RUB

RUHR-UNIVERSITÄT BOCHUM
Horst Görtz Institute for IT-Security

# Evaluating the Duplication of Dual-Rail Logics on FPGAs

Alexander Wild, Amir Moradi, Tim Güneysu

**April 13. 2015**

hgi
Horst Görtz Institute
for IT-Security

# Motivation

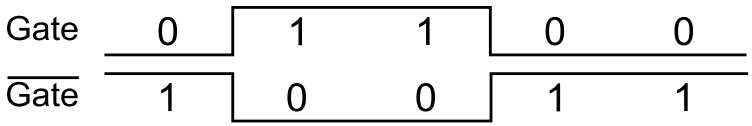
## Dual-rail precharge logic

# Motivation

## Dual-rail precharge logic

### Dual-rail logic

- Differential encoding
- Valid values: 10 or 01
- No inverter

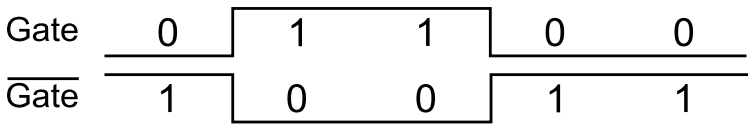


# Motivation

## Dual-rail precharge logic

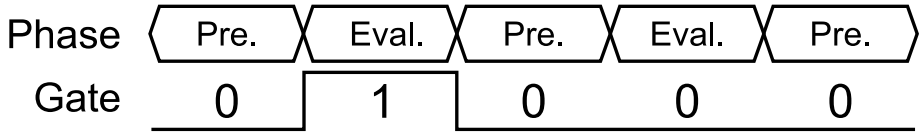
### Dual-rail logic

- Differential encoding
- Valid values: 10 or 01
- No inverter




### Precharge logic

- Alternates between precharge and logic value
  - Precharge phase
  - Evaluation phase

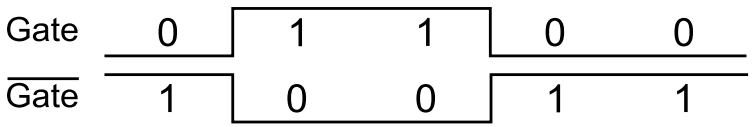


# Motivation

## Dual-rail precharge logic

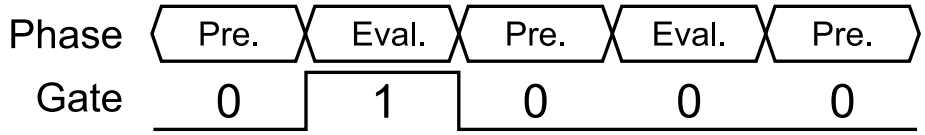
### Dual-rail logic

- Differential encoding
- Valid values: 10 or 01
- No inverter



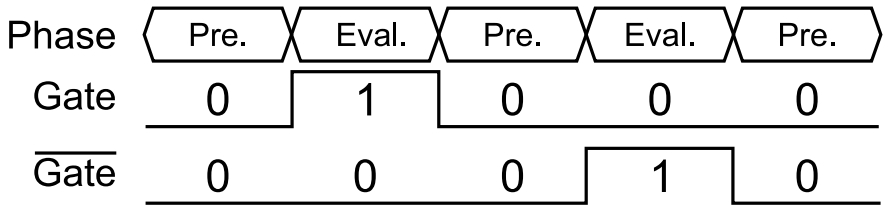

### Precharge logic

- Alternates between precharge and logic value
  - Precharge phase
  - Evaluation phase




### Dual-rail precharge logic

- Differential encoding
  - Precharge phase: 00 or 11
  - Evaluation phase 01 or 10
- One transition per phase

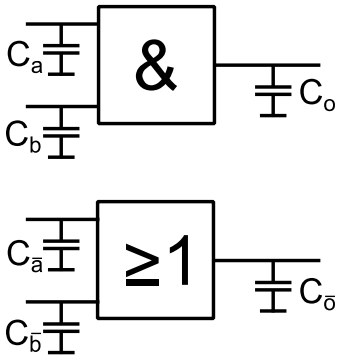


# Motivation

## Pitfalls

Signal delays/capacitance

- Different signal routings.

