

RUHR-UNIVERSITÄT BOCHUM

# Early Propagation and Imbalanced Routing, How to Diminish in FPGAs

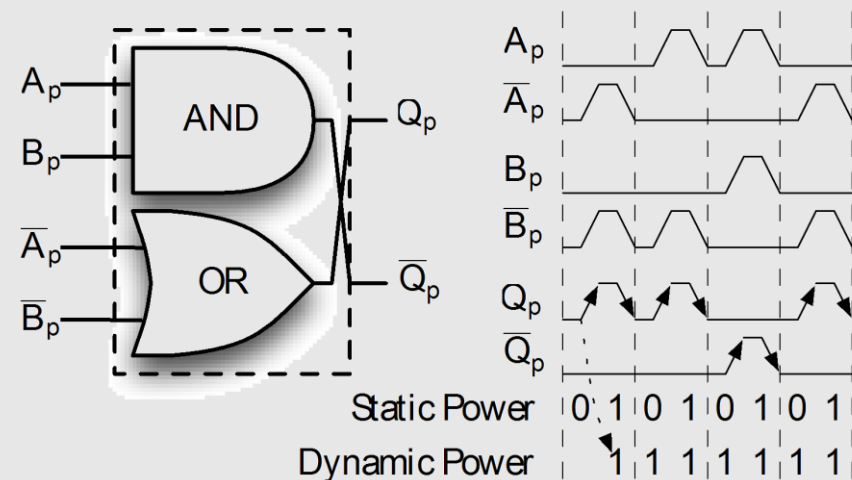
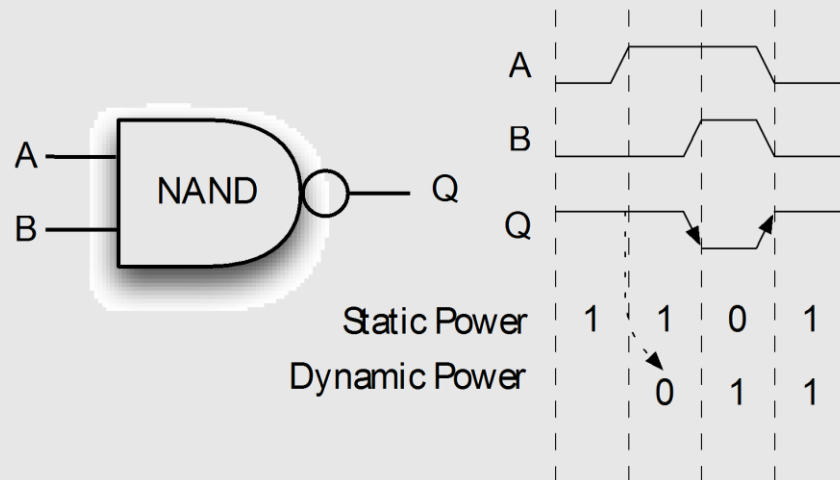
**26. September 2014**

**Amir Moradi** and Vincent Immler

Ruhr University Bochum, Fraunhofer Institution Munich

# Story?

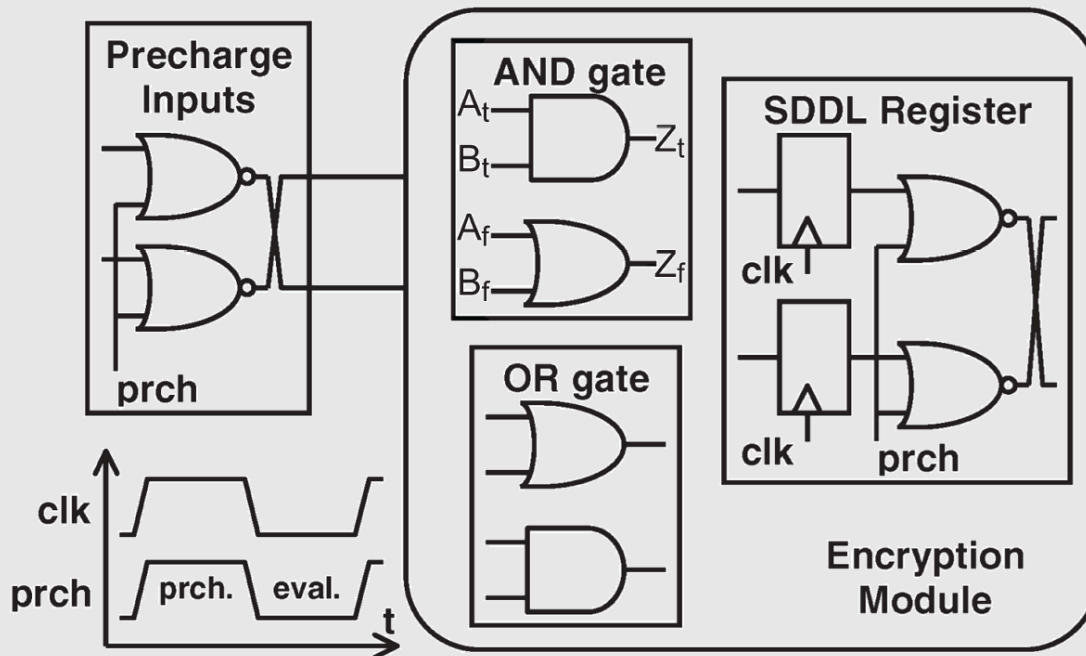
- 'Flatten' power consumption using complementary signals
- Fix number of toggles using Dual-Rail Pre-Charge Logic (DPL)



