Characterizing and Modeling Synchronous Clock-Glitch Fault Injection

Amélie Marotta[1]

amelie.marotta@inria.fr

Ronan Lashermes[1], Guillaume Bouffard[2], Olivier Sentieys[1], Rachid Dafali[3]

[1]University of Rennes, Inria
[2]National Cybersecurity Agency of France (ANSSI)
[3]DGA-MI

Introduction

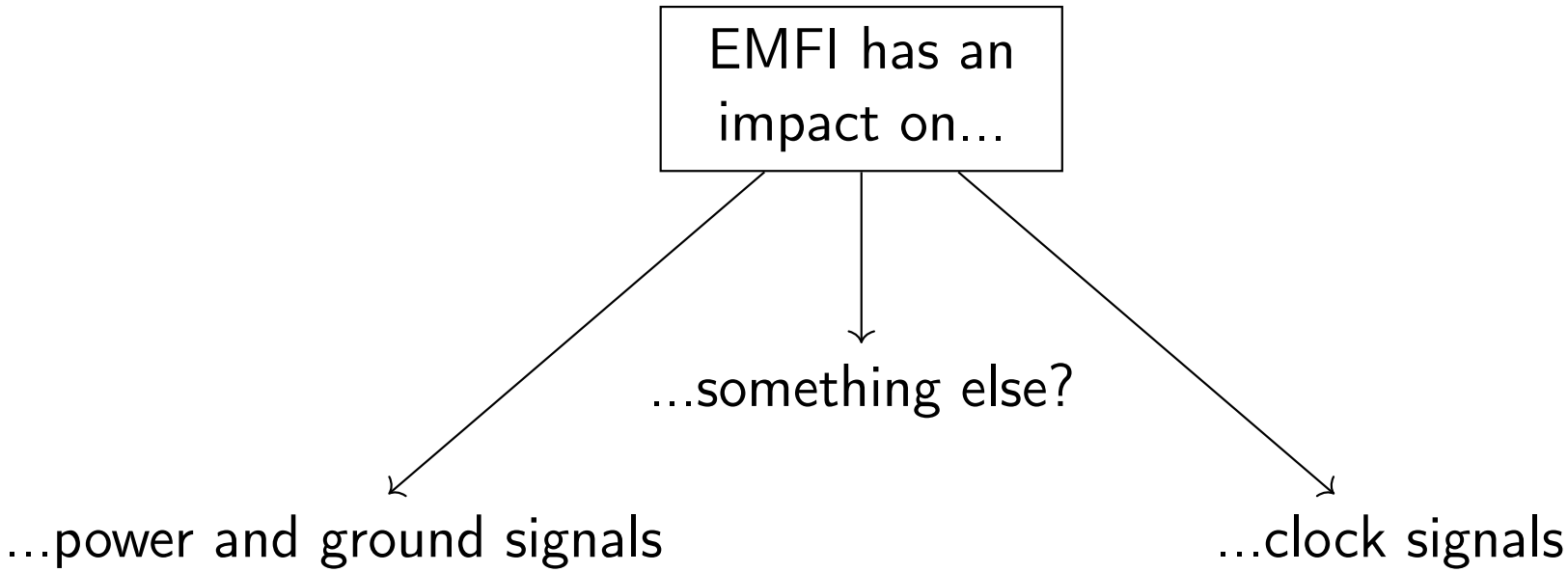
→ Electromagnetic fault injection (EMFI) has many effects of a circuit.

→ Fault model: explanation of a fault at different abstraction levels.

level	manifestation
microarchitectural	impact on the microarchitecture ↪ instruction skip
register-transfer	logic signal alteration ↪ bitflip propagating through a circuit
physical	interaction between fault injection and transistors/logic gates, analog signals ↪ DFF sampling an incorrect value