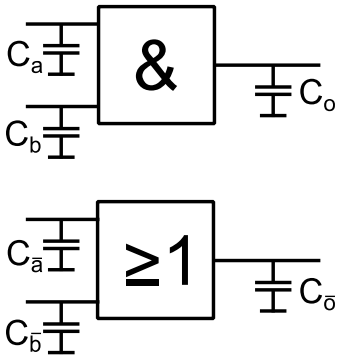


# Motivation

## Pitfalls

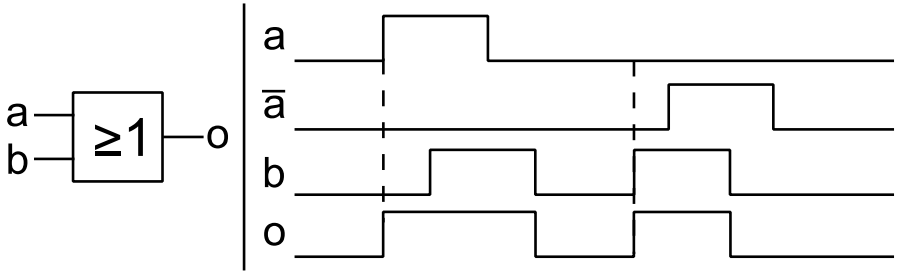
### Signal delays/capacitance

- Different signal routings.




### Early Evaluation

- Transition based on the arriving signals.
- Different and data-dependent point of evaluation.