# Story?

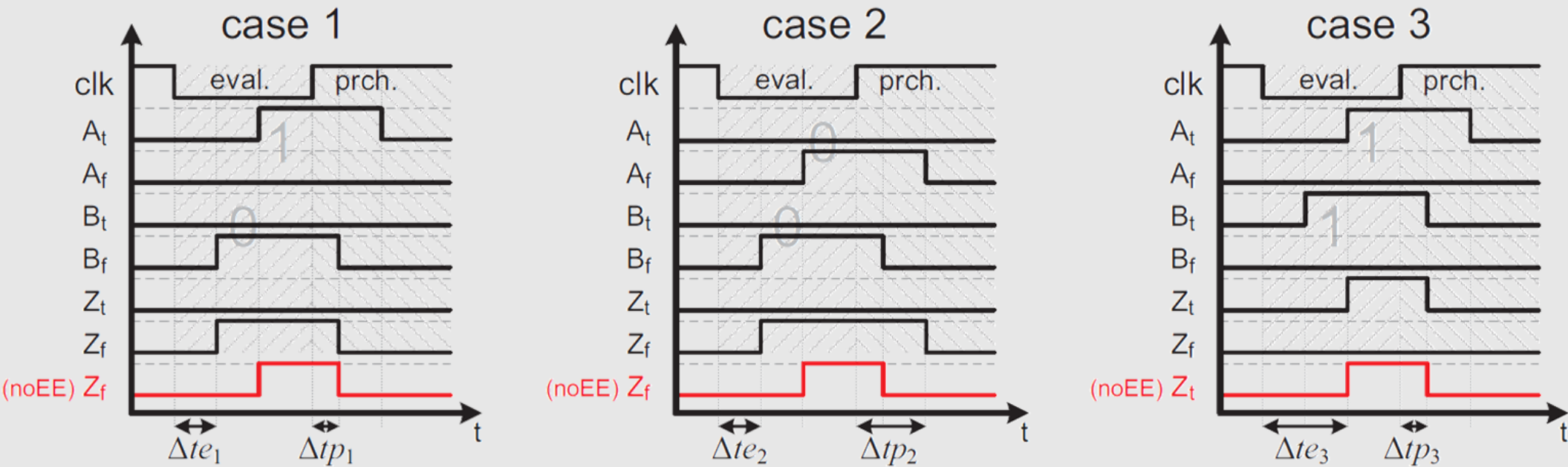
- Examples

WDDL



# Early Propagation

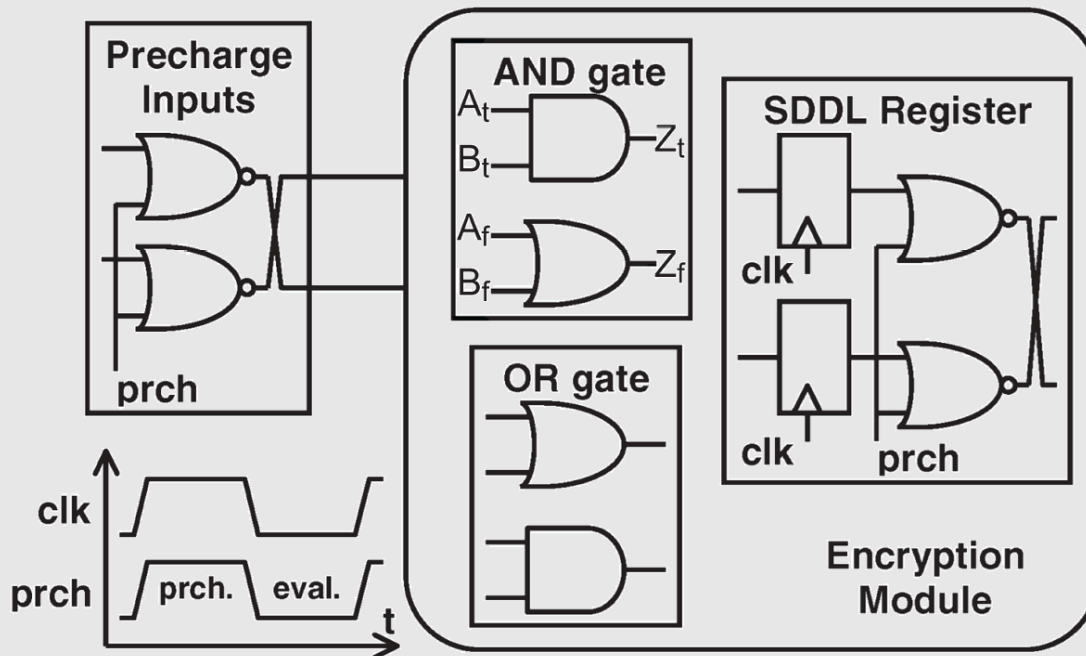
Delay(A) > Delay(B)



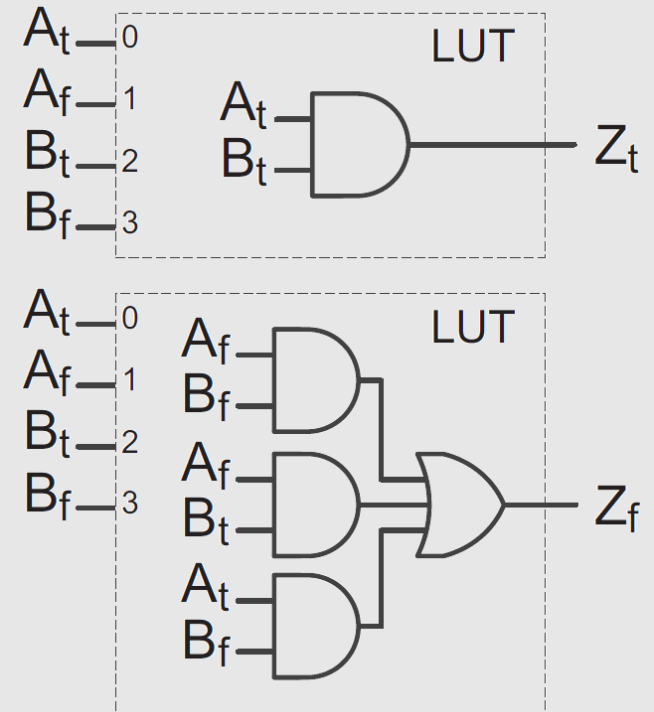
# Story?

