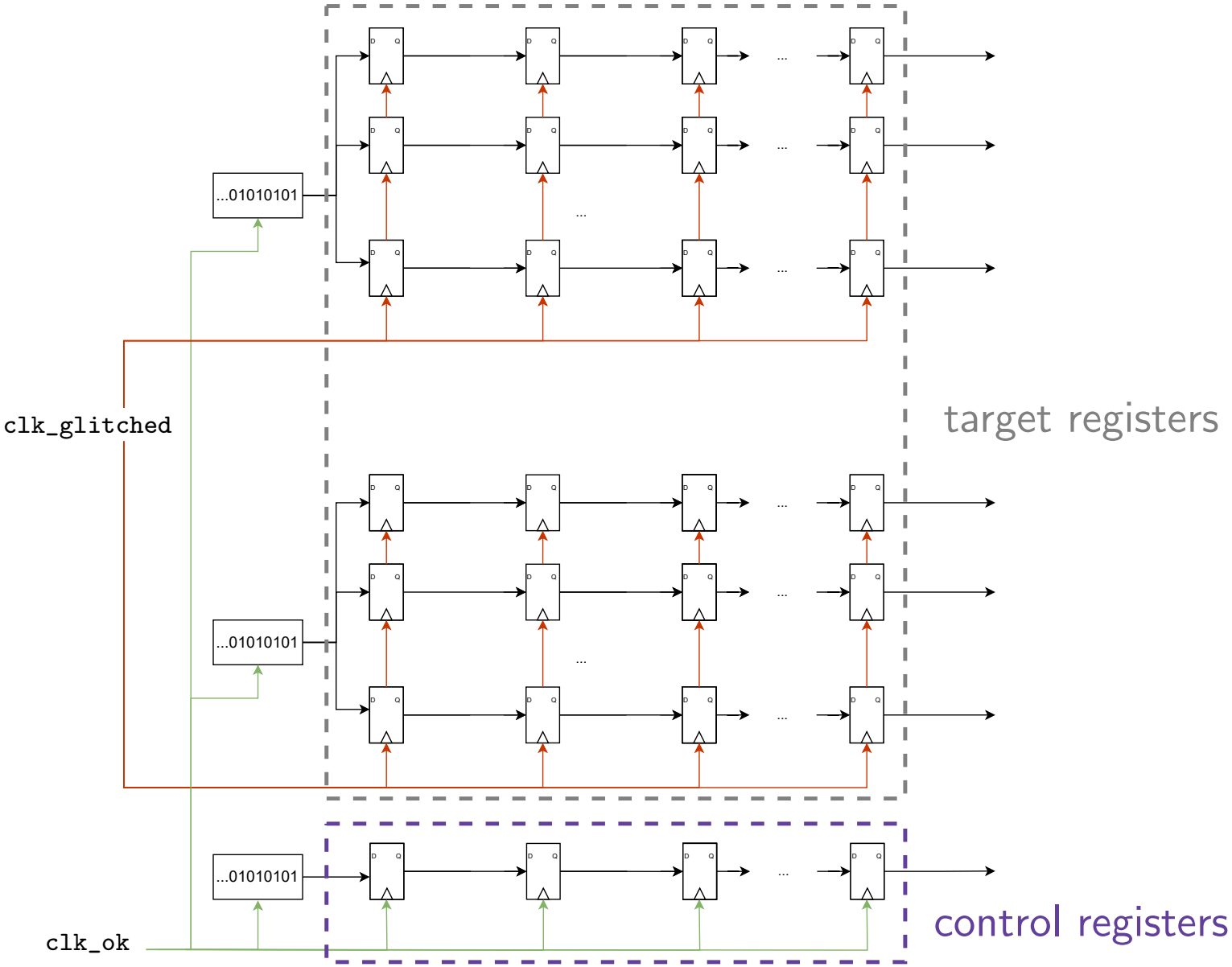
$$\texttt{clk\_glitched} = (\texttt{clk}_1 \hat{} \texttt{clk}_2) \,\&\, \texttt{clk}_1$$

TRAITOR: A Low-Cost Evaluation Platform for Multifault Injection. Ludovic Claudepierre, Pierre-Yves Péneau, Damien Hardy, Erven Rohou.

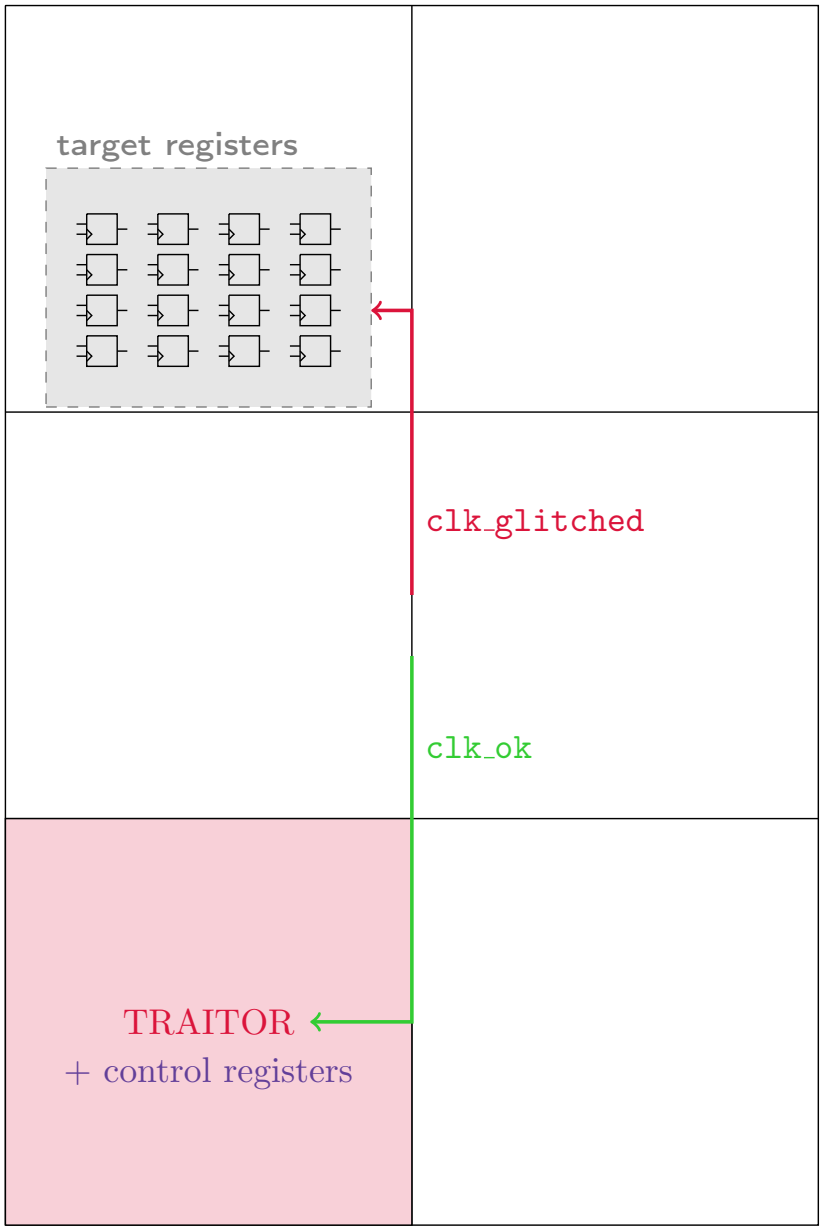
TRAITOR


MSO8204 Mon March 13 11:48:56 2023
RIGOL
STOP
H 50.0ns 2.5GSa/s 1.25kpts
MEASURE
STOP/RUN
D 150.5ns
T 2 1.76V A
1 1.00V 0.00V
2 1.00V -2.44V
3 100mV 0.00V
4 100mV 0.00V
L 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
11:48