Overview

EMFI, physical effects



Underpowered circuit: Timing Fault Model

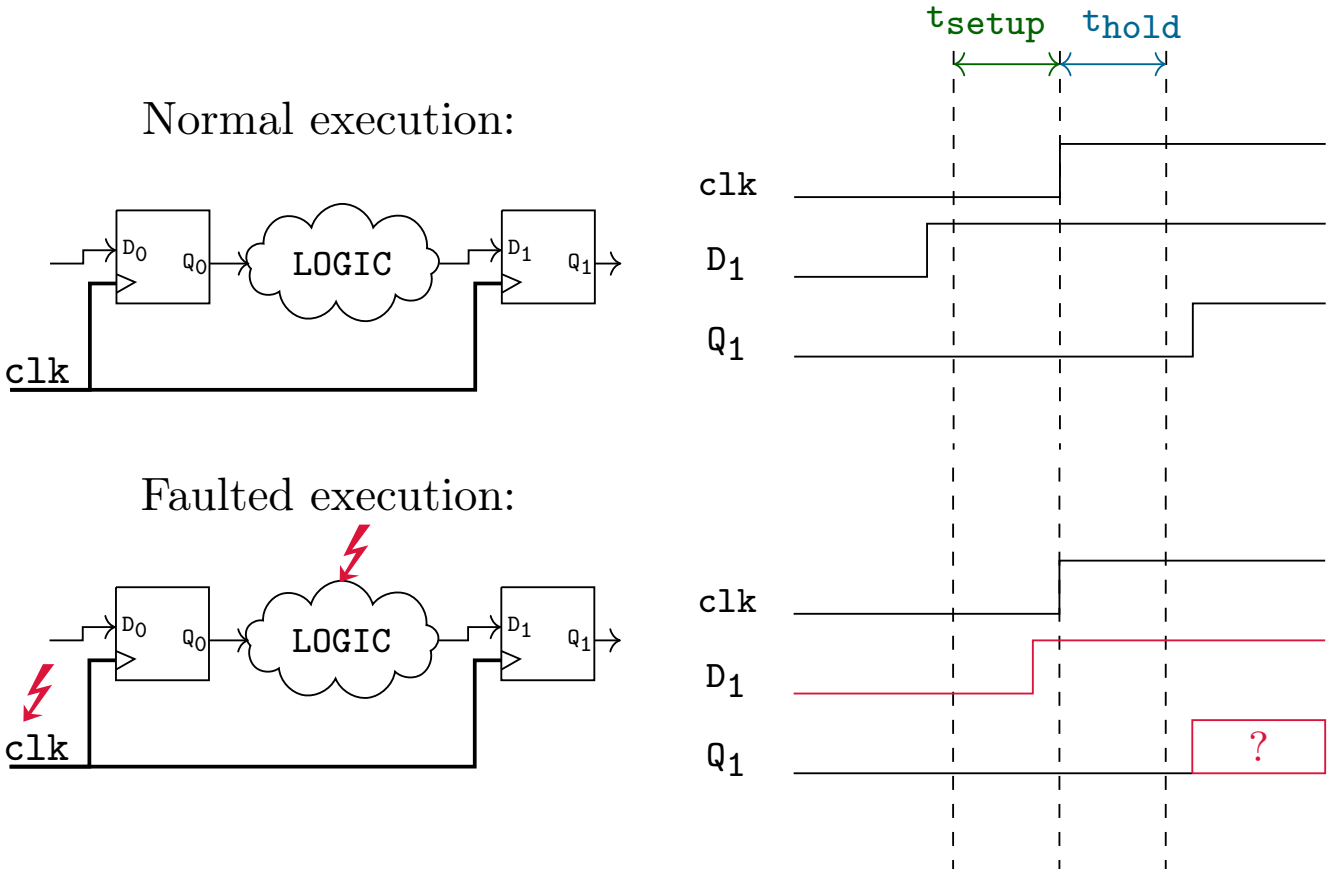


Figure: Timing Fault Model [3] on a simple circuit

Voltage bounces and drops: Sampling Fault Model

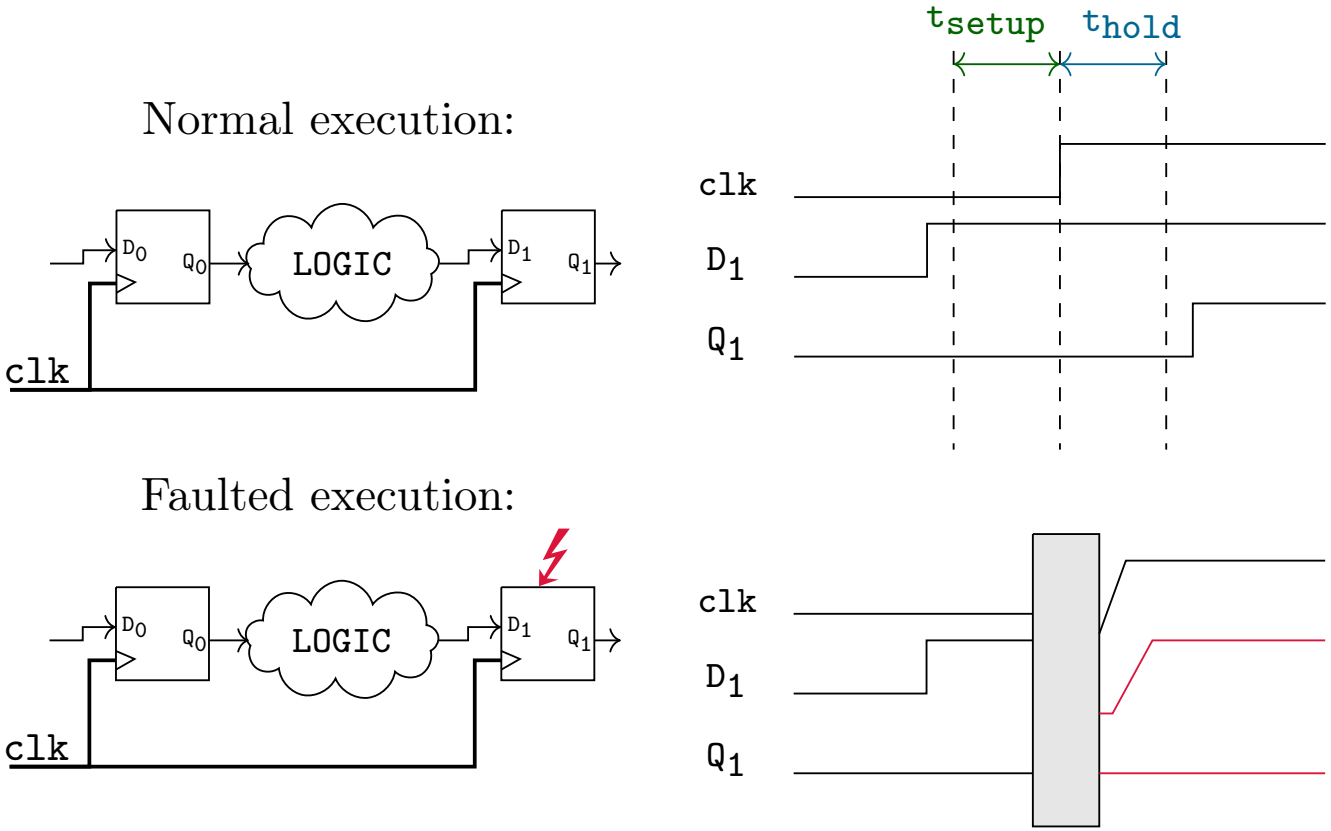


Figure: Sampling Fault Model [4] on a simple circuit

Modified clock cycle

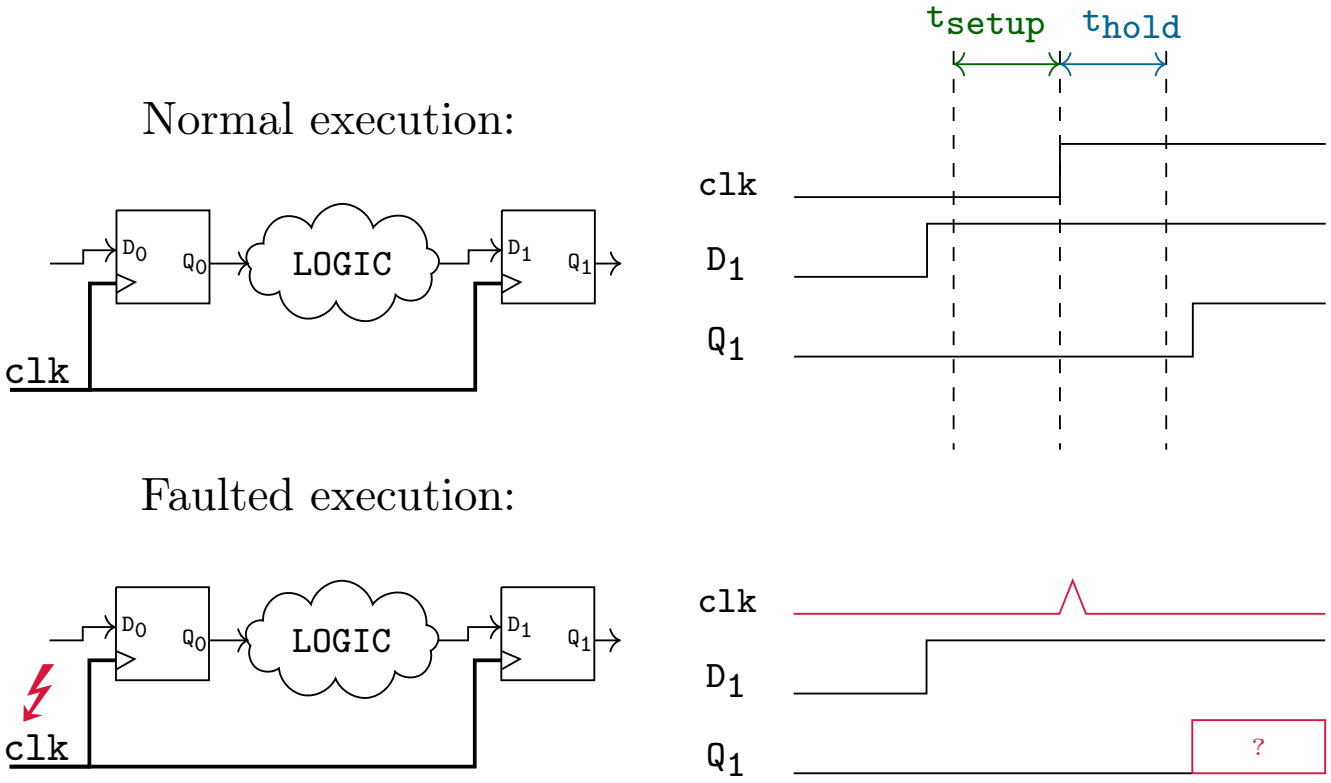


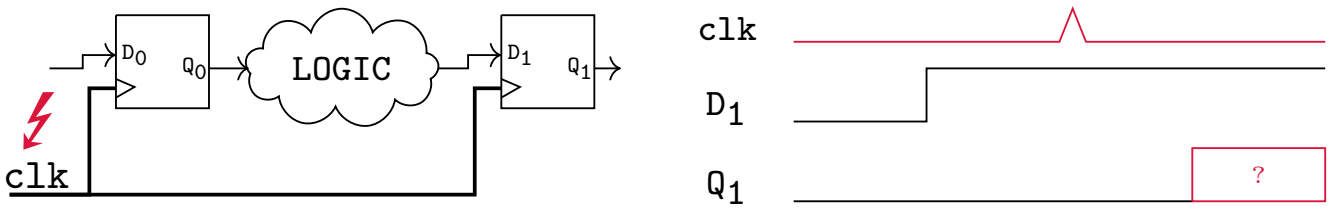
Figure: Synchronous Clock Glitch (SCG) impact on a simple circuit [1]

× Timing Fault Model

× Sampling Fault Model

Our goals

Faulted execution:



⇒ provide a physical fault model that explain how the SCG leads to faults.