- Examples

## WDDL

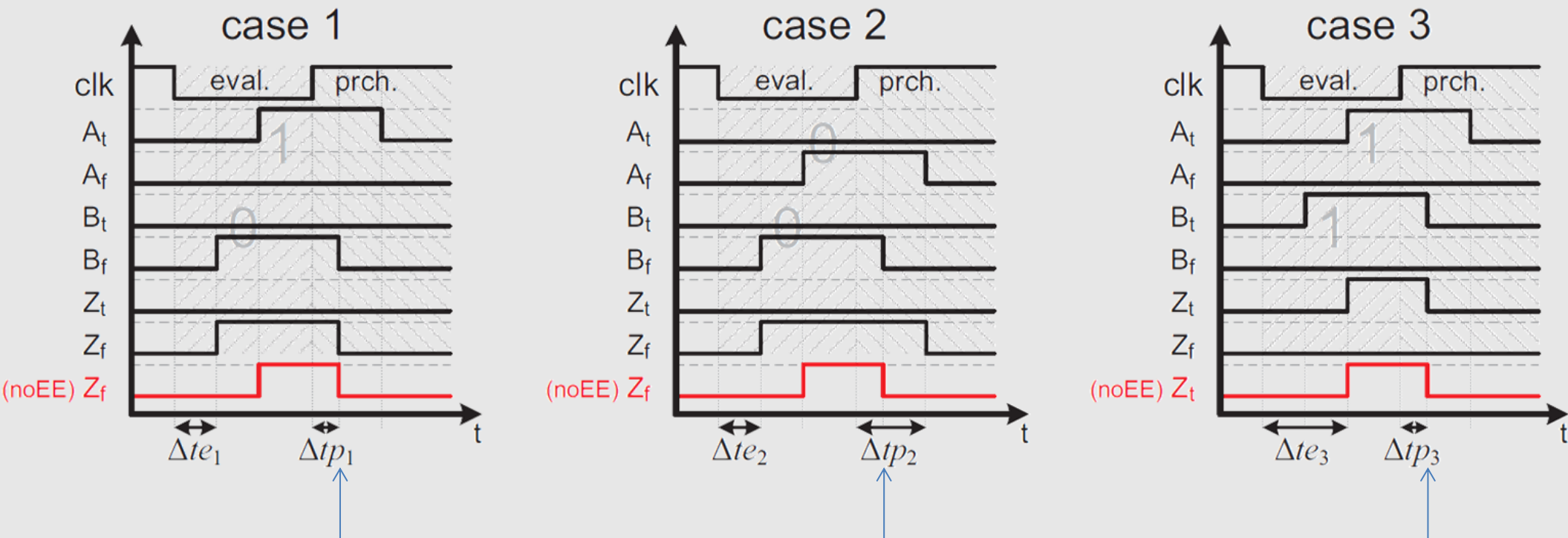


## DPL\_noEE



# Early Propagation

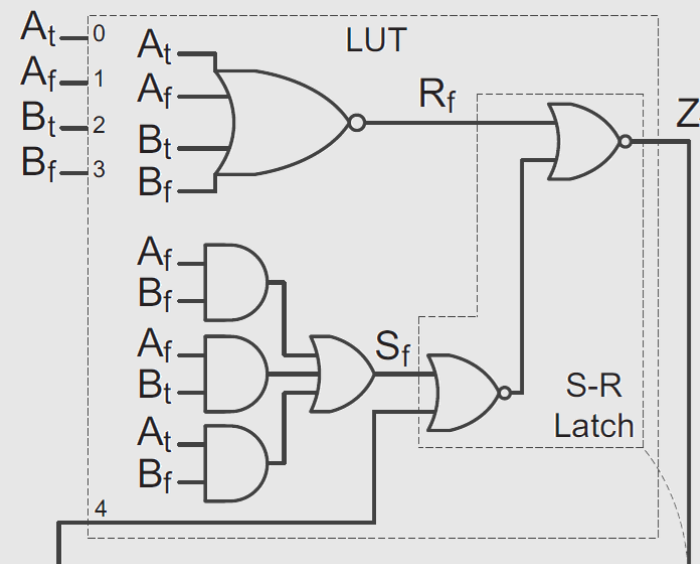
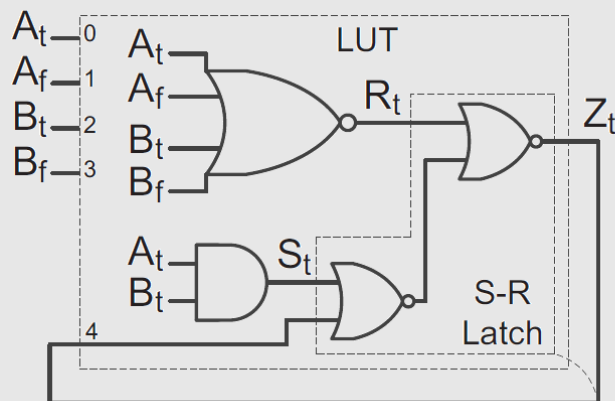
- Delay(A) > Delay(B)



- precharge phase starts once an input is in precharge

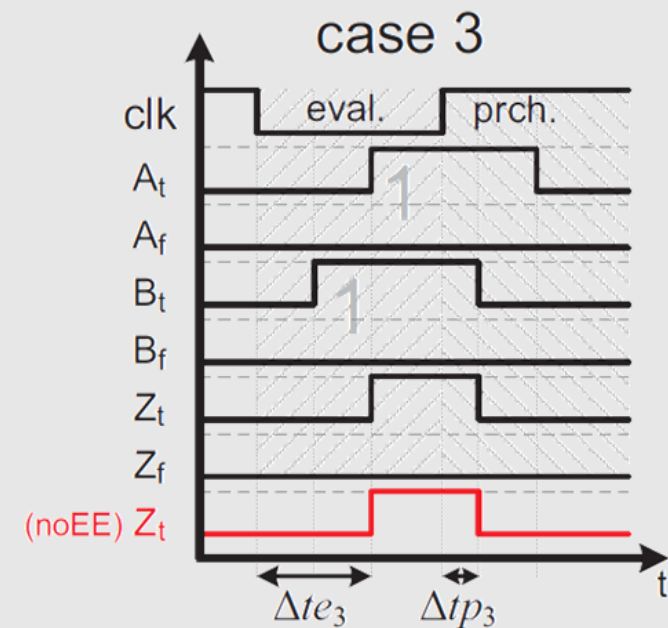
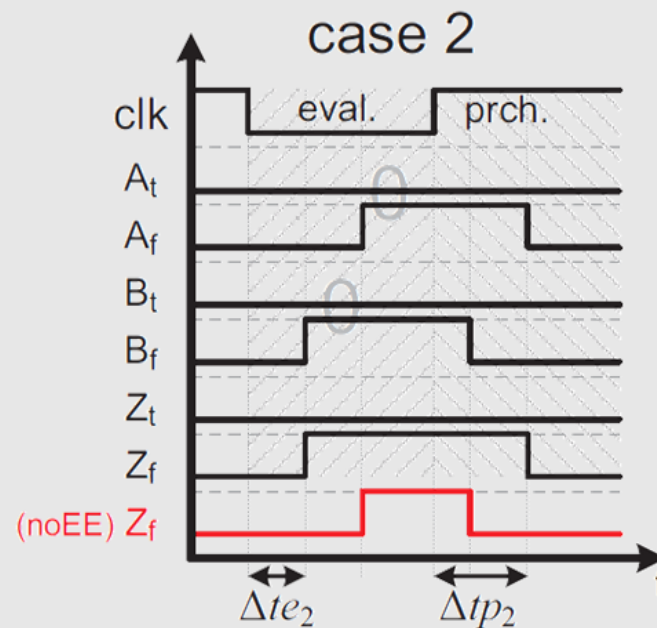
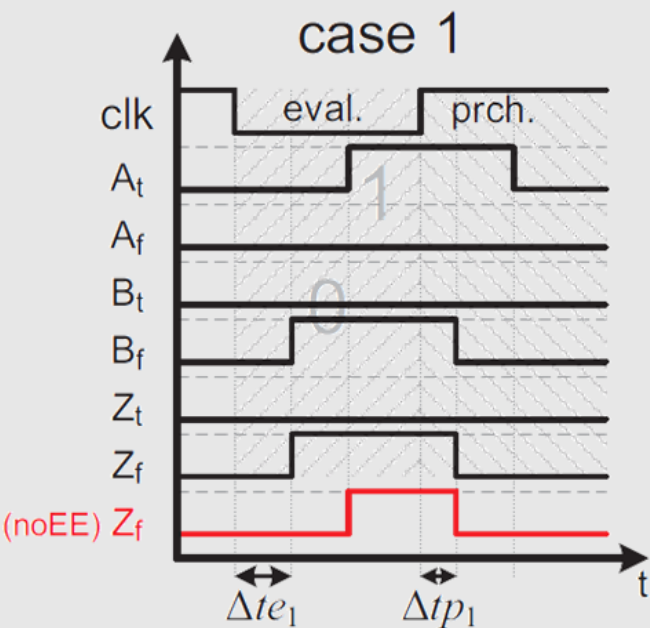
# What to do in precharge phase?