Design under test



Design under test

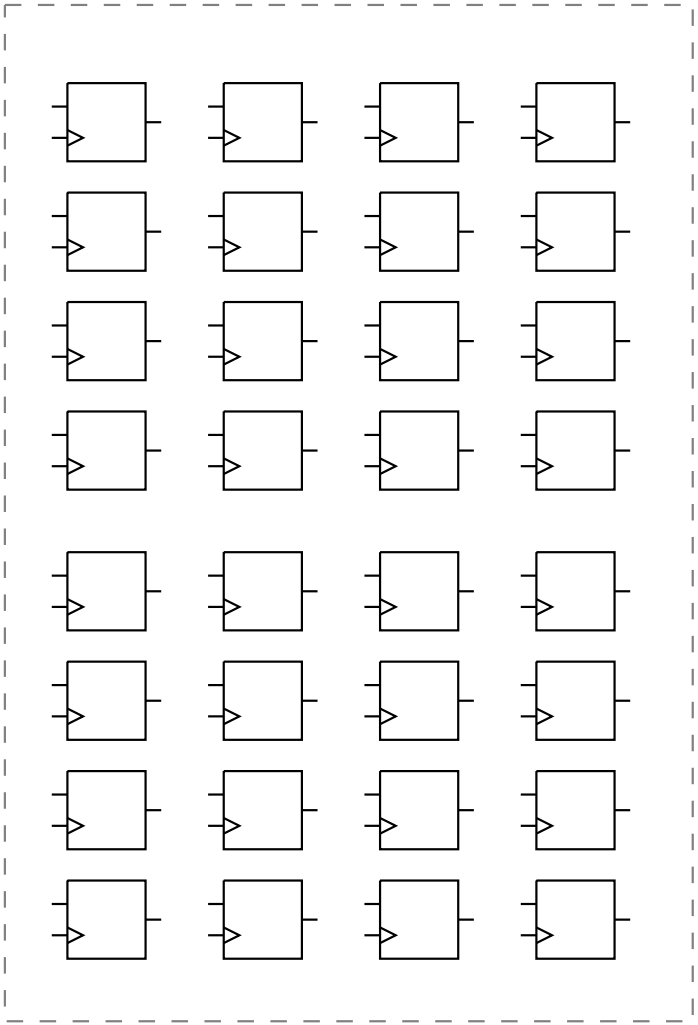


Experiment set-up:

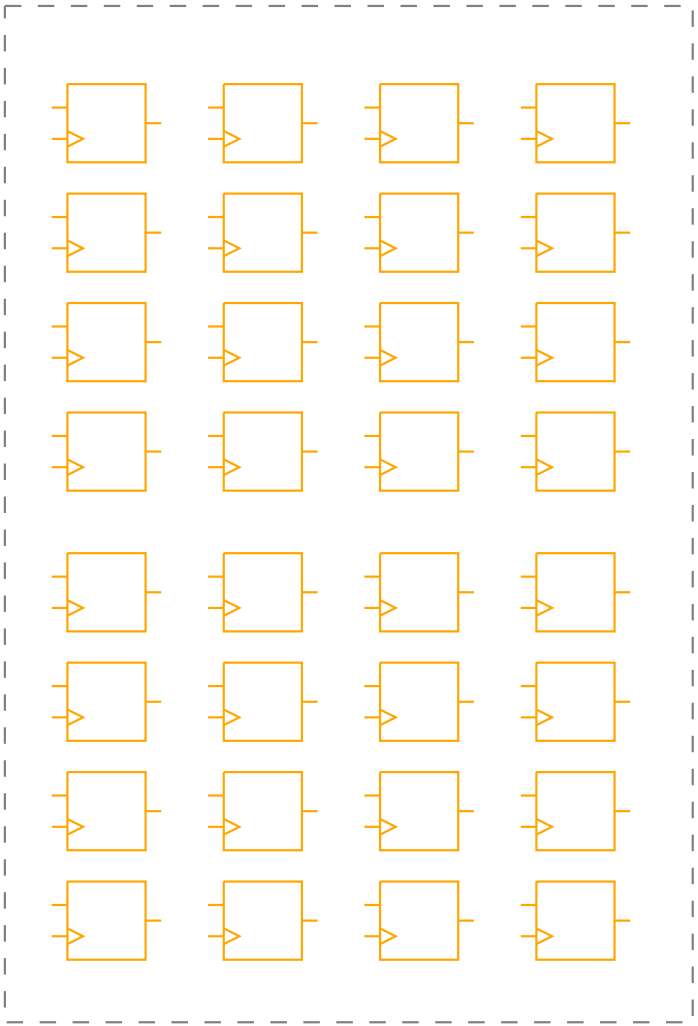
→ Artix-7

→ faults injected from `amp. 0`

Design under test

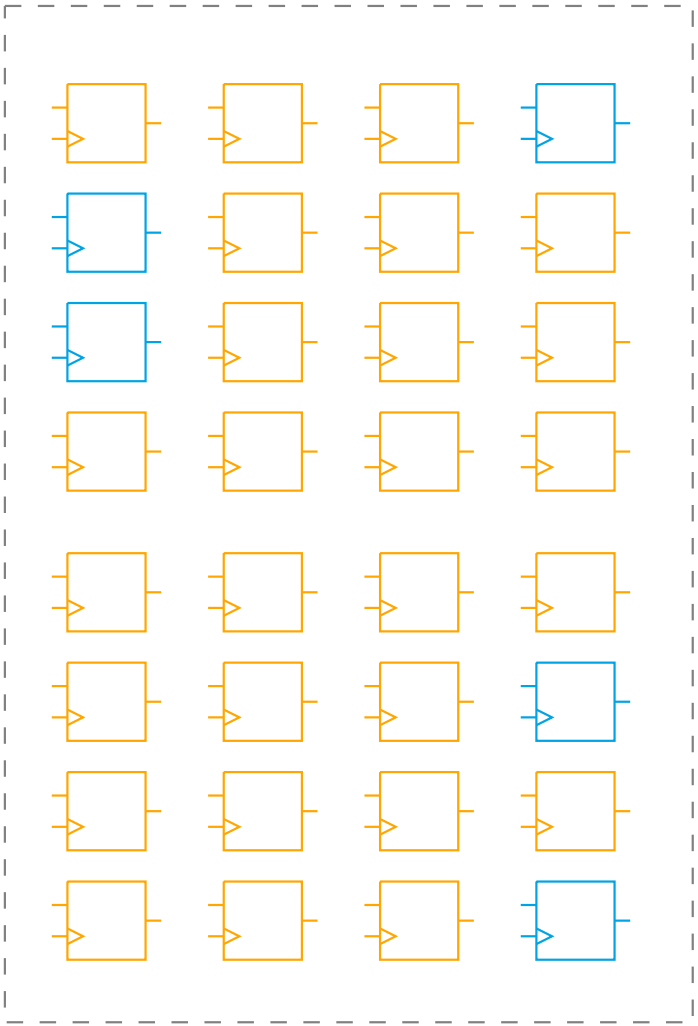


Design under test



Phase 1 (`amp. 0 à X`): all registers are faulted

Design under test

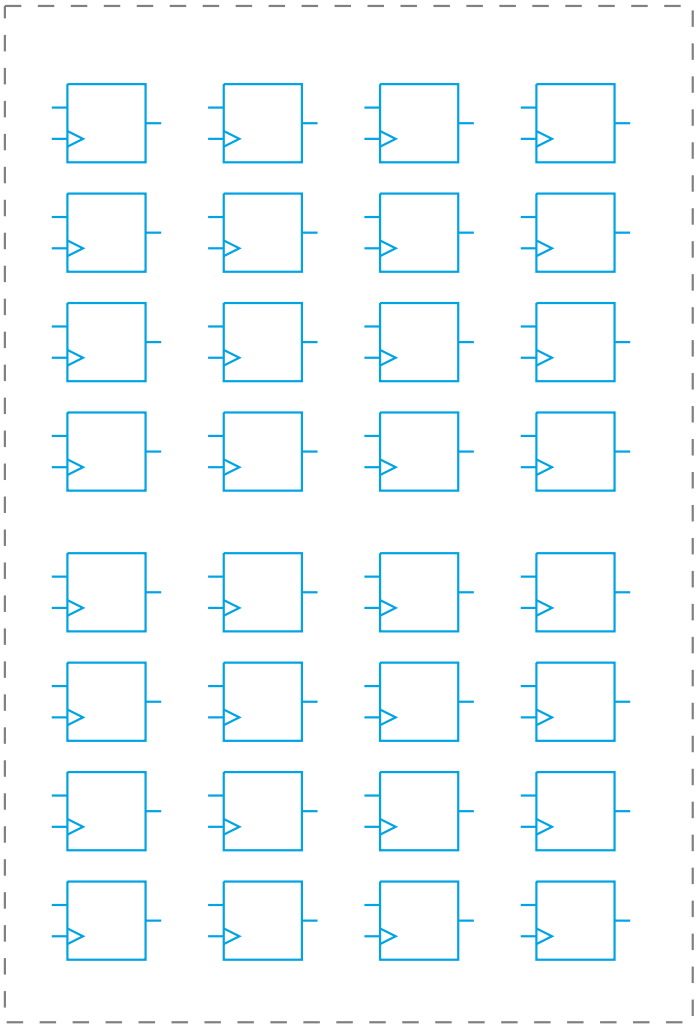


Phase 1 (`amp. 0` à `X`): all registers are faulted

Phase 2 (`amp. X+1` à `X+k`): some registers remain faulted, some registers become unfaulted

$\Rightarrow$ *fault sensitivity*

Design under test



Phase 1 (`amp. 0` à `X`): all registers are faulted

Phase 2 (`amp. X+1` à `X+k`): some registers remain faulted, some registers become unfaulted