↪ physical experimentations

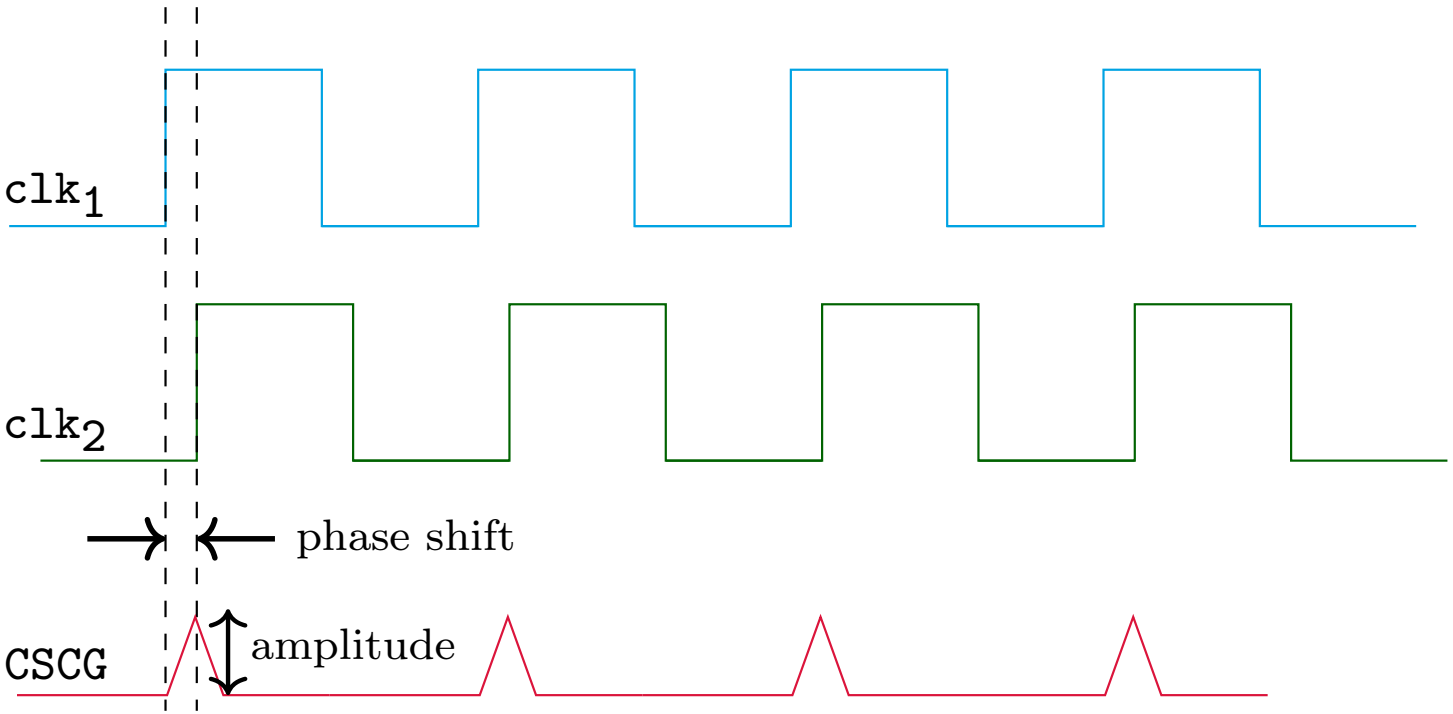
↪ simulations

⇒ glitch carried out by the clock

↪ DFFs impacted

Overview

TRAITOR: generation of the CSCG



$$\texttt{CSCG} = (\texttt{clk}_1 \oplus \texttt{clk}_2) \cdot \texttt{clk}_1$$

Figure: The Controlled Synchronous Clock Glitch (CSCG) is generated using two out-of-phase clocks, `clk1` and `clk2` [2]. The TRAITOR user has the capability to replace the regular clock signal with CSCG at their discretion.

TRAITOR

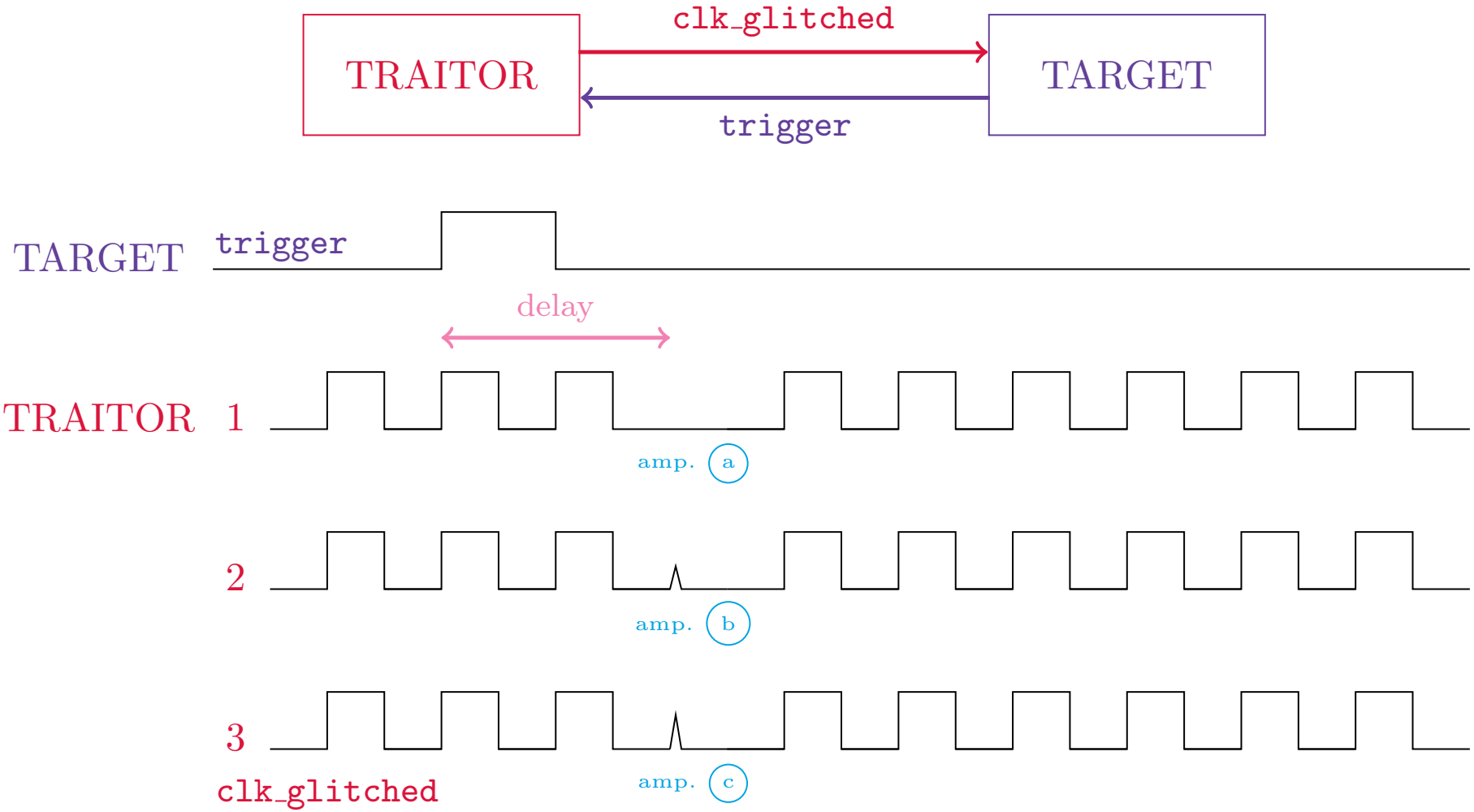


Figure: 3 examples of clock signals generated by TRAITOR, implemented on a Artix-7 FPGA, illustrating its possibilities.

Device Under Test (DUT)