# Motivation

## Logic Styles

# Motivation

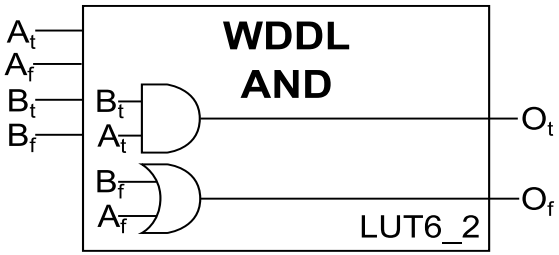
## Logic Styles

## WDDL

K. Tiri and I. Verbauwhede

DATE‘04

- No Glitches



# Motivation

## Logic Styles

### WDDL

K. Tiri and I. Verbauwhede

DATE‘04

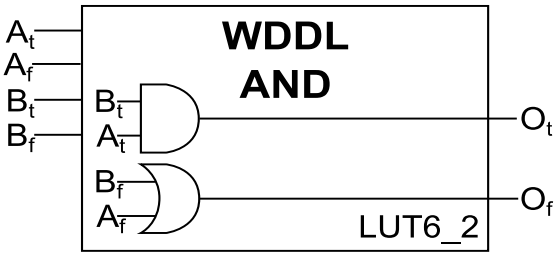
- No Glitches

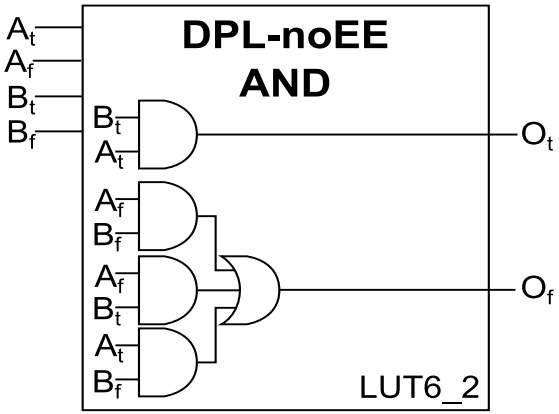
### DPL-noEE

S. Bhasin et al.

WESS‘10

- No Glitches
- No Early Evaluation



# Motivation

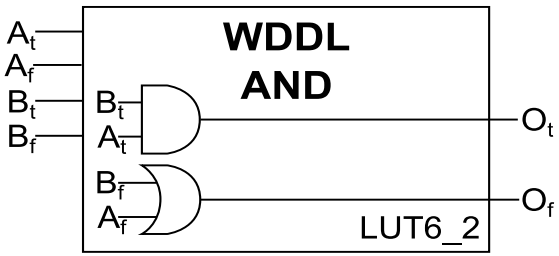
## Logic Styles

### WDDL

K. Tiri and I. Verbauwhede

DATE‘04

- No Glitches

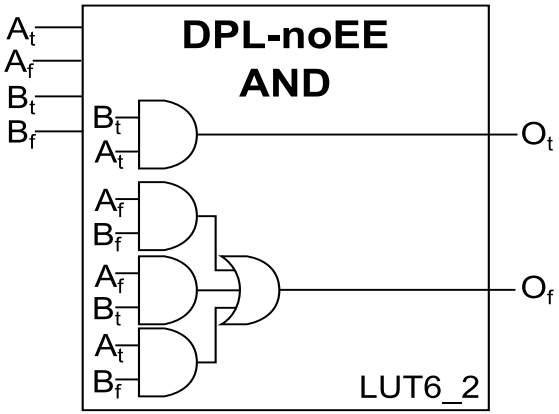



### DPL-noEE

S. Bhasin et al.

WESS‘10