$\Rightarrow$ *fault sensitivity*

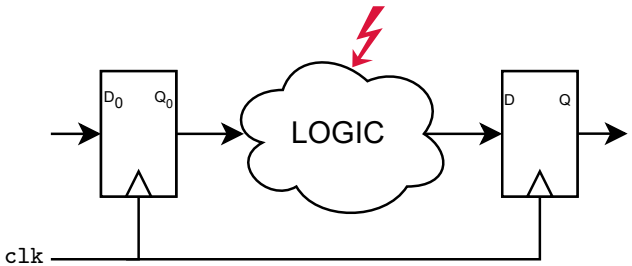
Phase 3 ($>$ `amp X+k`): all registers are unfaulted

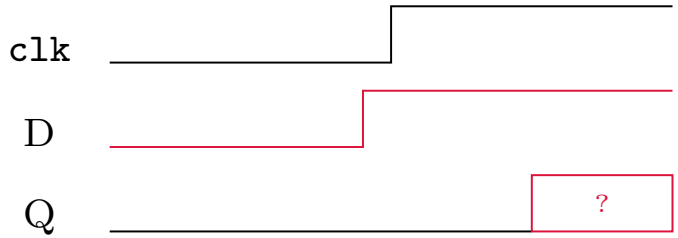
Hypotheses

1. TRAITOR's fault model is the *Timing Fault Model*.
2. TRAITOR's fault model is the *Sampling Fault Model*.

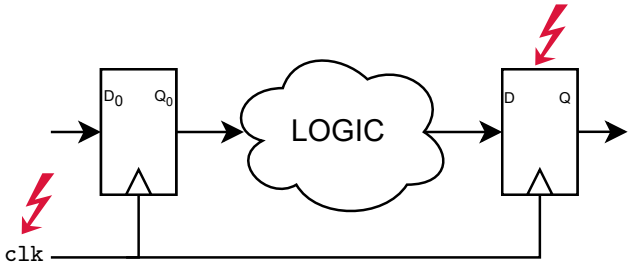
Timing Fault Model ?

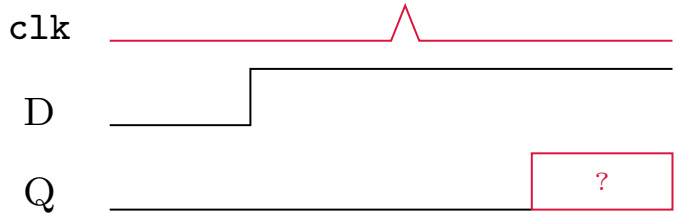
Timing Fault Model:





TRAITOR's Fault Model:

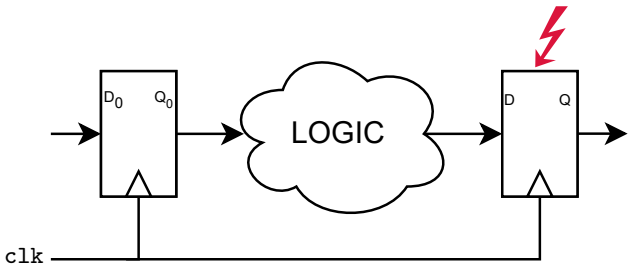


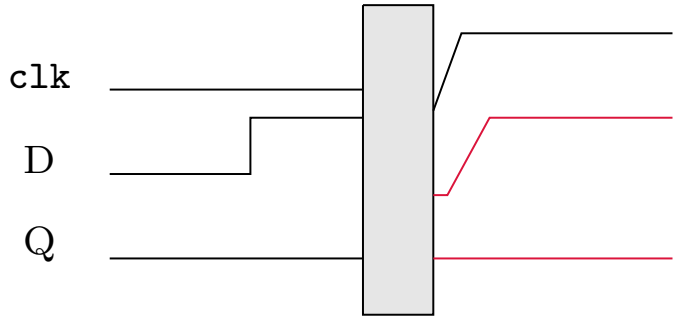


Electromagnetic Transient Faults Injection on a hardware and a software implementation of AES. Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, Assia Tria

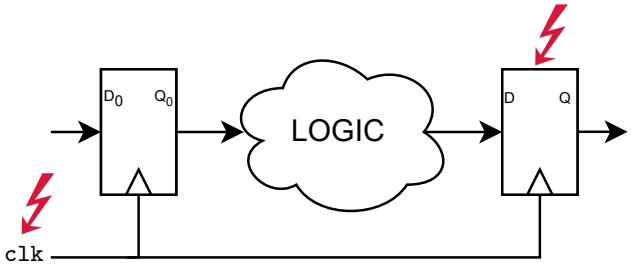
Sampling Fault Model ?

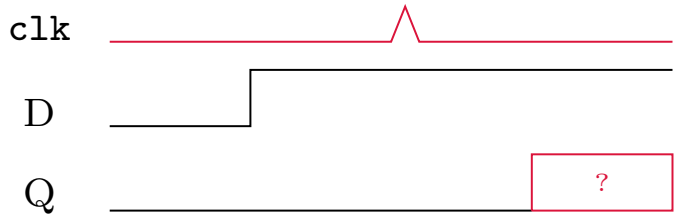
Sampling Fault Model:





TRAITOR's Fault Model:



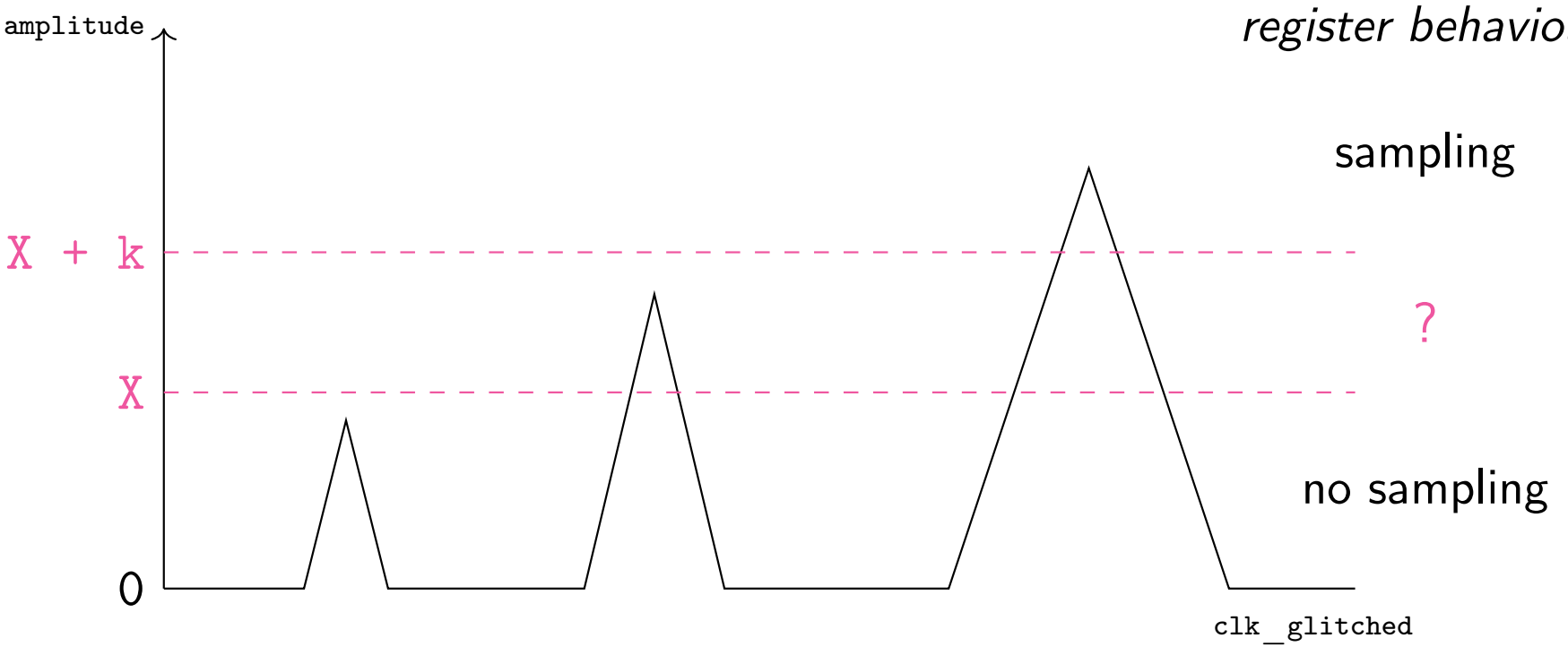


Modeling and Simulating Electromagnetic Fault Injection. Mathieu Dumont, Mathieu Lisart, Philippe Maurine

Hypotheses

1. TRAITOR's fault model is the *Timing Fault Model*. ×
2. TRAITOR's fault model is the *Sampling Fault Model*. ×
3. *Energy-threshold Fault Model.* For a DFF to correctly register a clock rising edge, the clock signal is required to be above some energy threshold, combination of a voltage threshold and a width threshold.