- borrow knowledge from asynchronous circuit design
- form S-R latches by a feedback loop
  - evaluation works as DPL\_noEE
  - precharge does not start till all inputs in precharge
- the first (FPGA-based) logic with no early propagation in both phases



# Early Propagation

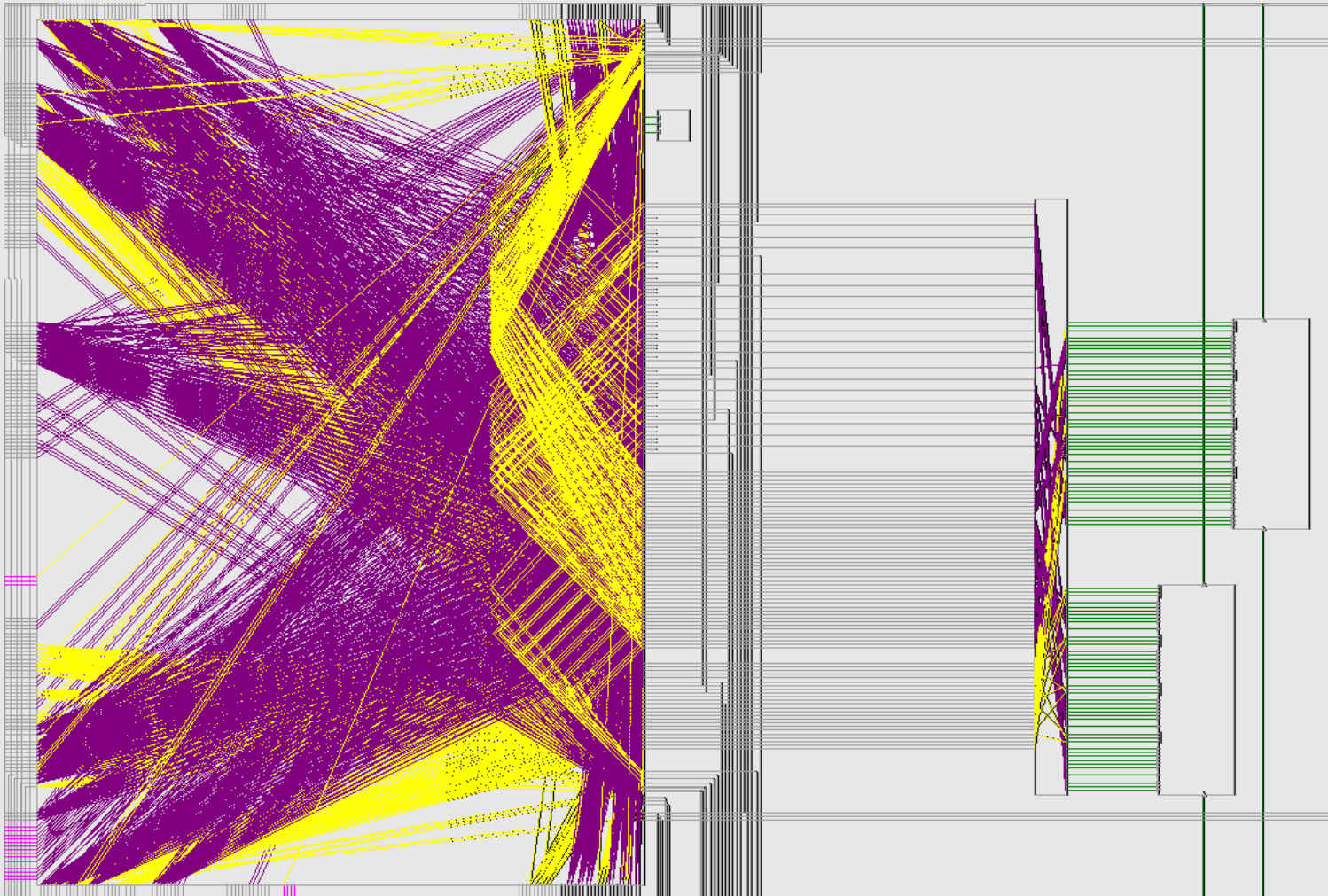
- Delay (A) > Delay (B)
- Delay (A<sub>f</sub>) = Delay (A<sub>t</sub>)
- Delay (B<sub>f</sub>) = Delay (B<sub>t</sub>)