- No Glitches
- No Early Evaluation

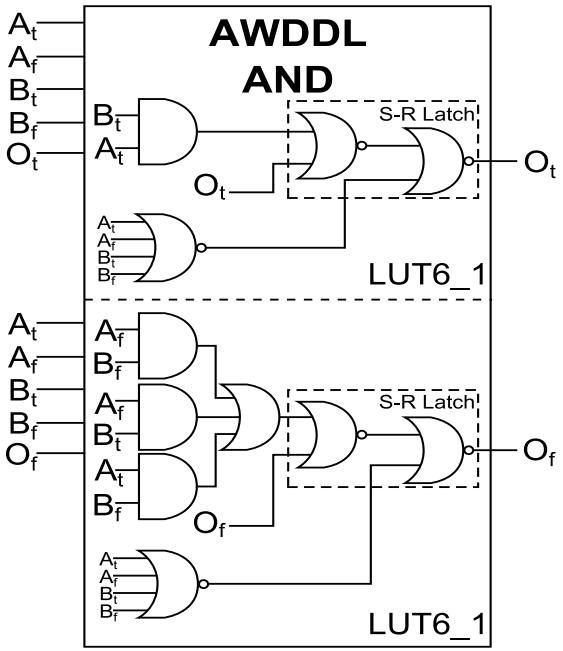



### AWDDL

A. Moradi and V. Immler

CHES‘14

- No Glitches
- No Early Propagation



# Motivation

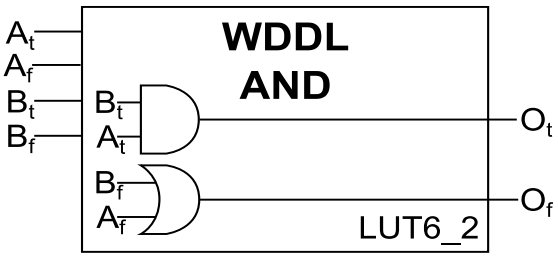
## Logic Styles

### WDDL

K. Tiri and I. Verbauwhede

DATE‘04

- No Glitches

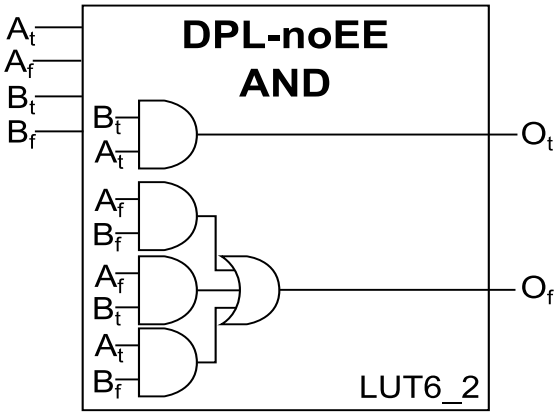



### DPL-noEE

S. Bhasin et al.

WESS‘10

- No Glitches
- No Early Evaluation

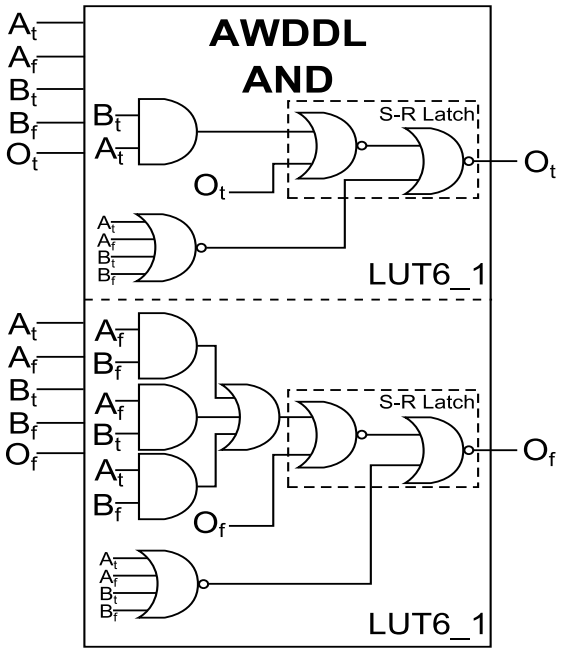



### AWDDL

A. Moradi and V. Immler

CHES‘14

- No Glitches
- No Early Propagation



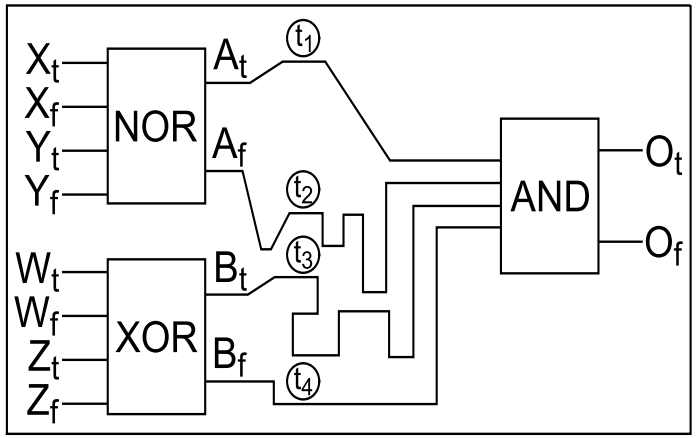

Wire Capacities / Routing imbalances!