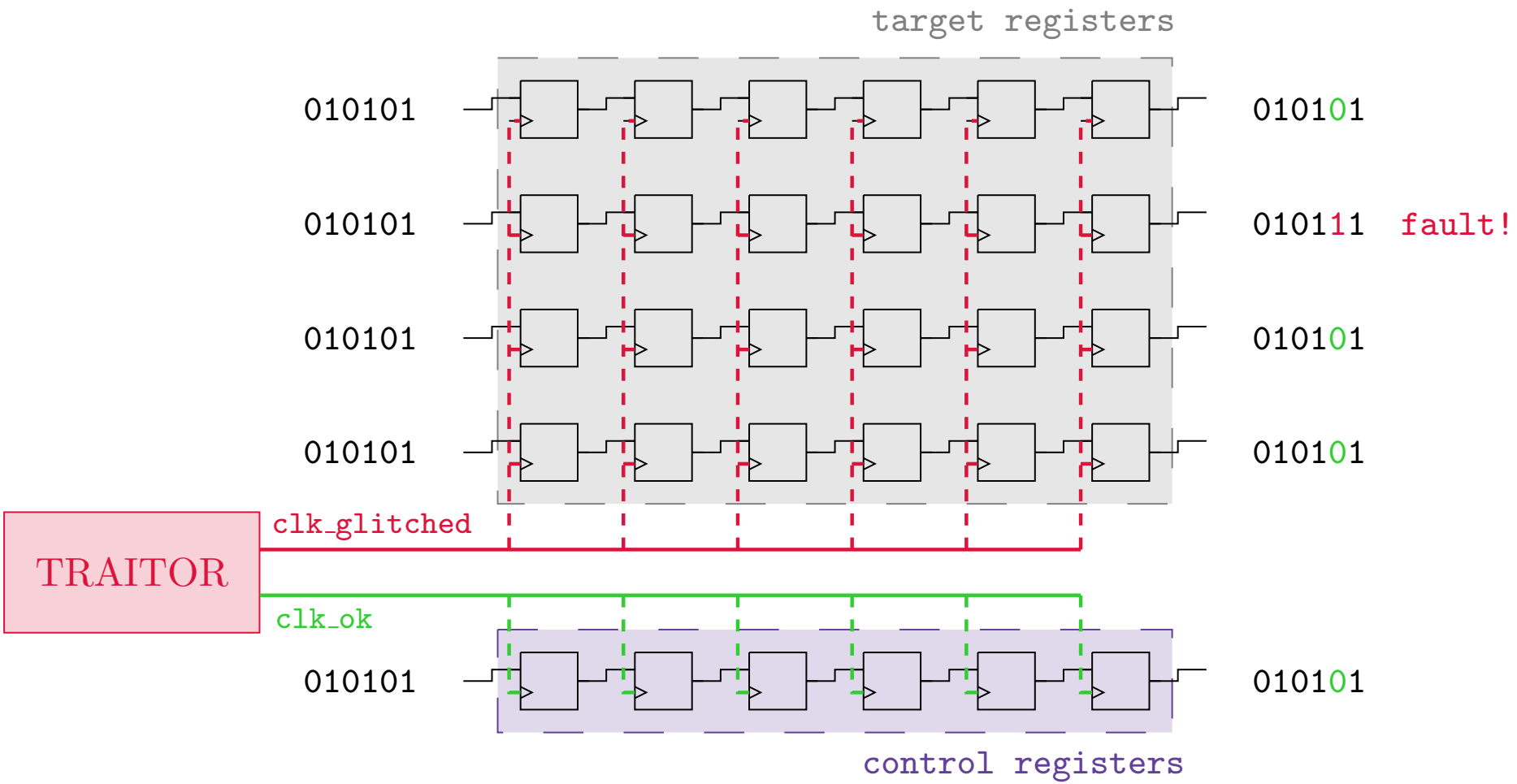


Figure: DUT and TRAITOR on an Artix-7 FPGA.

Logical and physical, in-order and randomized

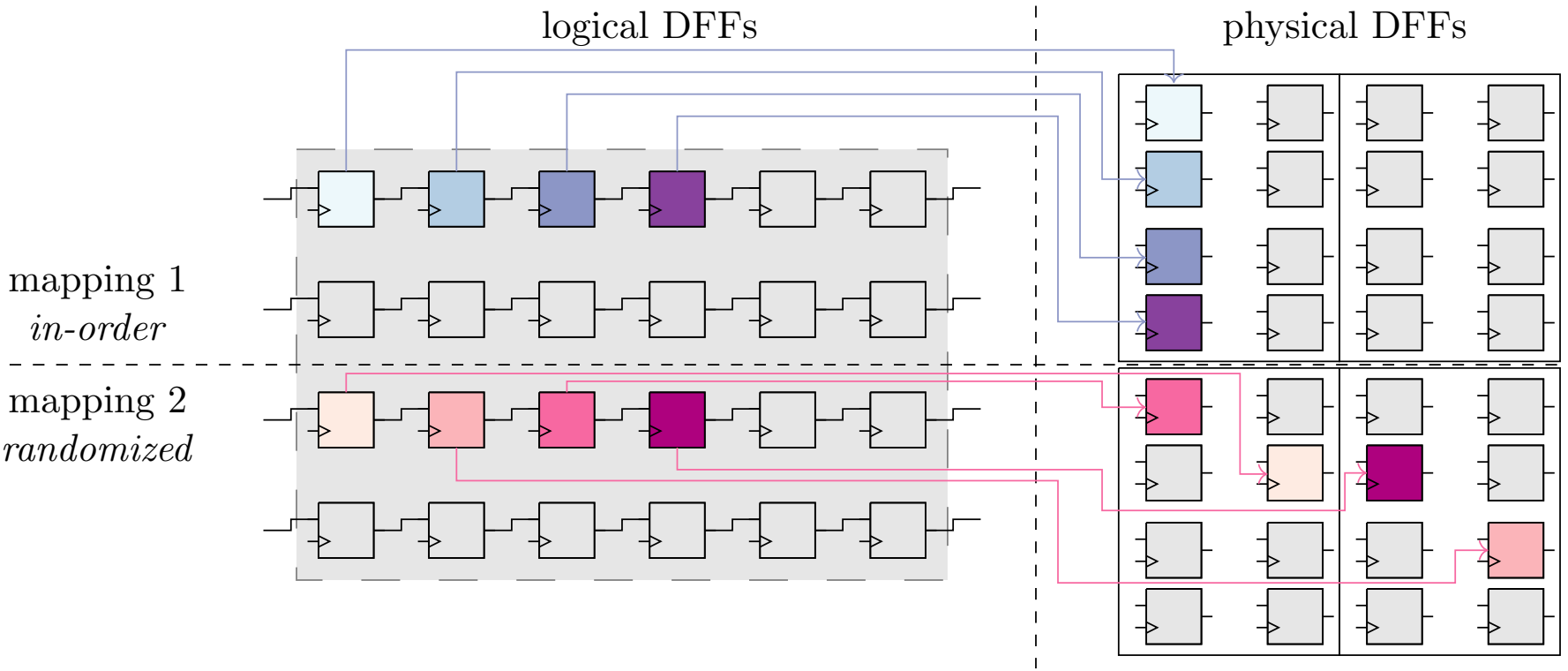


Figure: The two logical-to-hardware mappings: mapping 1 is in-order and mapping 2 is randomized.

Overview

1. Introduction

2. Electromagnetic Fault Injection

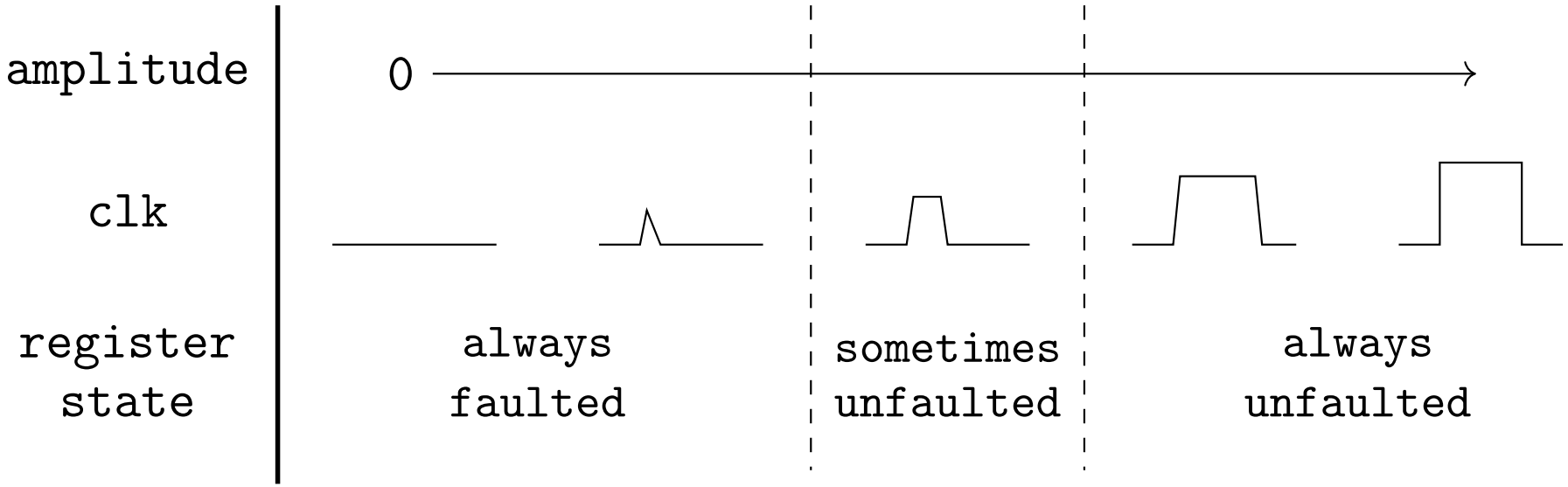
3. Experimental set-up
   → TRAITOR
   → Device Under Test

4. Hypotheses

5. Conclusion

Hypotheses

Hypothesis 1 (Energy Threshold) *For a DFF to correctly sample a clock's rising edge, the clock signal must meet a certain energy threshold, combination of voltage amplitude and width thresholds.*