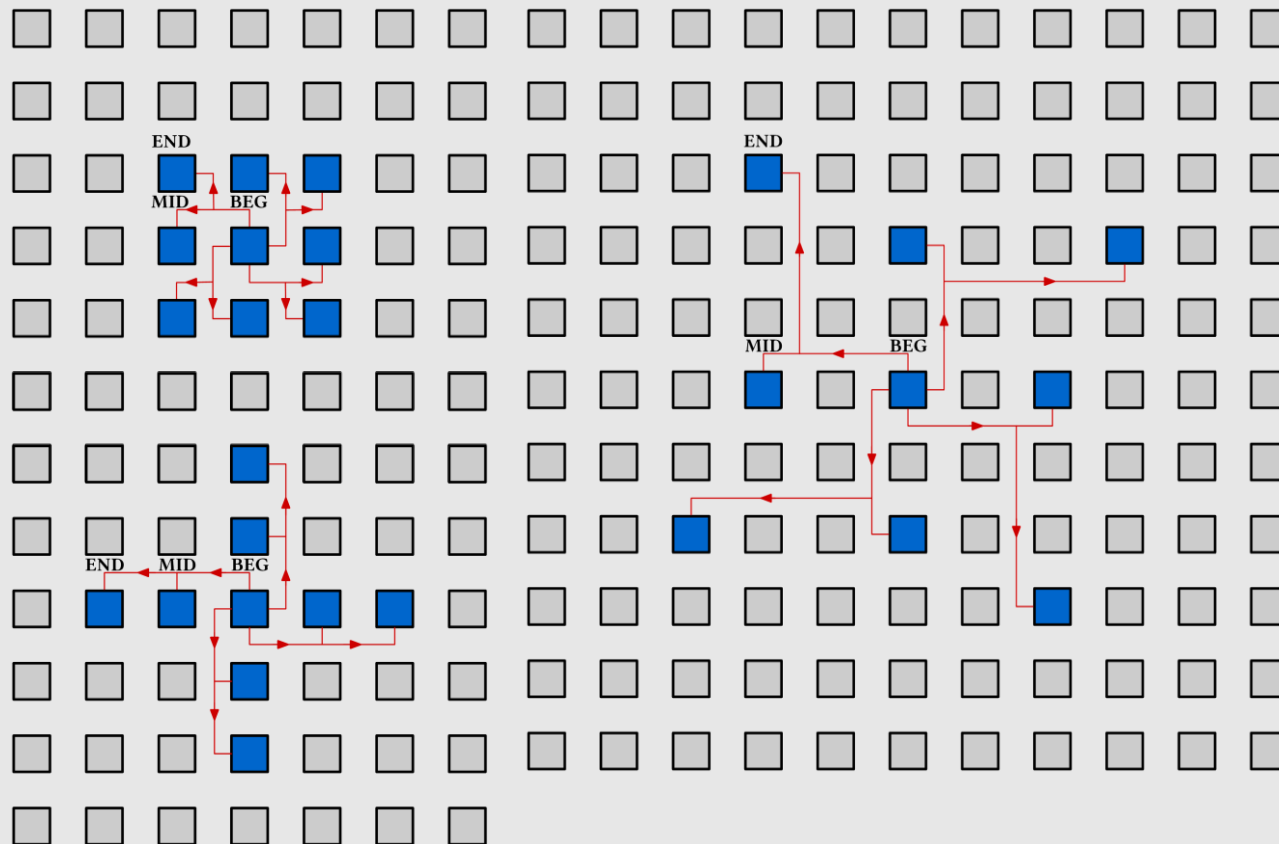
# Balanced Routings

- If not considered, the same principle as early propagation
- Problem of most DRP logics
  - some solutions for ASIC, e.g., fat-wire approach
  - no way for FPGAs
    - missing routing flexibilities
    - no control over routing via FPGA standard tools
    - conceptual routing delays

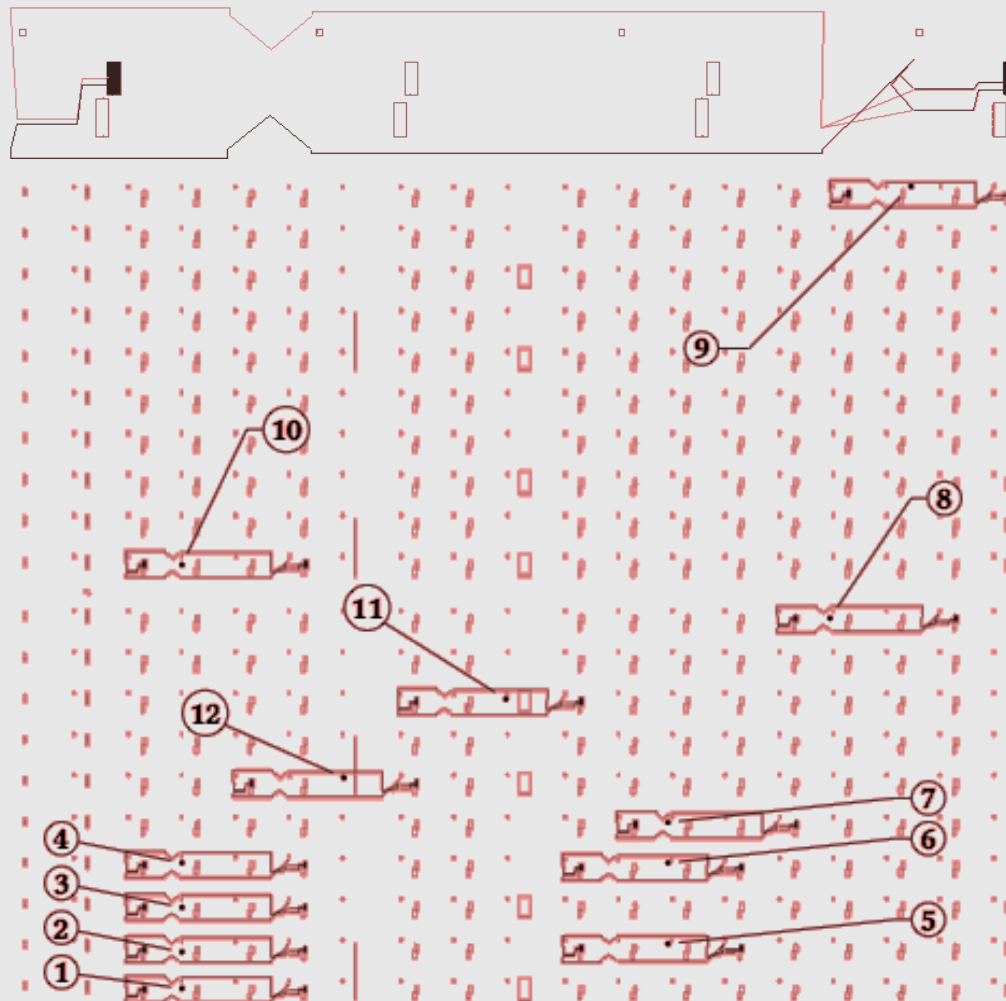
# Representation in Xilinx FPGA Editor



# FPGA Routing Architecture



# Brief Analysis of Virtex-5 Routing Architecture



| #  | $d(m_1)$ | $d(m_0)$ | $ \Delta d $ | Slice Source | Slice Sink |
|----|----------|----------|--------------|--------------|------------|
| 1  | 1018     | 1018     | 0            | X1Y0         | X7Y0       |
| 2  | 1015     | 1013     | 2            | X1Y1         | X7Y1       |
| 3  |          |          | 2            |              |            |
| 4  |          |          | 2            |              |            |
| 5  |          |          | 2            |              |            |
| 6  | 1007     | 1009     | 2            | X13Y3        | X13Y3      |
| 7  |          |          | 2            |              |            |
| 8  |          |          | 2            |              |            |
| 9  |          |          | 2            |              |            |
| 10 |          |          | 4            |              |            |
| 11 | 1030     | 1032     | 2            | X9Y7         | X13Y7      |
| 12 | 1097     | 1100     | 3            | X5Y5         | X9Y5       |