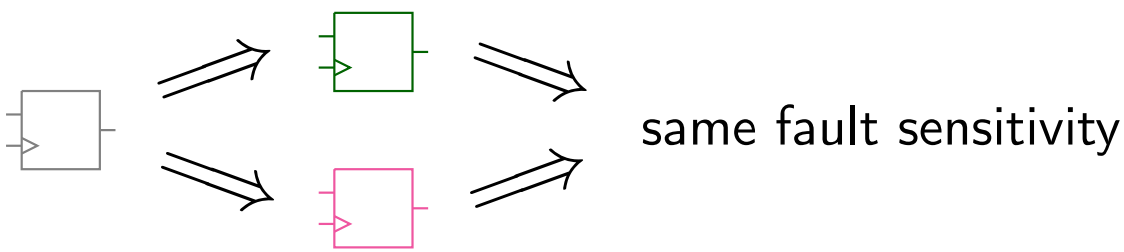
Energy-threshold Fault Model



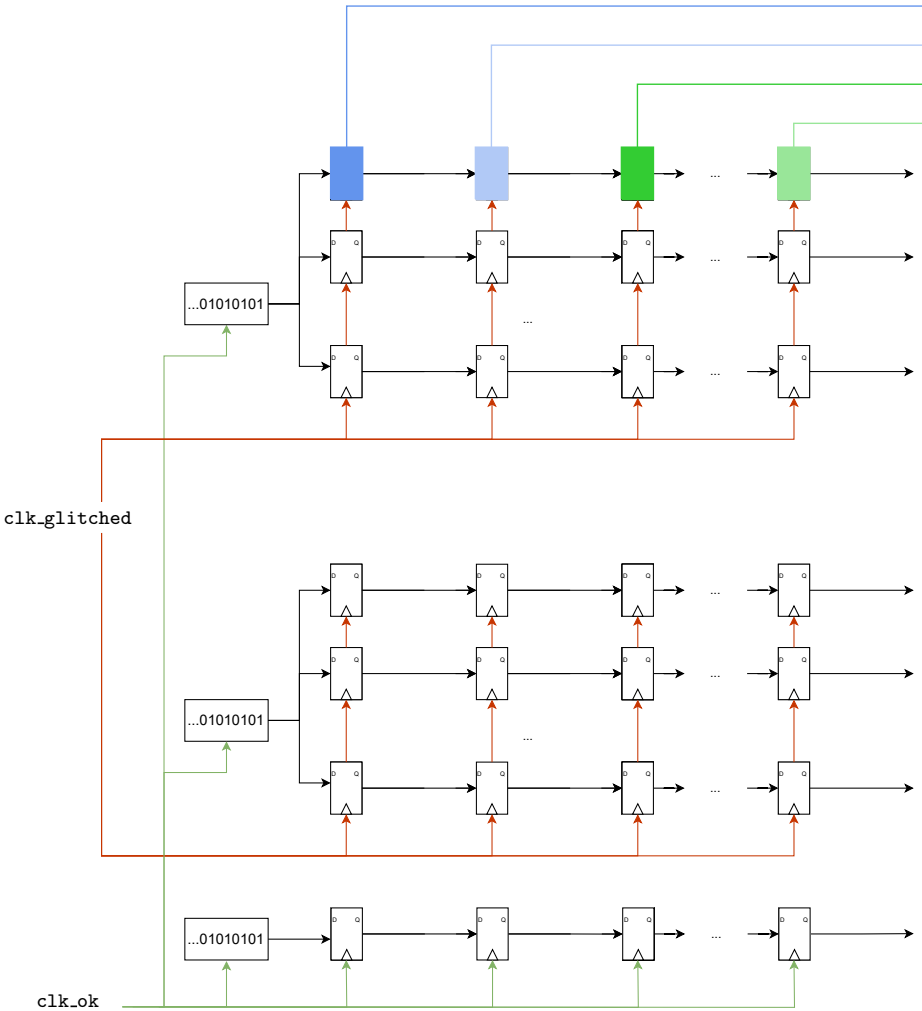
Impact of the glitched clock on one register

Hypotheses

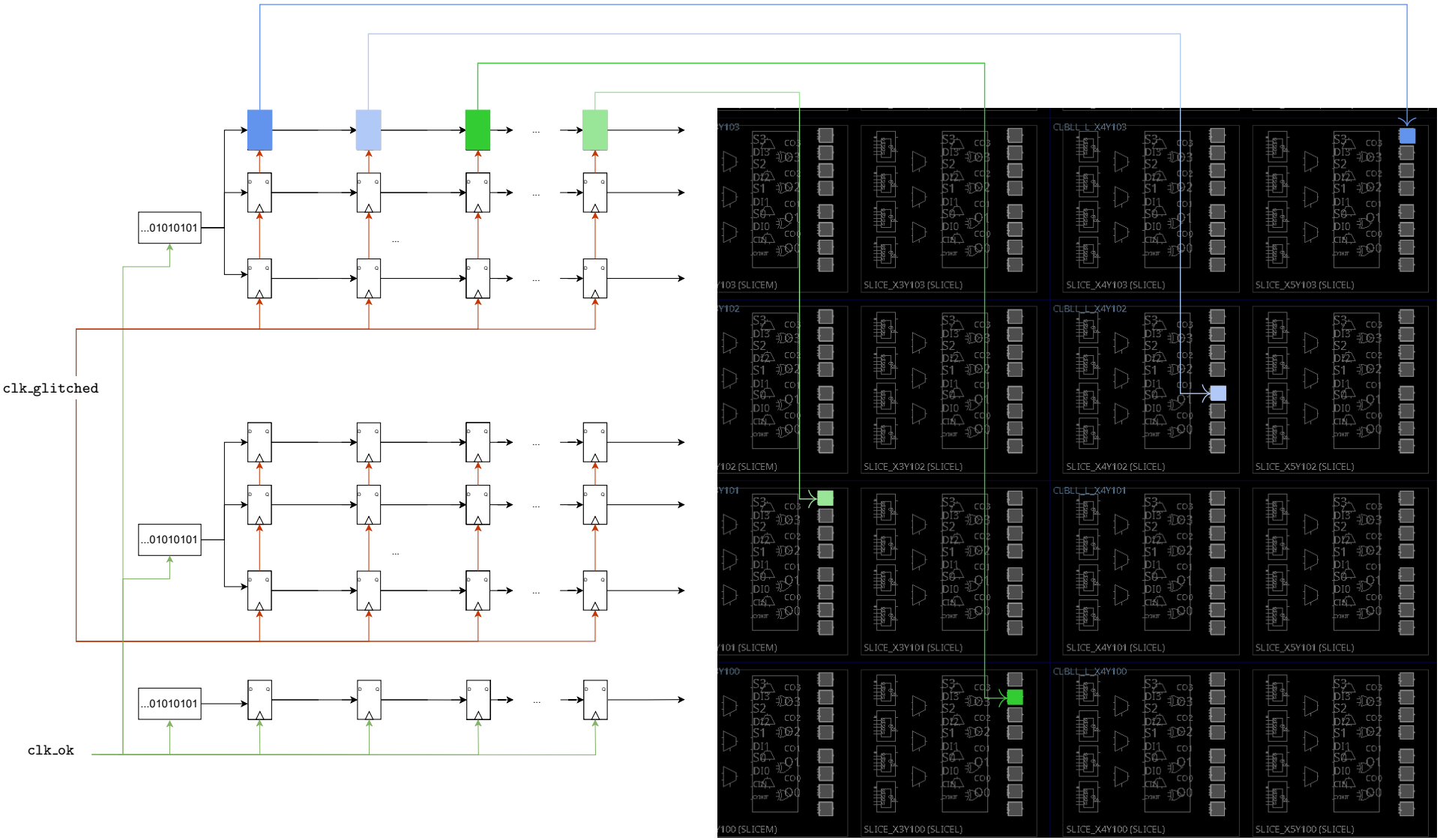
1. TRAITOR's fault model is the *Timing Fault Model*. ×
2. TRAITOR's fault model is the *Sampling Fault Model*. ×
3. *Energy-threshold Fault Model.* For a DFF to correctly register a clock rising edge, the clock signal is required to be above some energy threshold, combination of a voltage threshold and a width threshold. ✓
4. *Fault sensitivity variation.* The fault sensitivity only depends on the register.