Behaviour of 3 selected DFF

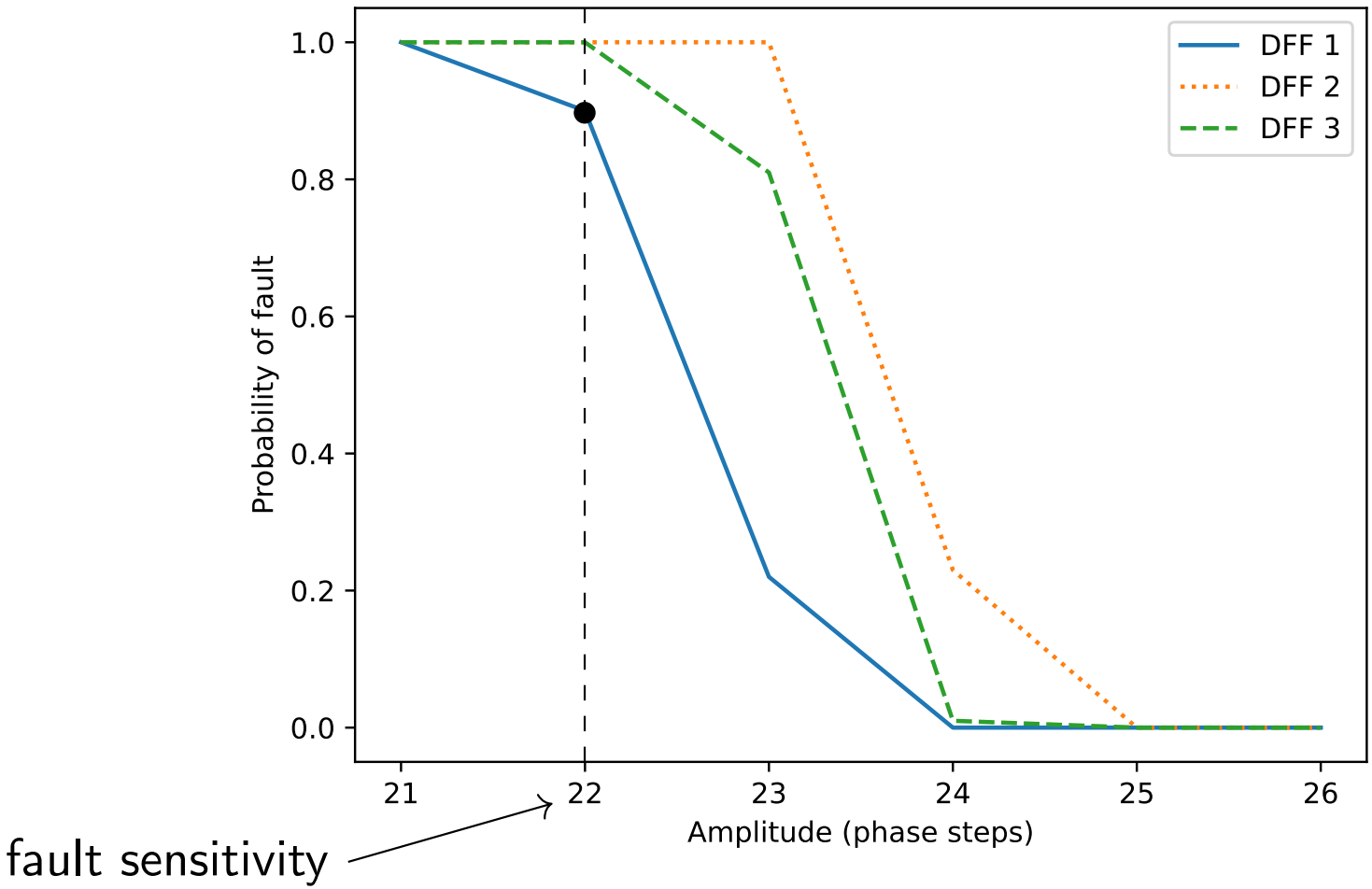
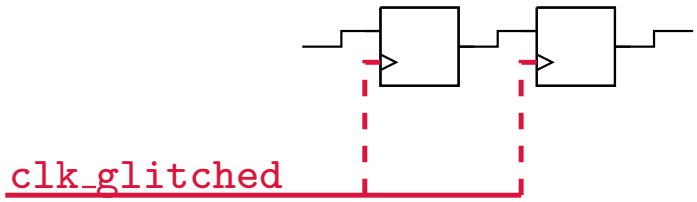


Figure: Transitions phases of three target physical DFFs chosen since they exhibit different characteristics.

Simulation set-up



- → SPICE simulation
- → 28nm DFF
  - ↪ not the exact same as the Artix-7 DFF
  - ↪ designed for similar technology so should behave the same way
- → focus on the state change of the first DFF

Goal: estimate the impact of the voltage and width of the CSCG

Simulation results

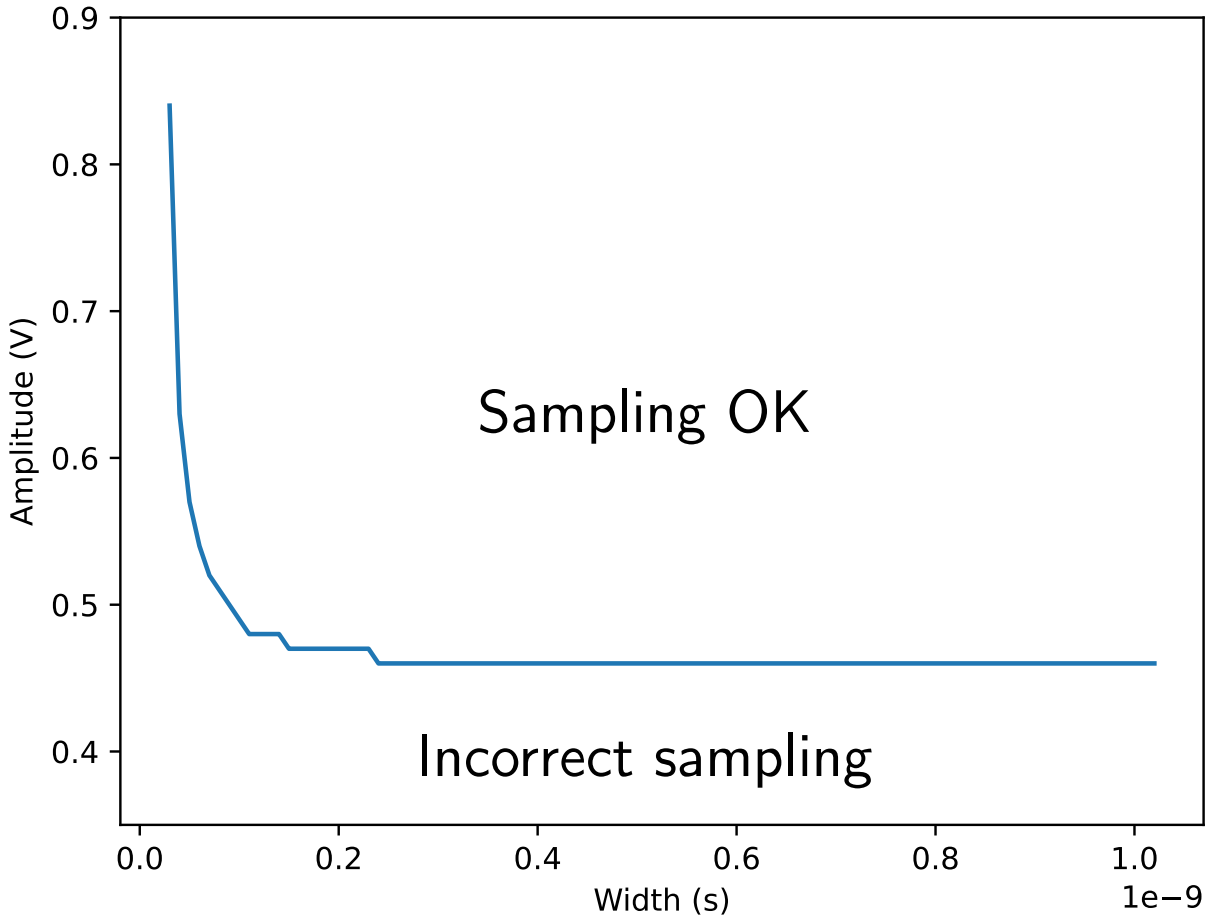


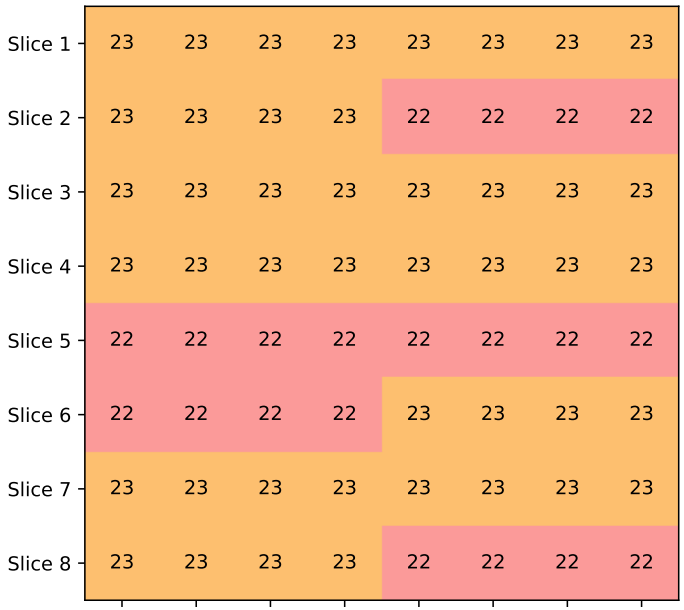
Figure: Simulated sampling results: for a given glitch with voltage amplitude and width above this curve, sampling is correct.