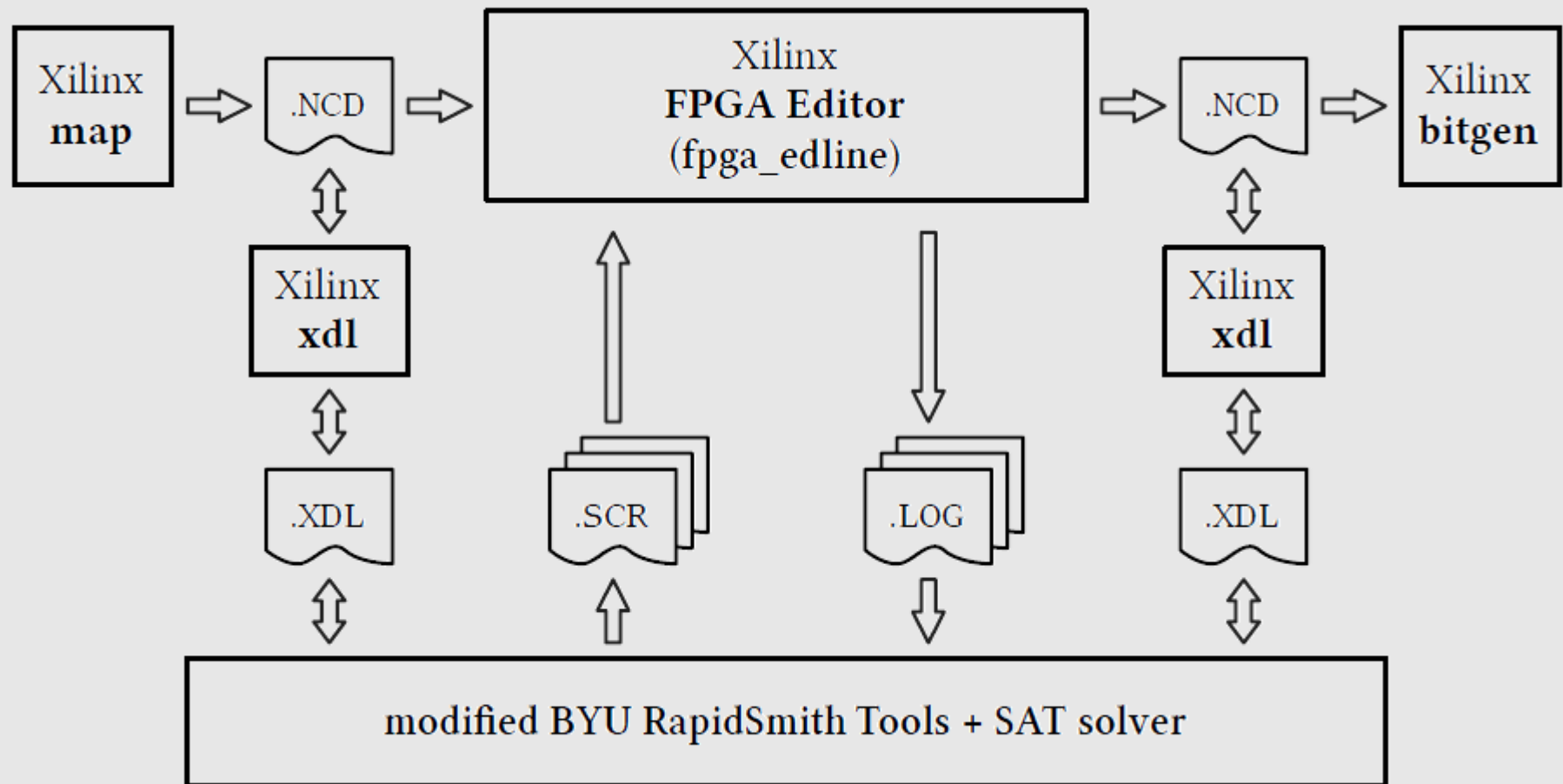
# Routing Issues

- No documentation of switch box from Xilinx
- No support for balanced rails in any FPGA related tool
- No API for extracting relevant information / FPGA Editor
- Two open source projects target this issue:
  - Torc (Tools for Open Reconfigurable Computing, written in C++)
  - Rapidsmith (written in Java)
- Both use unsupported intermediate file format:
  - XDL (Xilinx Design Language)
  - Human-readable file format equivalent to proprietary NCD format