Fault sensitivity variation: configuration 1

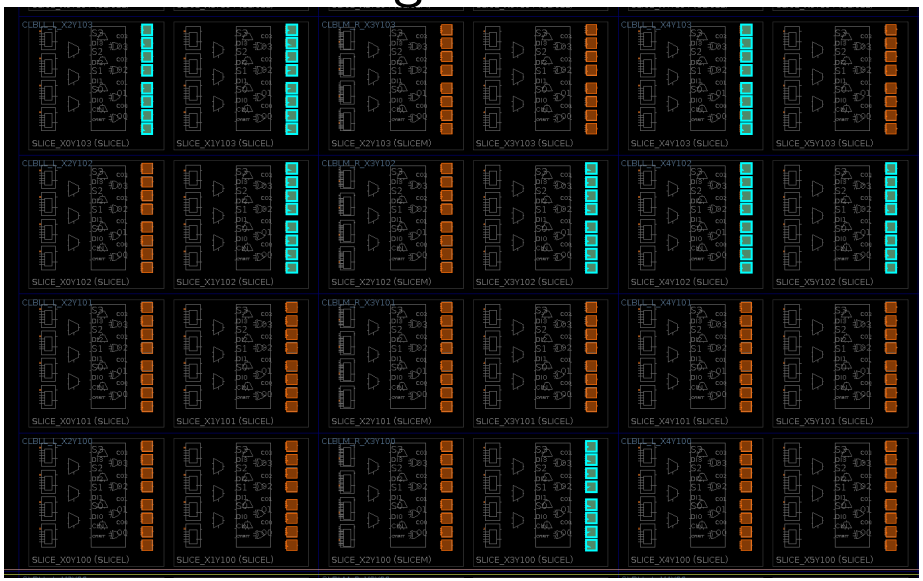


Fault sensitivity variation: configuration 2

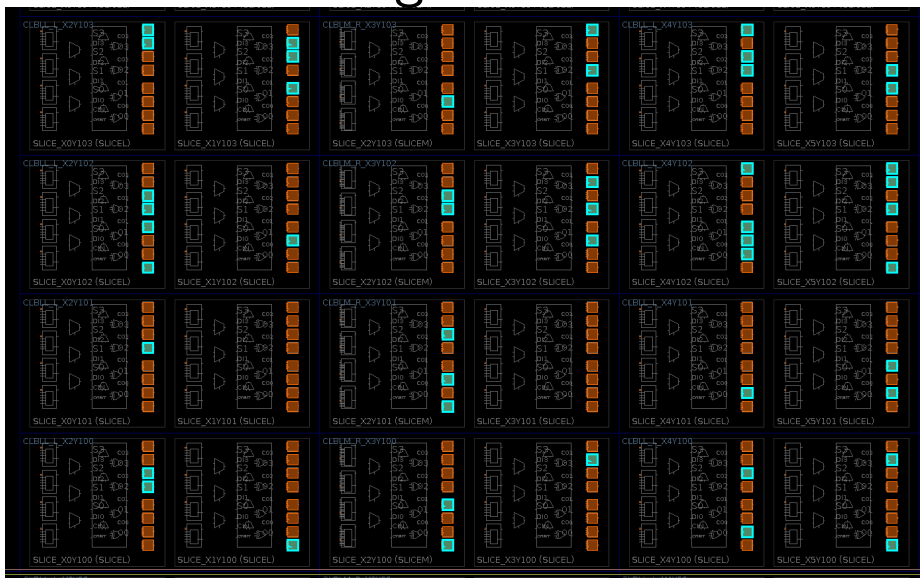


Fault sensitivity variation

configuration 1



configuration 2

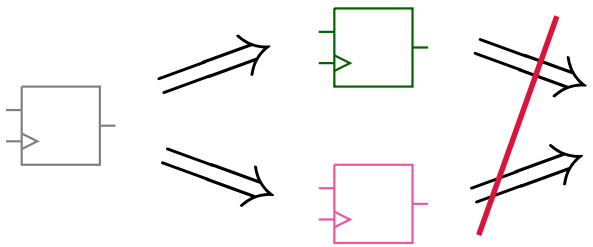


- unfaulted register
- faulted register

Registers' status for `amp. 22`

Fault sensitivity variation

(4) *Fault sensitivity variation.* The fault sensitivity only depends on the register.



same fault sensitivity

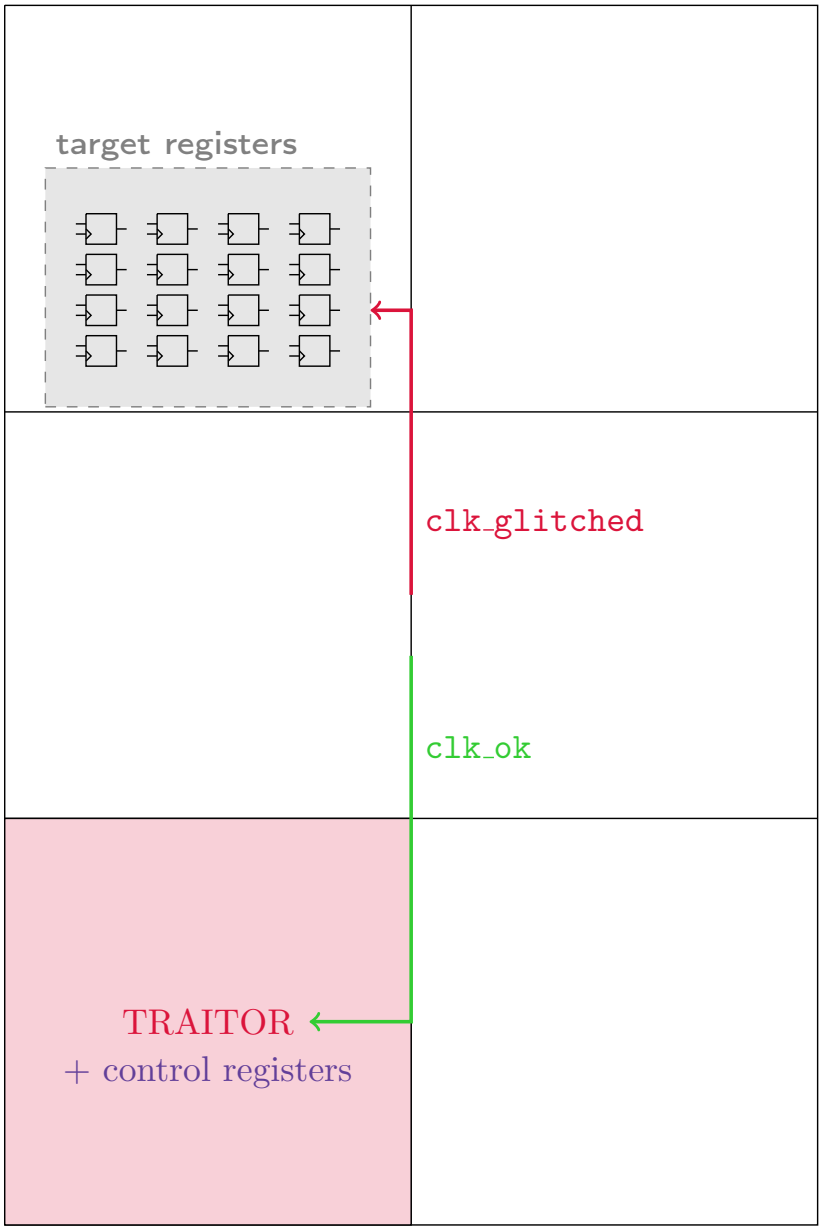
$\Rightarrow$ why ?

New hypothesis: the only thing that changes is the routing between registers... does it influence the glitched clock ?

Hypotheses

1. TRAITOR's fault model is the *Timing Fault Model*. ×
2. TRAITOR's fault model is the *Sampling Fault Model*. ×
3. *Energy-threshold Fault Model.* For a DFF to correctly register a clock rising edge, the clock signal is required to be above some energy threshold, combination of a voltage threshold and a width threshold. ✓
4. *Fault sensitivity variation.* The fault sensitivity only depends on the register. ×
5. *Registers and clock routing cross-talk.* Data routes influence TRAITOR's glitched clock.
6. *Inter-clock routing cross-talk.* Other clock routing on the same FPGA influences TRAITOR's glitched clock.