# Motivation

## Duplication

### DWDDL

P. Yu, P. Schaumont CODES+ISSS‘07

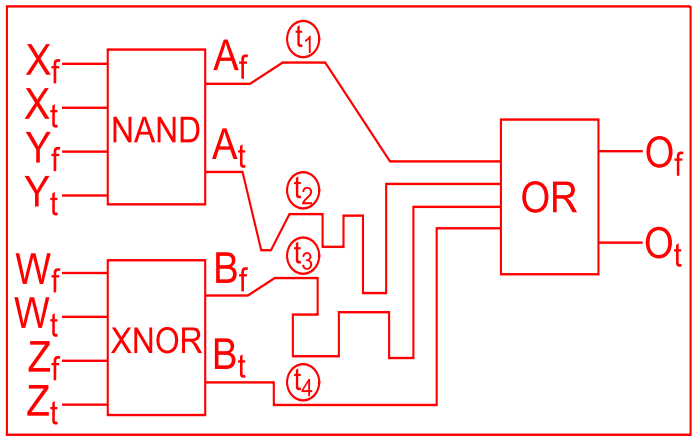


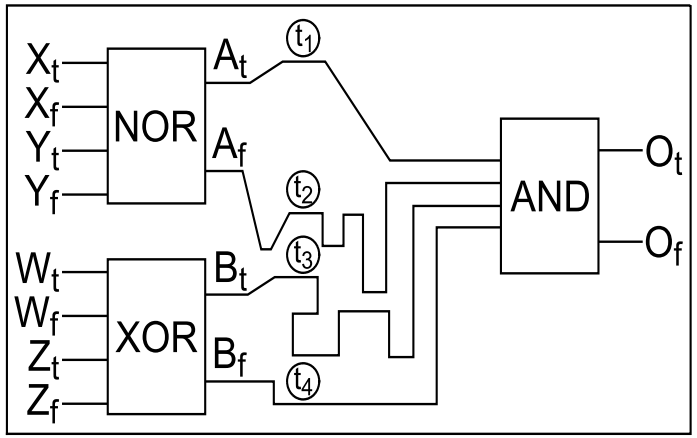
# Motivation

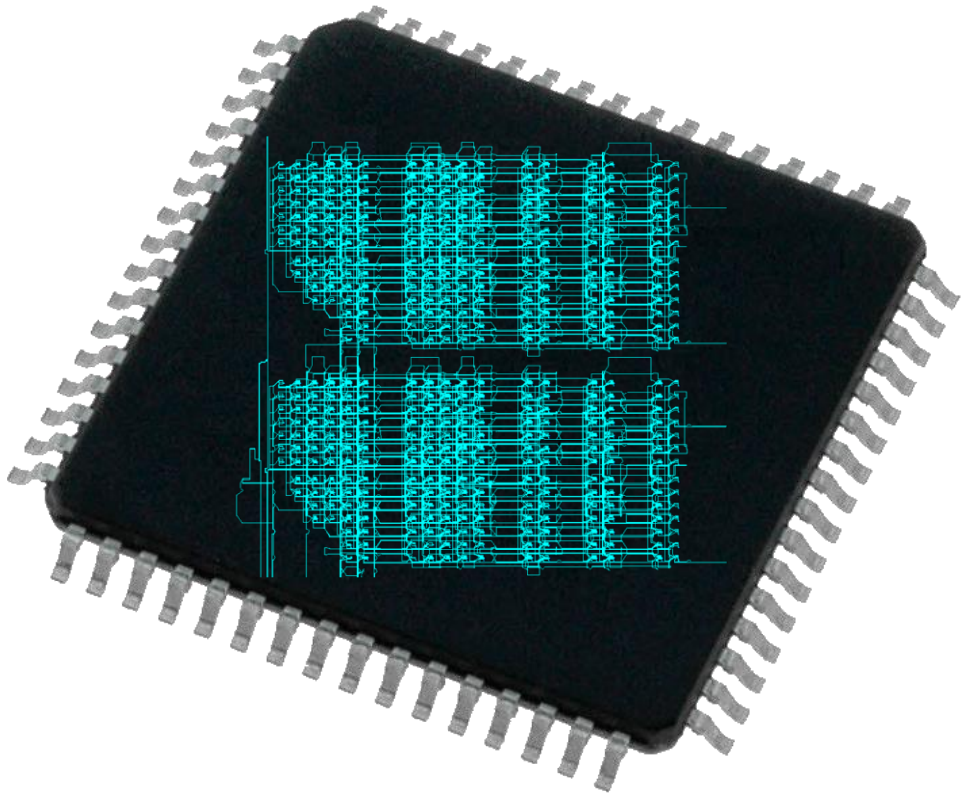
## Duplication

## DWDDL

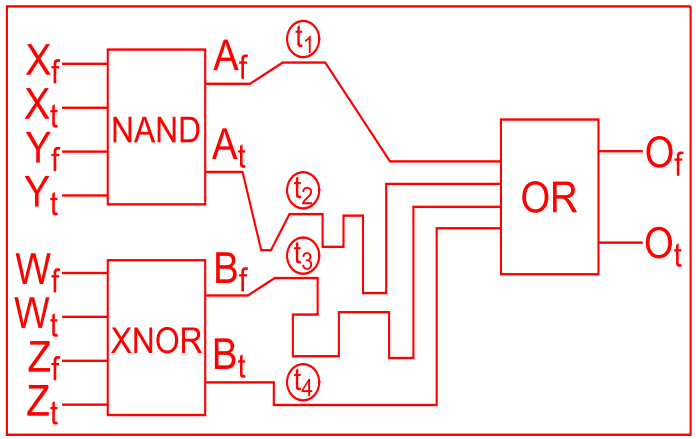
P. Yu, P. Schaumont CODES+ISSS'07