# Our Solution

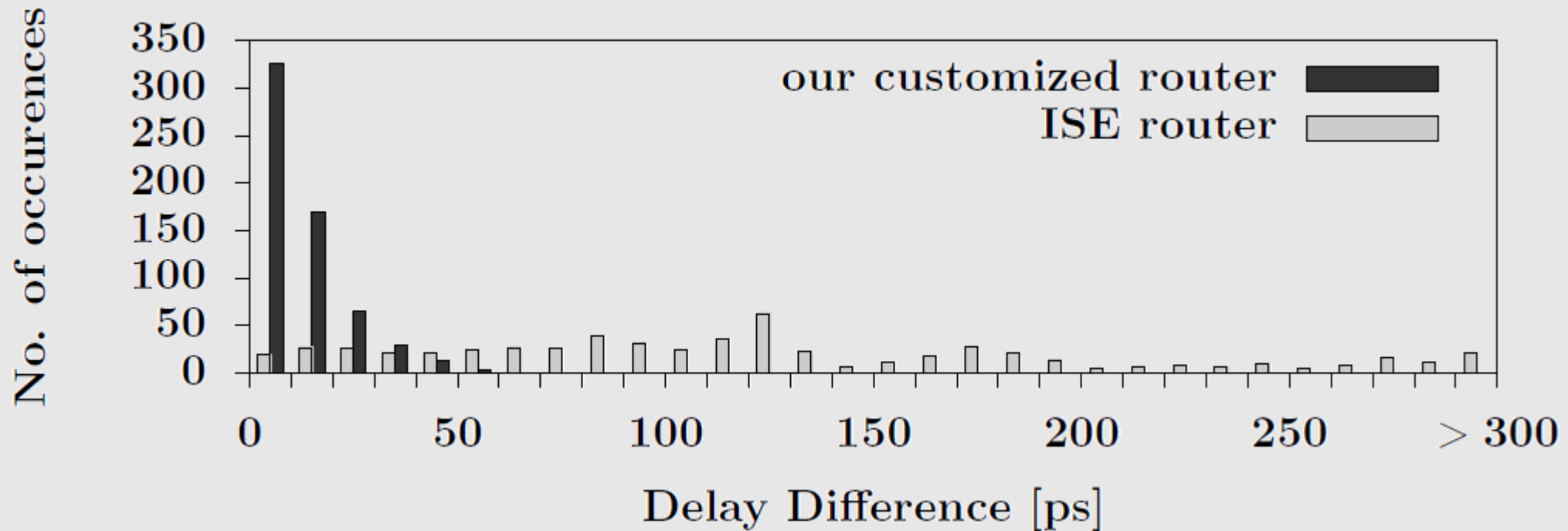
- for every dual-rail route, all possible routes are extracted
- based on the delay of the routes reported by *Xilinx FPGA Editor*
- customized router
  - parsing and modifying XDL file by *RapidSmith*
  - routing algorithm, sat solver, ...
    - achieving the best possible route with minimal delay difference between the rails

# Our Solution



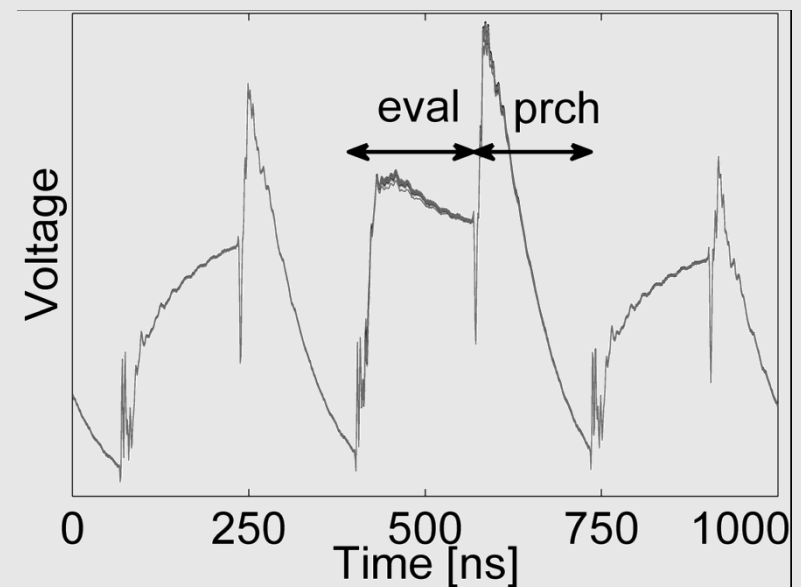
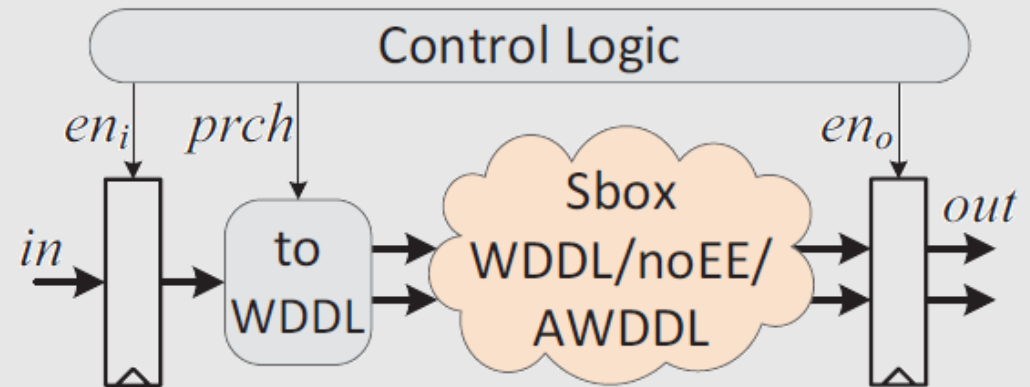
## Case Study

- again Canright Sbox 😊
- 122 gates, 606 dual-rail routes



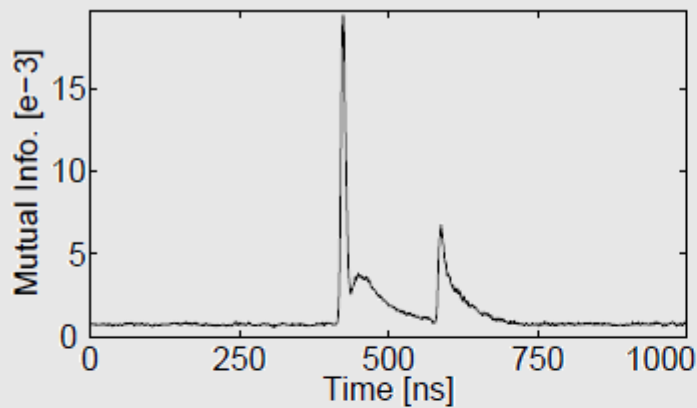
## Case Study

- SASEBO-GII (Virtex-5)
- Profiles to compare
  - WDDL, Xilinx routing
  - DPL\_noEE, Xilinx routing
  - AWDDL, Xilinx routing
  - AWDDL, customized routing