Registers and clock routing cross-talk

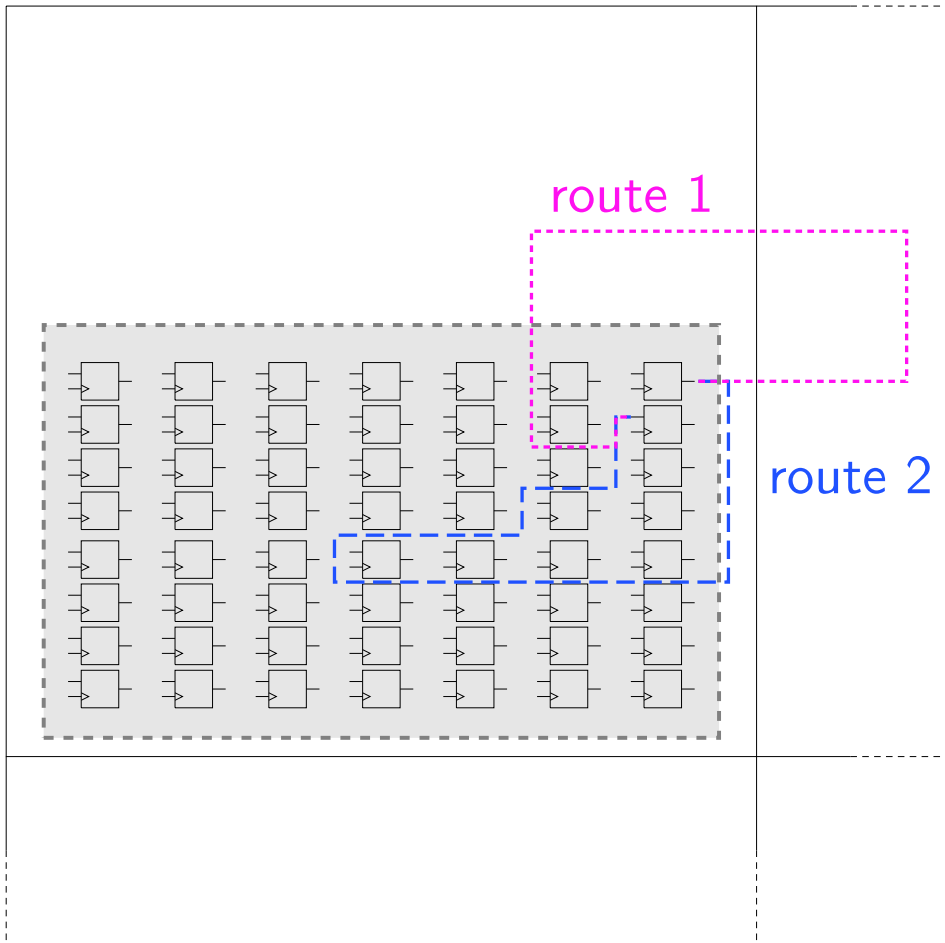


Experiment set-up:

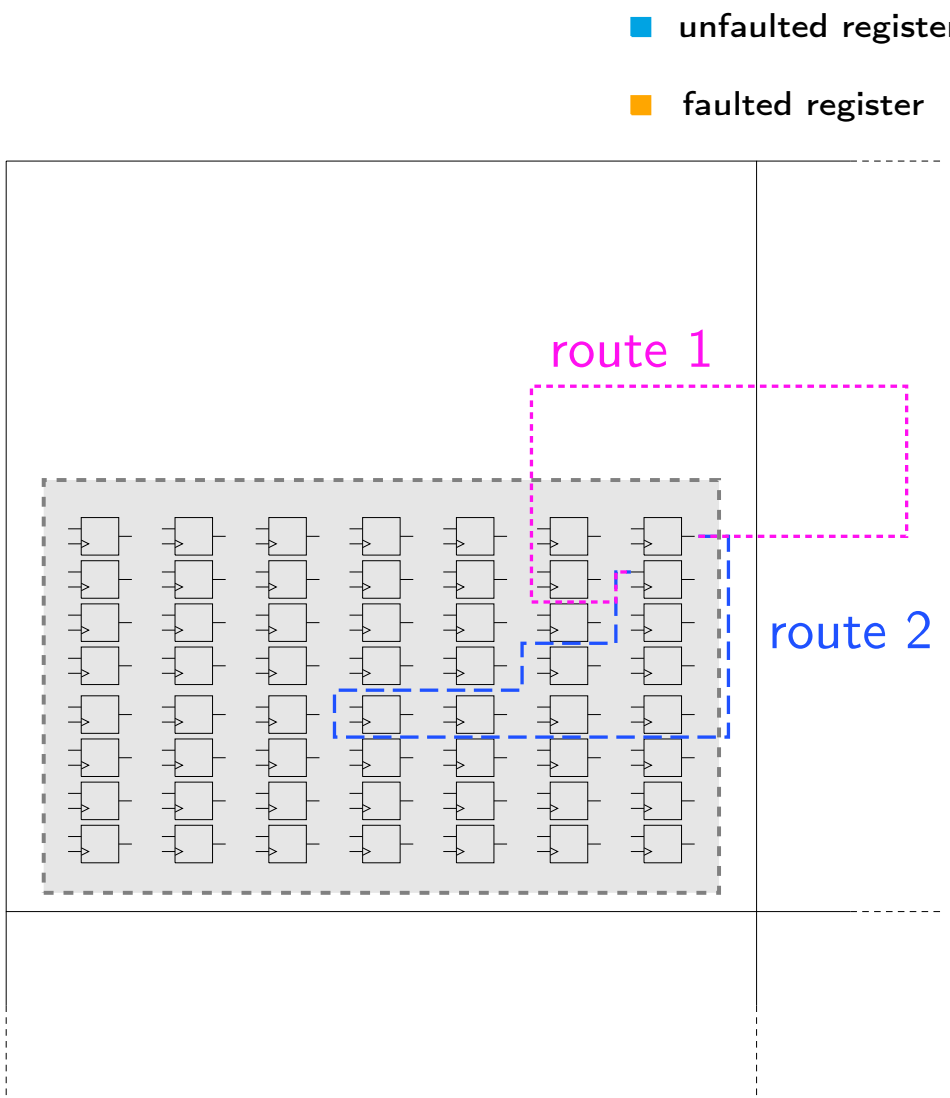
→ Artix-7

→ faults injected from `amp. 0`

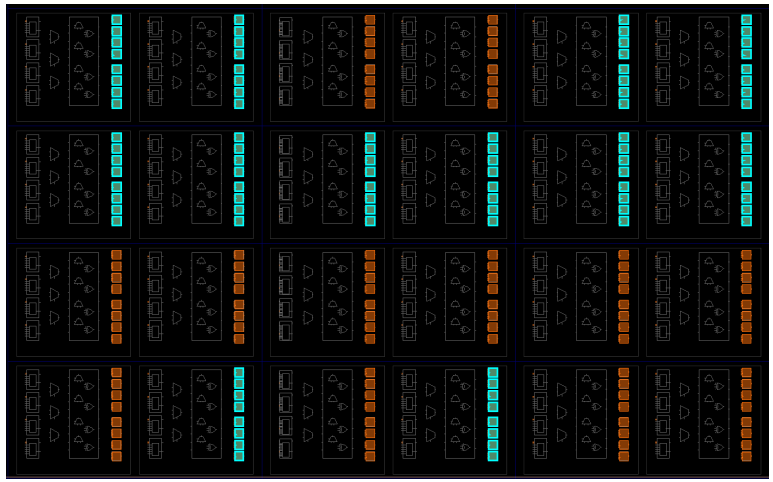
Registers and clock routing cross-talk



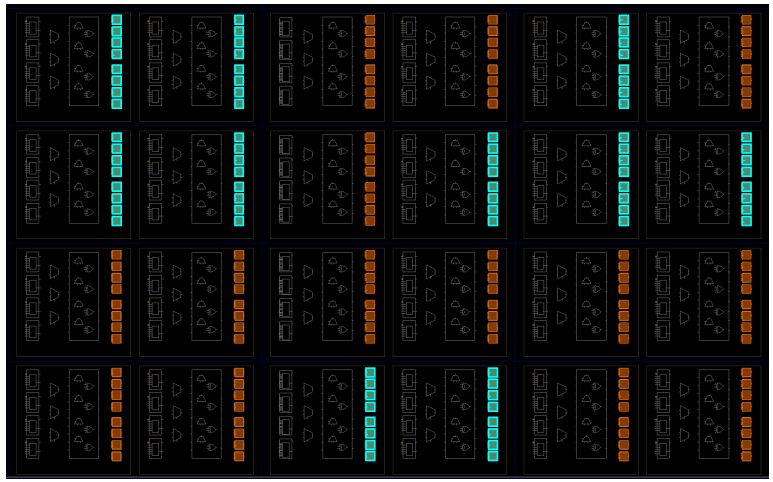
Registers and clock routing cross-talk



route 1 (amp. 22)