Hypotheses

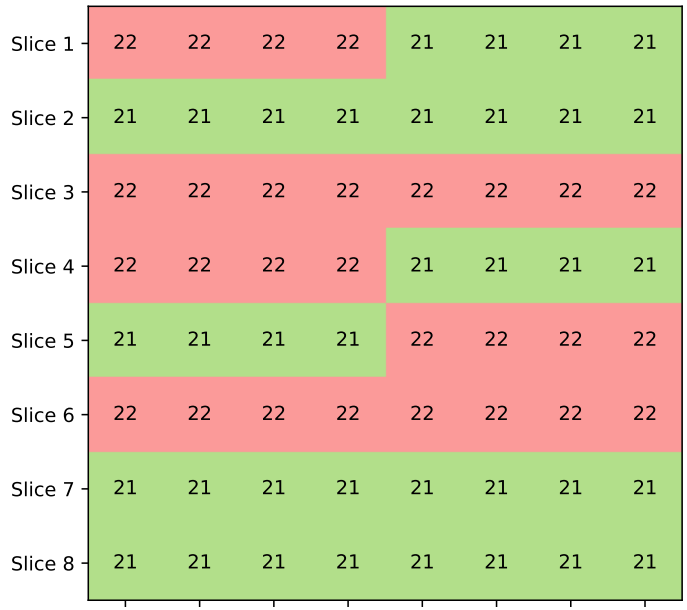
Hypothesis 2 (Fault Sensitivity Dependency on Intrinsic Properties)
The fault sensitivity of a DFF depends on its intrinsic properties, such as clock routing up to the DFF among others.

$\longrightarrow$ Only clock routing?
$\hookrightarrow$ same DUT on two Artix-7 FPGAs

Only clock routing?



(a) Color coded fault sensitivities of the first 64 registers on mapping 1 on FPGA 1.



(b) Color coded fault sensitivities of the first 64 registers on mapping 1 on FPGA 2.

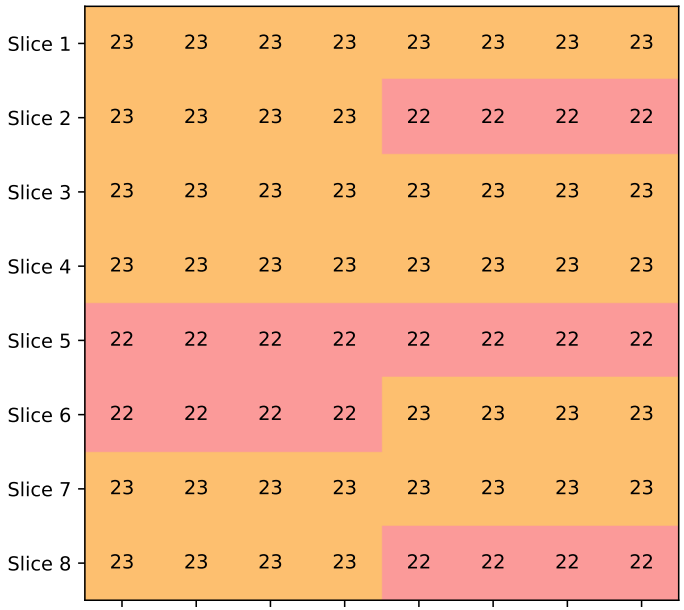
Figure: Comparing fault sensitivities between physical DFFs on two Artix-7 FPGAs.

Hypotheses

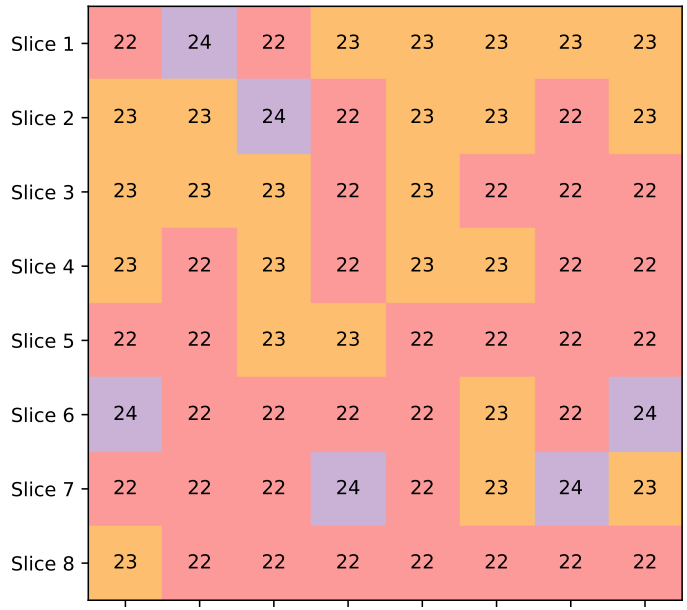
Hypothesis 2 (Fault Sensitivity Dependency on Intrinsic Properties)
The fault sensitivity of a DFF depends on its intrinsic properties, such as process variability and clock routing up to the DFF among others.

$\longrightarrow$ Only intrinsic properties?
$\hookrightarrow$ same FPGA, different mappings

Only intrinsic properties?



(a) Color coded fault sensitivities of the first 64 registers on mapping 1 *in-order* on FPGA 1.



(b) Color coded fault sensitivities of the first 64 registers on mapping 2 *randomized* on FPGA 1.

Figure: Comparing fault sensitivities between physical DFFs for different mappings.

Hypotheses

Hypothesis 3 (Fault Sensitivity Dependency on Extrinsic Properties) *The fault sensitivity of a DFF may also be affected by extrinsic factors, such as the activity in neighboring wires (including routing between DFFs and the routing of the clock tree).*

Hypotheses

Hypothesis 3 (Fault Sensitivity Dependency on Extrinsic Properties) *The fault sensitivity of a DFF may also be affected by extrinsic factors, such as the activity in neighboring wires (including routing between DFFs and the routing of the clock tree).*