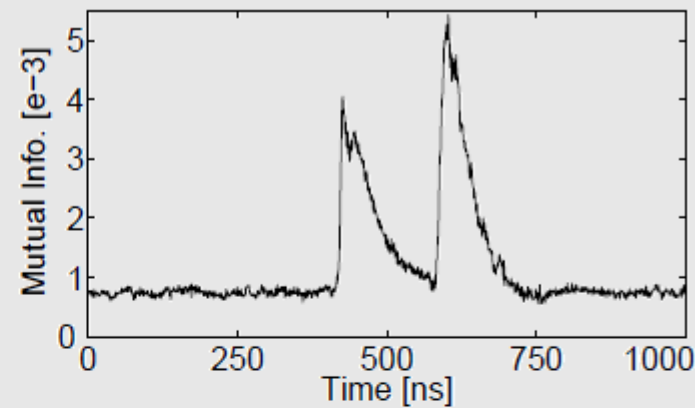


# Mutual (Perceived) Information

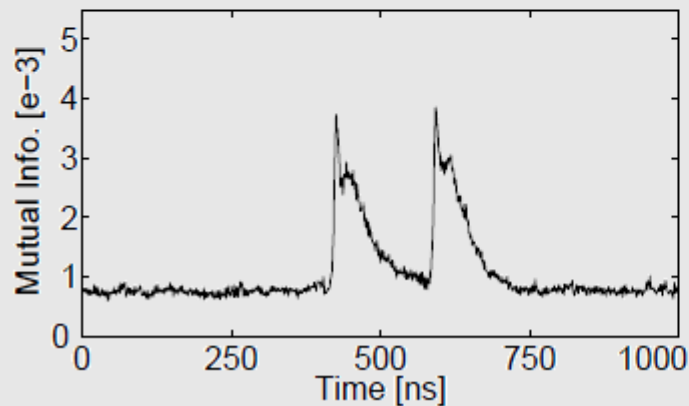
based on 500k traces



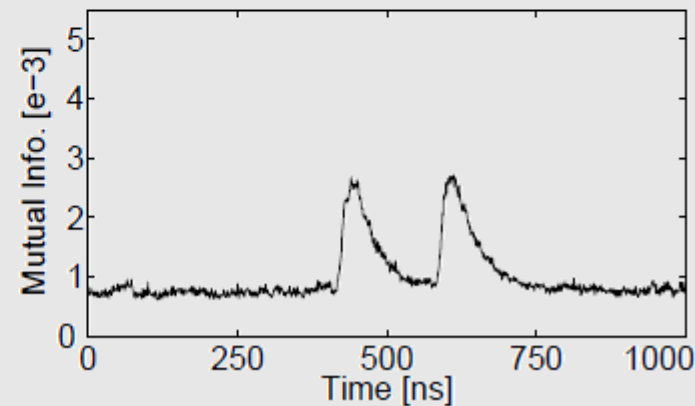
(a) WDDL



(b) DPL\_noEE



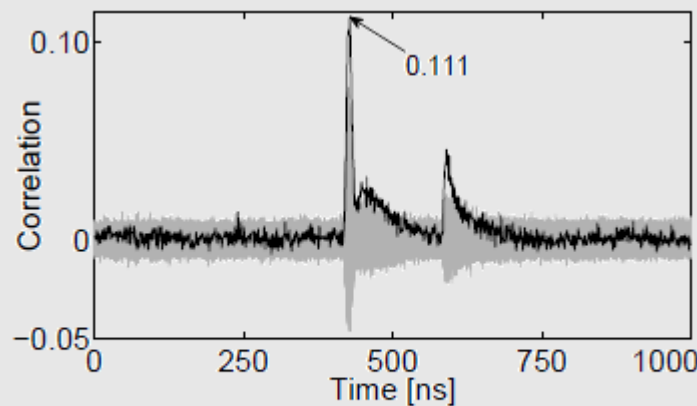
(c) AWDDL



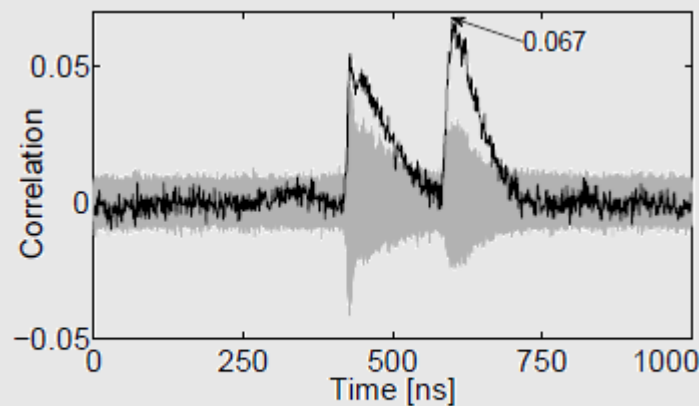
(d) AWDDL (custom routing)

# Moments-correlating DPA

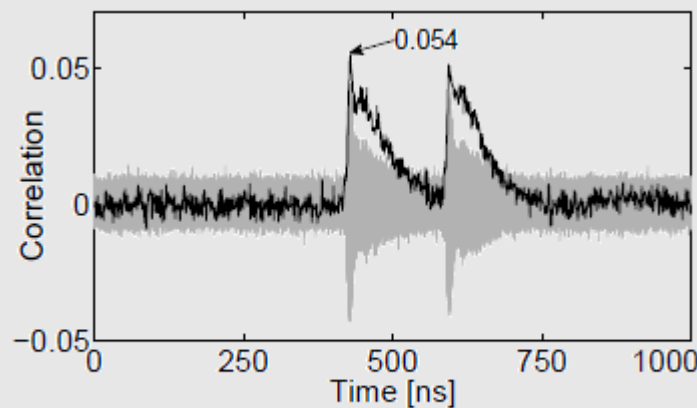
500k traces for profiling, another 500k traces for the attack



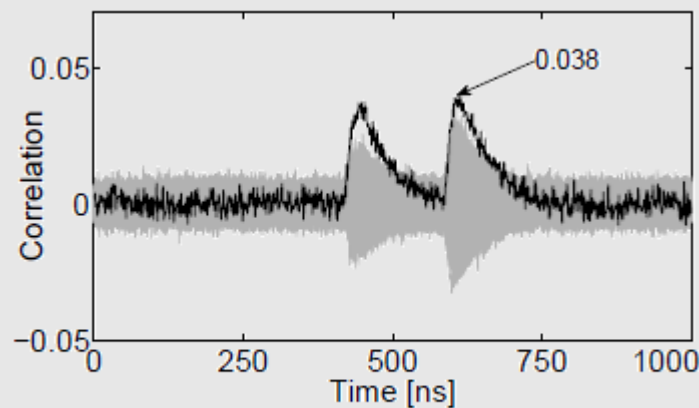
(a) WDDL



(b) DPL\_noEE



(c) AWDDL



(d) AWDDL (custom routing)

## Final Message

- By the customized router there is still a detectable leakage
  - a perfect dual-rail route with null delay difference does not always exist for all routes
  - in case of their existence, all such routes cannot be selected without conflict
  - the customized router is based on delay report of Xilinx tools
    - worst-case simulation results
    - diverse/different in practice due to process variations
  - measuring such device-specific delay differences is in progress



# Thanks!

## Any questions?

[amir.moradi@rub.de](mailto:amir.moradi@rub.de)

Embedded Security Group, Ruhr University Bochum, Germany