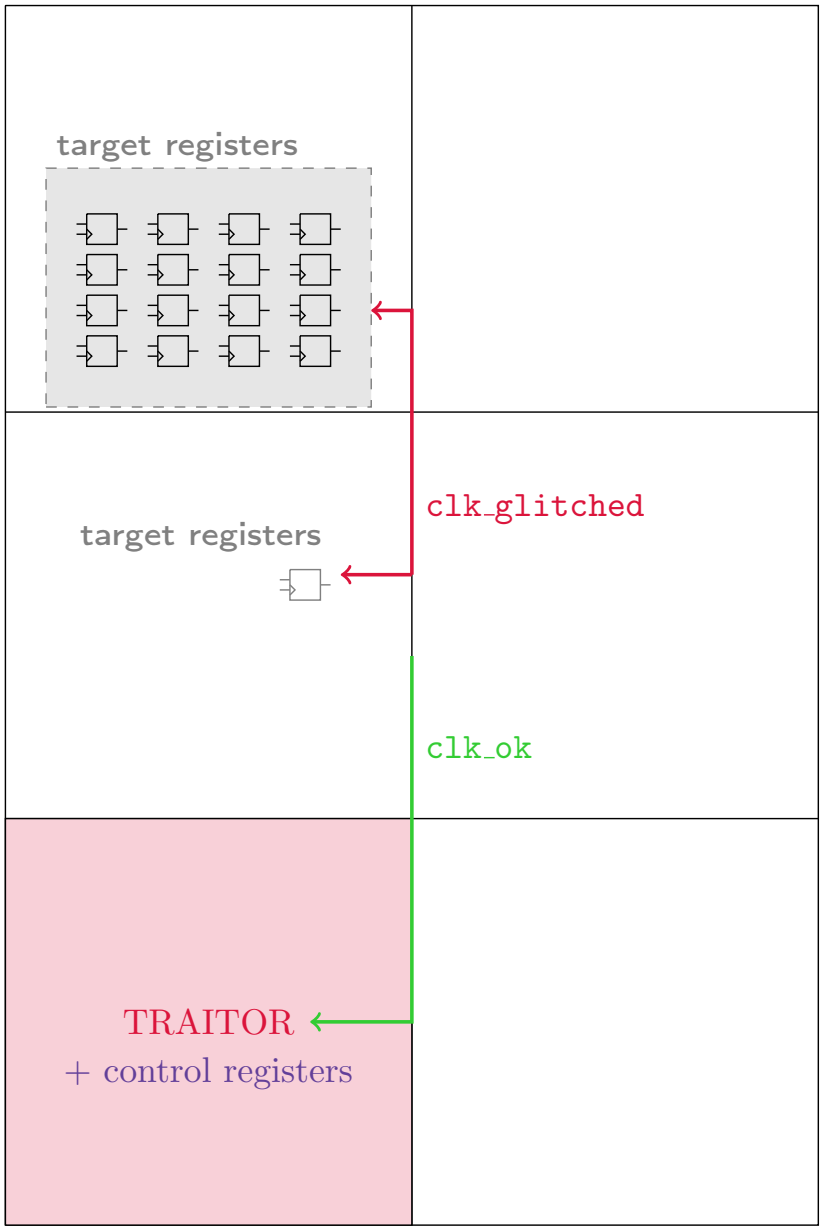
route 2 (amp. 22)



Hypotheses

1. TRAITOR's fault model is the *Timing Fault Model*. ×
2. TRAITOR's fault model is the *Sampling Fault Model*. ×
3. *Energy-threshold Fault Model.* For a DFF to correctly register a clock rising edge, the clock signal is required to be above some energy threshold, combination of a voltage threshold and a width threshold. ✓
4. *Fault sensitivity variation.* The fault sensitivity only depends on the register. ×
5. *Registers and clock routing cross-talk.* Data routes influence TRAITOR's glitched clock. ✓
6. *Inter-clock routing cross-talk.* Other clock routing on the same FPGA influences TRAITOR's glitched clock.

Inter-clock routing cross-talk



Experiment set-up:

→ Artix-7

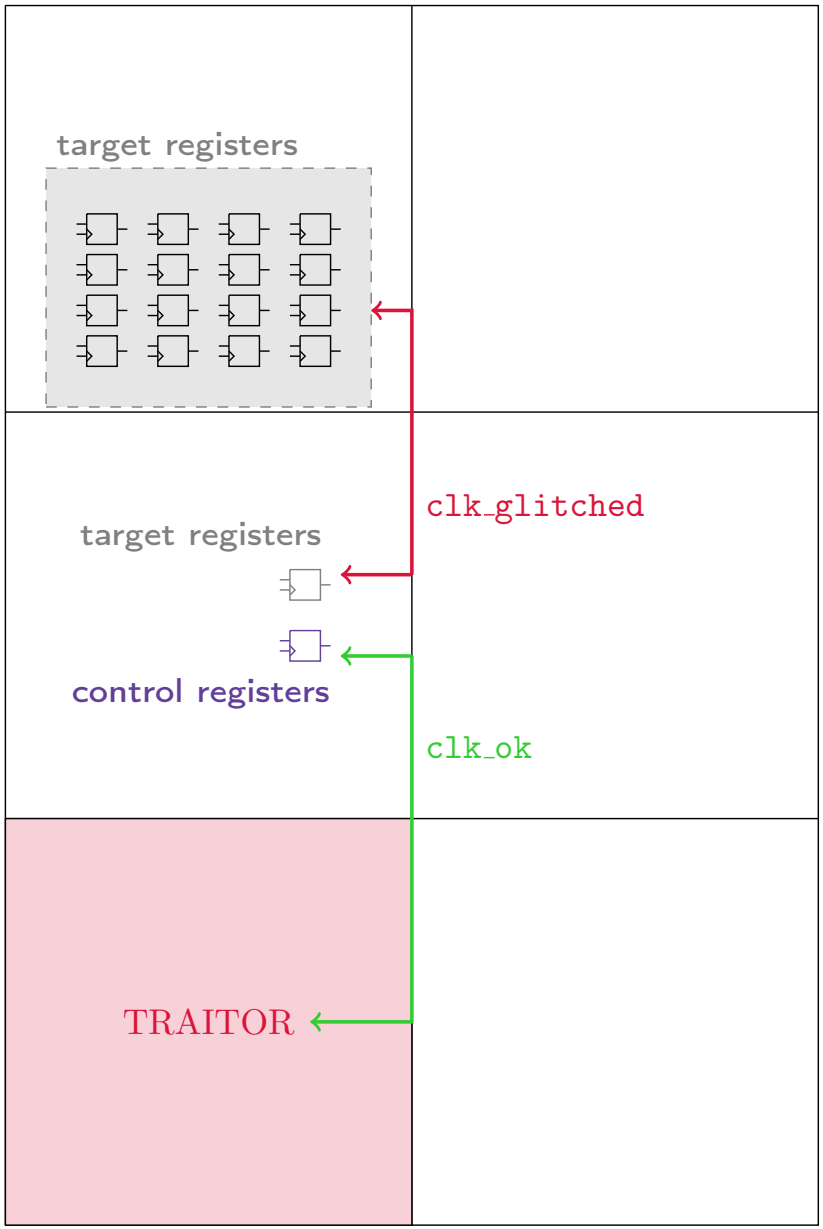
→ faults injected from amp. 0

Registers' behaviour:

→ fault sensitivity of singled-out target registers : 21

→ fault sensitivity of other target registers : 22

Inter-clock routing cross-talk



Experiment set-up:

→ Artix-7

→ faults injected from `amp. 0`

Registers' behaviour:

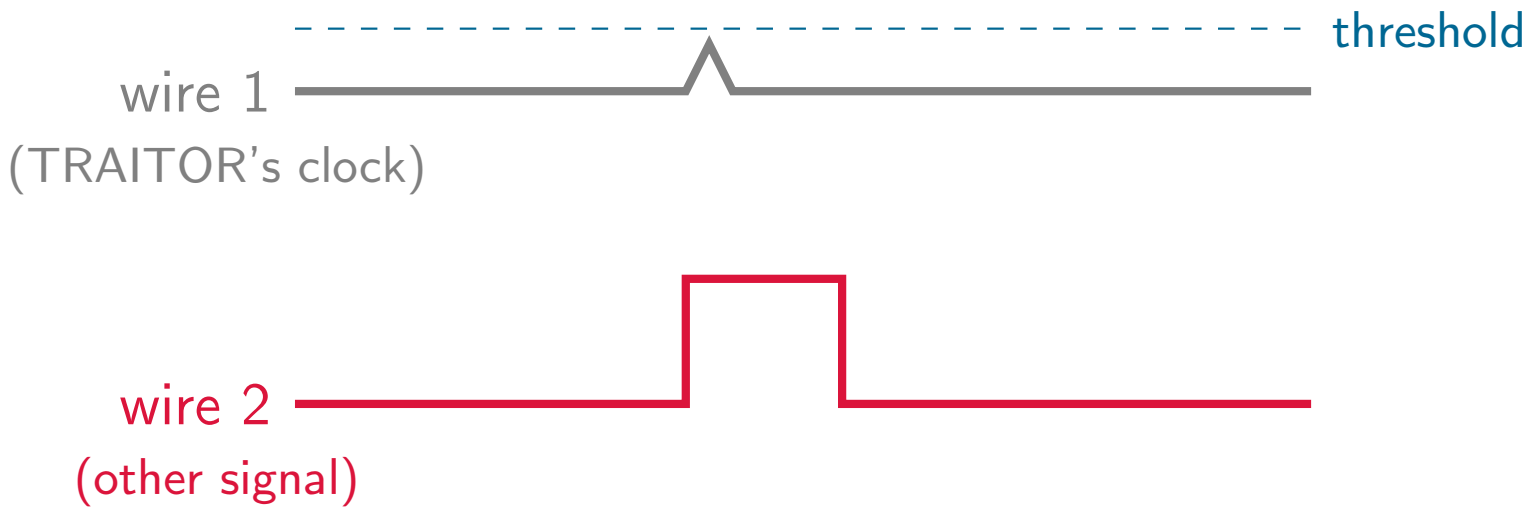
→ fault sensitivity of singled-out target registers : 20