$\longrightarrow$ Impact of data wires

$\hookrightarrow$ same route, different implementation

Impact of data wires

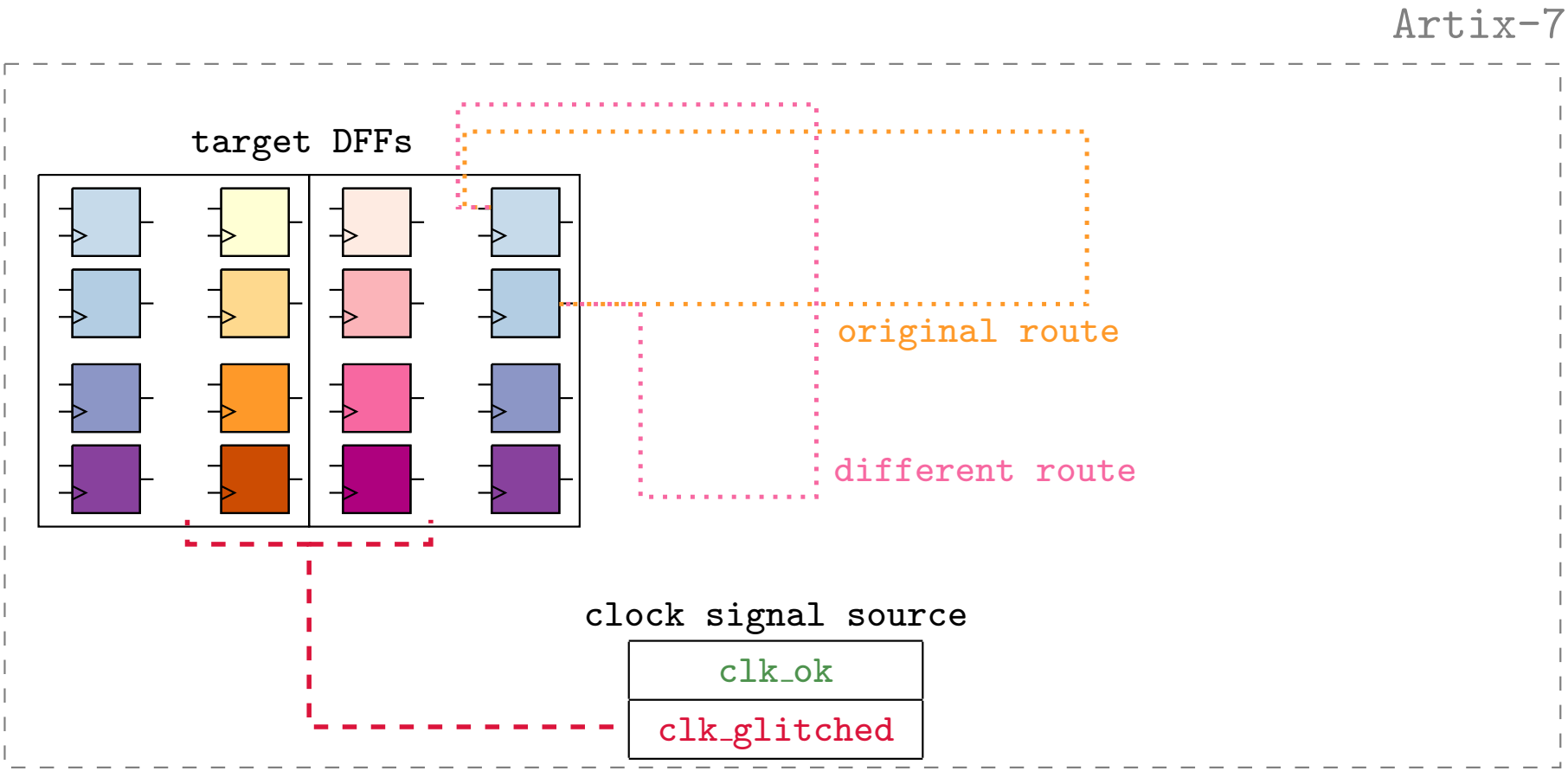
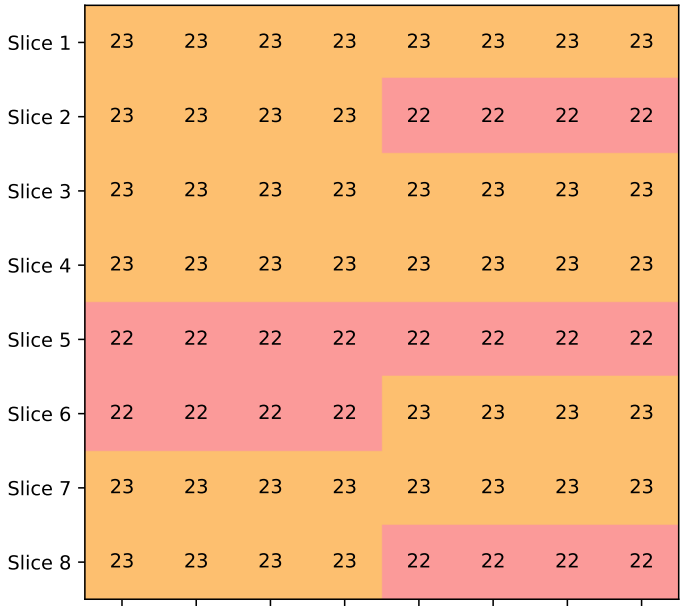
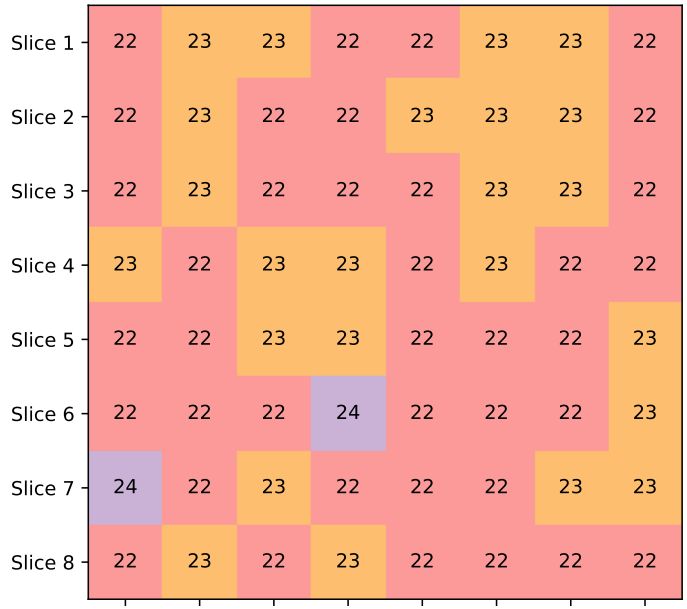


Figure: Abstract representation of the DUT placement on a Artix-7 FPGA, with route variations between two DFFs.

Impact of data wires



(a) Color coded fault sensitivities of the first 64 registers on mapping 1 *in-order* on FPGA 1.



(b) Color-coded fault sensitivities of the first 64 registers on mapping 1 *in-order* with different data routing on FPGA 1

Figure: Comparing fault sensitivities between physical DFFs for different data routing.

Hypotheses

Hypothesis 3 (Fault Sensitivity Dependency on Extrinsic Properties) *The fault sensitivity of a DFF may also be affected by extrinsic factors, such as the activity in neighboring wires (including routing between DFFs and the routing of the clock tree).*

$\longrightarrow$ Impact of clock wires

$\hookrightarrow$ forced adjacent clock paths

Impact of clock wires

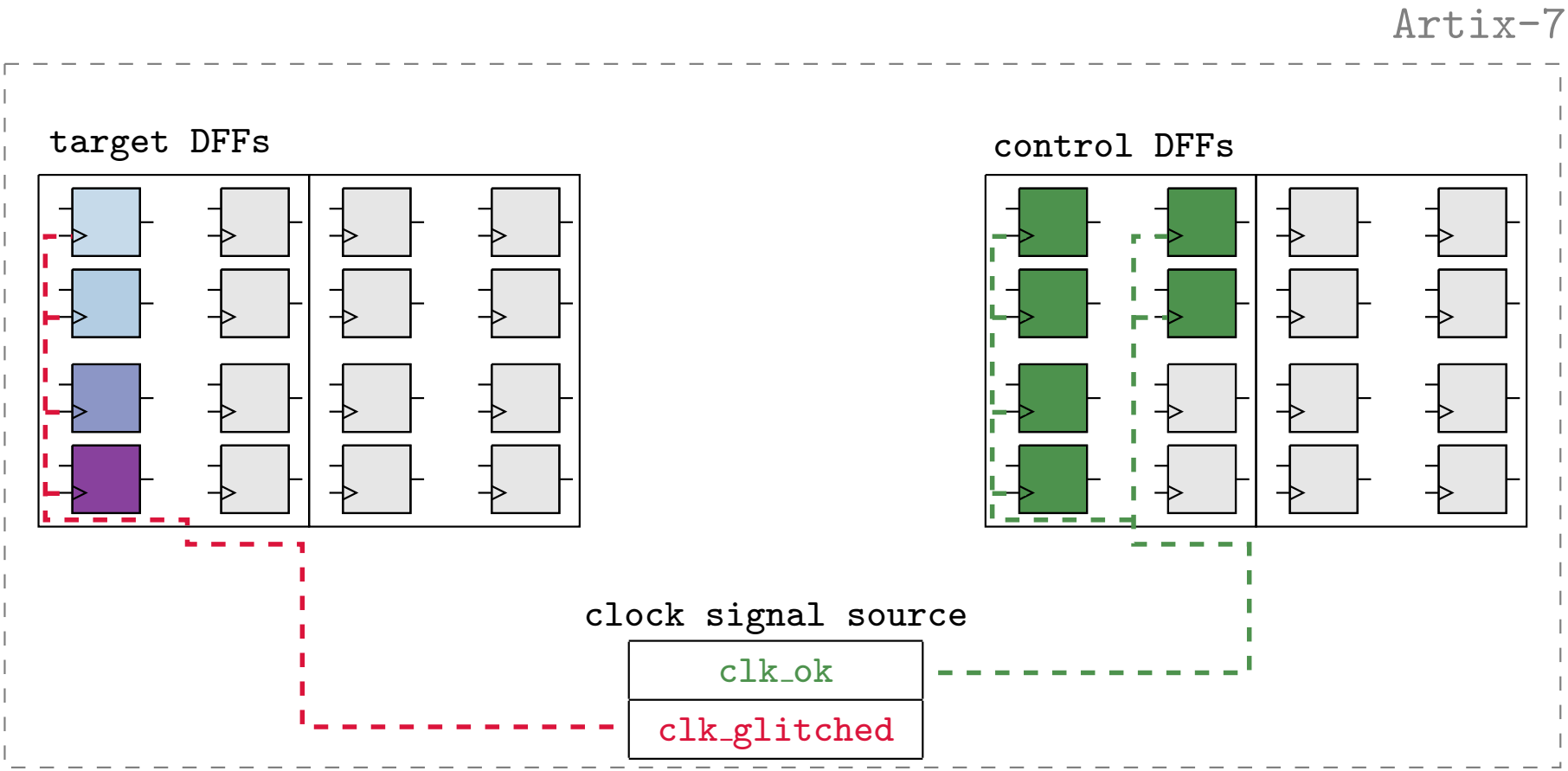


Figure: Abstract representation of the DUT placement on a Artix-7 FPGA, with clock routes forced to be apart