→ fault sensitivity of other target registers : 22

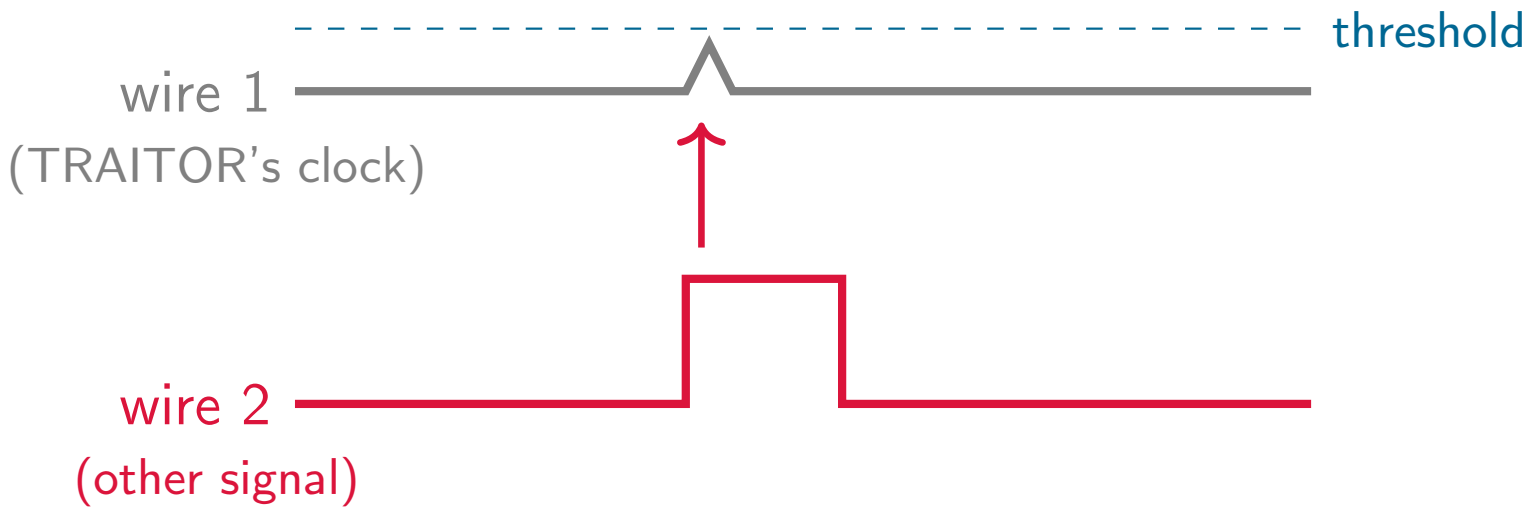
Hypotheses

1. TRAITOR's fault model is the *Timing Fault Model*. ×
2. TRAITOR's fault model is the *Sampling Fault Model*. ×
3. *Energy-threshold fault model.* For a DFF to correctly register a clock rising edge, the clock signal is required to be above some energy threshold, combination of a voltage threshold and a width threshold. ✓
4. *Fault sensitivity variation.* The fault sensitivity only depends on the register. ×
5. *Registers and clock routing cross-talk.* Data routes influence TRAITOR's glitched clock. ✓
6. *Inter-clock routing cross-talk.* Other clock routing on the same FPGA influences TRAITOR's glitched clock. ✓

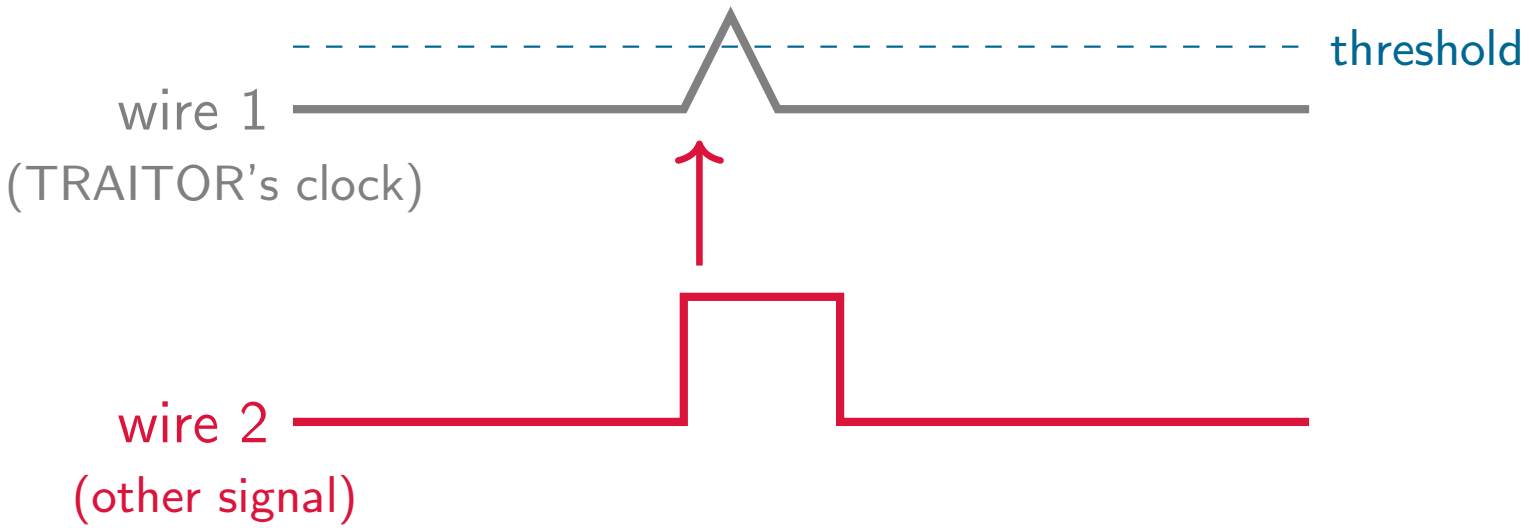
Cross-talk



Cross-talk

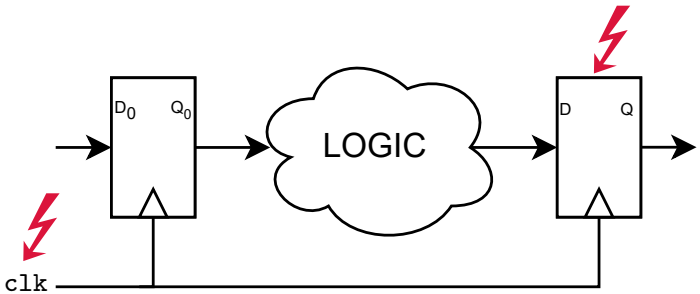


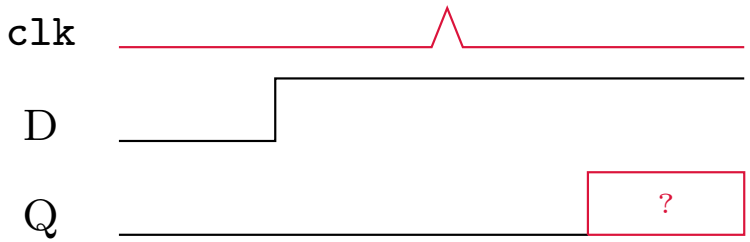
Cross-talk

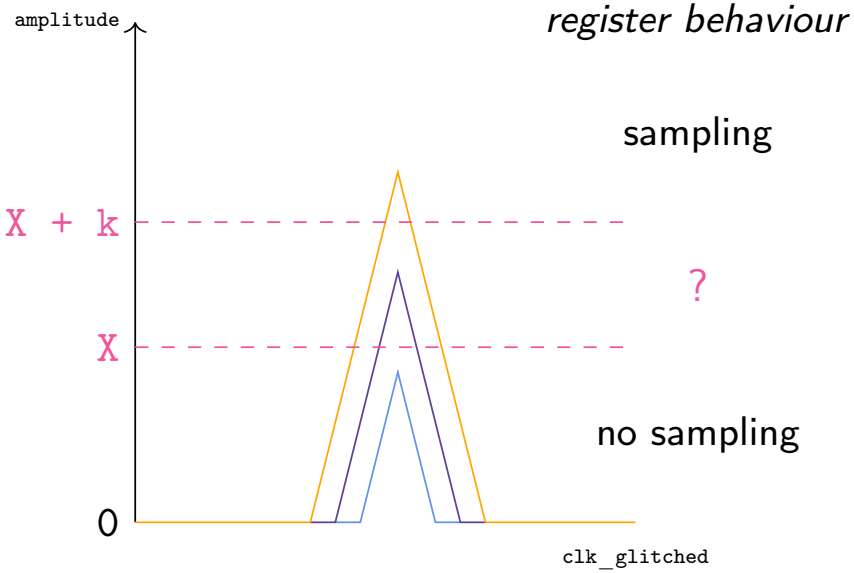


Conclusion

Energy-threshold Fault Model:







→ Energy threshold (voltage and width)

→ Cross-talk (register/clock routing and clock/clock routing)

→ Explanation for some electromagnetic faults ?