Impact of clock wires

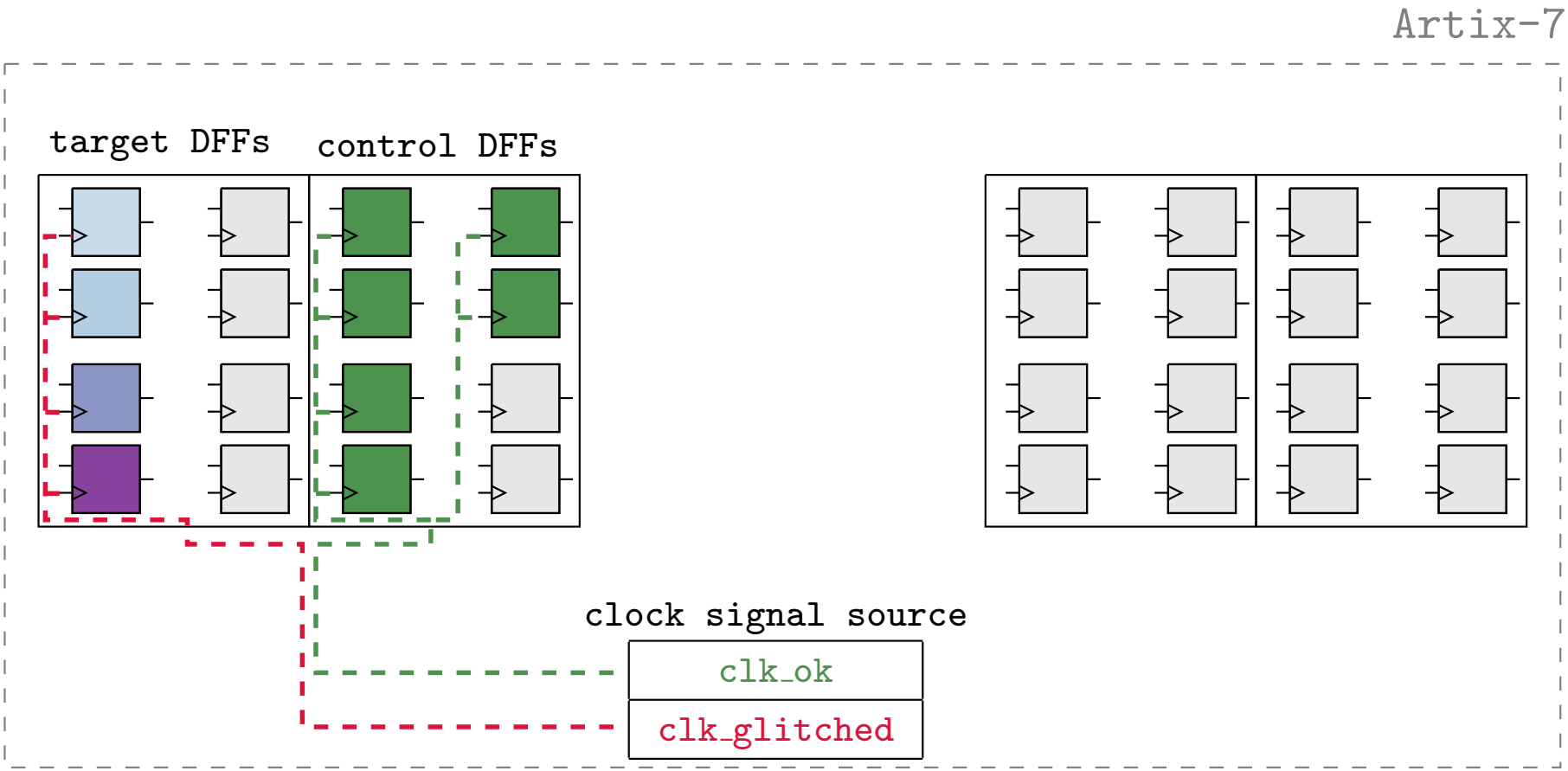
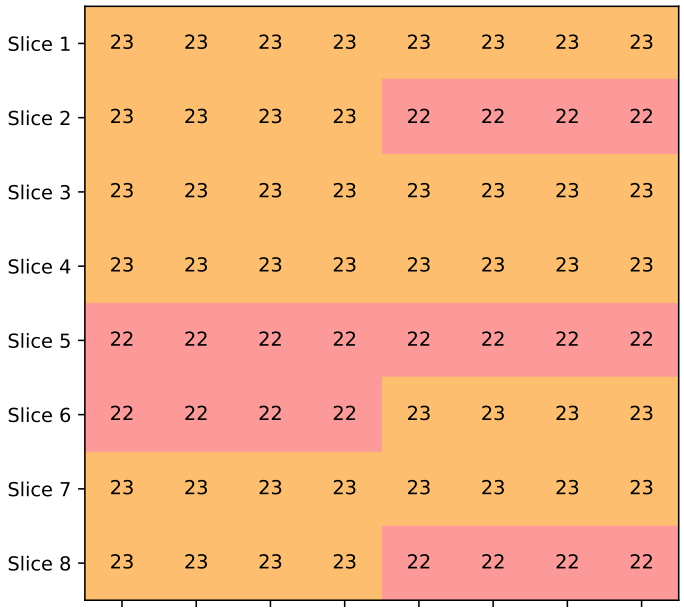
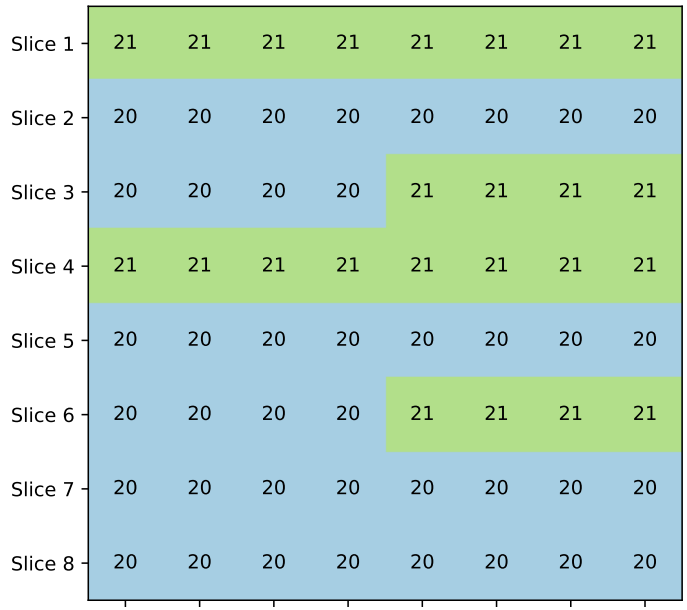


Figure: Abstract representation of the DUT placement on a Artix-7 FPGA, with clock routes forced to be parallel

Impact of clock wires



(a) Color coded fault sensitivities of the first 64 registers on mapping 1 *in-order* on FPGA 1.



(b) Color-coded fault sensitivities of the first 64 registers on mapping 1 *in-order* with a forced adjacent path for the clock on FPGA 1

Figure: Comparing fault sensitivities between physical DFFs for different clock routing.

Conclusion

$\Longrightarrow$ the Energy-Threshold Fault Model

1. For a DFF to correctly sample a clock's rising edge, the clock signal must meet a certain energy threshold
2. The threshold of a DFF varies based on intrinsic properties (clock routing, process variability)
3. The threshold of a DFF can be influenced by extrinsic properties (acitivity of neighbouring wires) due to cross-talk

$\Longrightarrow$ Future work: recreate the synchronous clock glitch with EMFI and verify if the Energy-threshold Fault Model requires adjusments

Bibliography

Ludovic Claudepierre and Philippe Besnier.
Microcontroller Sensitivity to Fault-Injection Induced by Near-Field Electromagnetic Interference.
In *APEMC - Asia-Pacific International Symposium on Electromagnetic Compatibility*, pages 1–4, Sapporo, Japan, June 2019.

Ludovic Claudepierre, Pierre-Yves Péneau, Damien Hardy, and Erven Rohou.
TRAITOR: A Low-Cost Evaluation Platform for Multifault Injection.
In Weizhi Meng and Li Li, editors, *ASSS'21: Proceedings of the 2021 International Symposium on Advanced Security on Software and Systems, Virtual Event, Hong Kong*, pages 51–56. ACM, June 2021.

Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, and Assia Tria.
Electromagnetic Transient Faults Injection on a Hardware and a Software Implementations of AES.
In Guido Bertoni and Benedikt Gierlichs, editors, *Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, Belgium*, pages