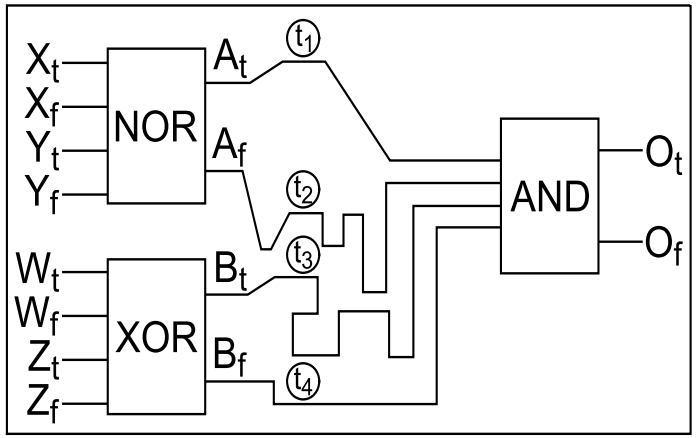


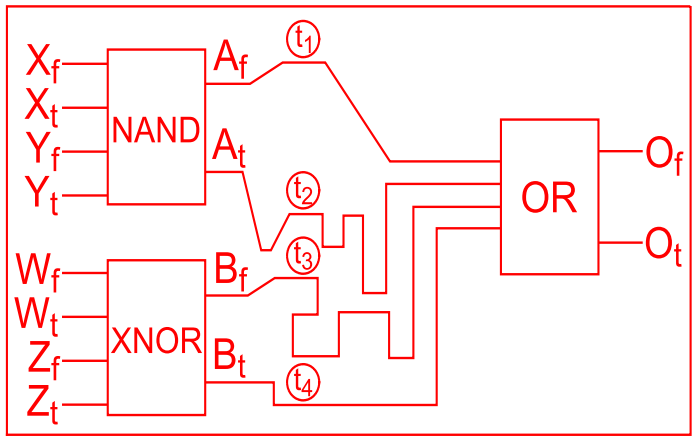



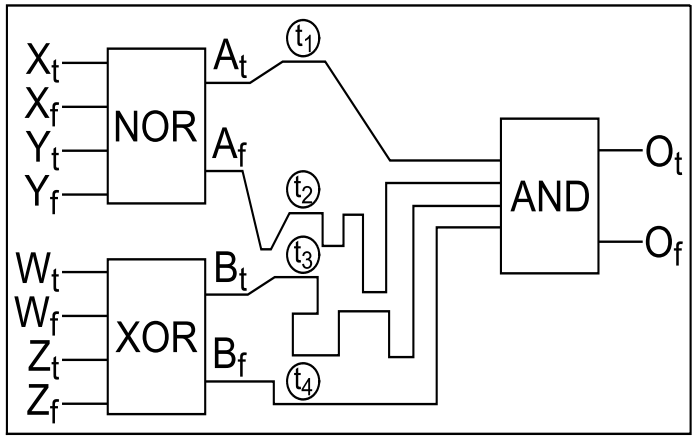
# Data-Dependent Time of Evaluation

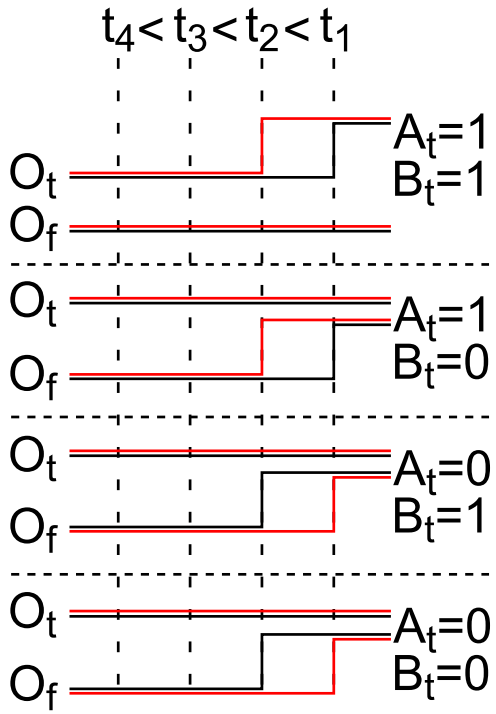


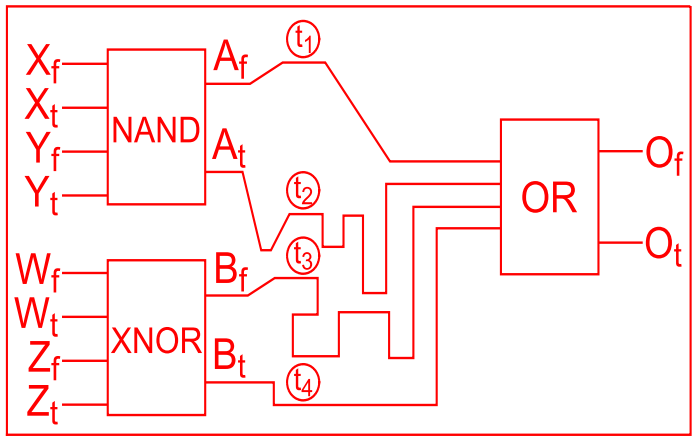
# Data-Dependent Time of Evaluation

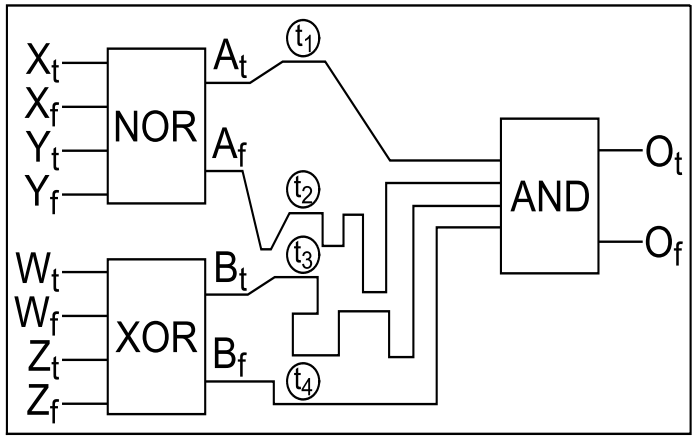


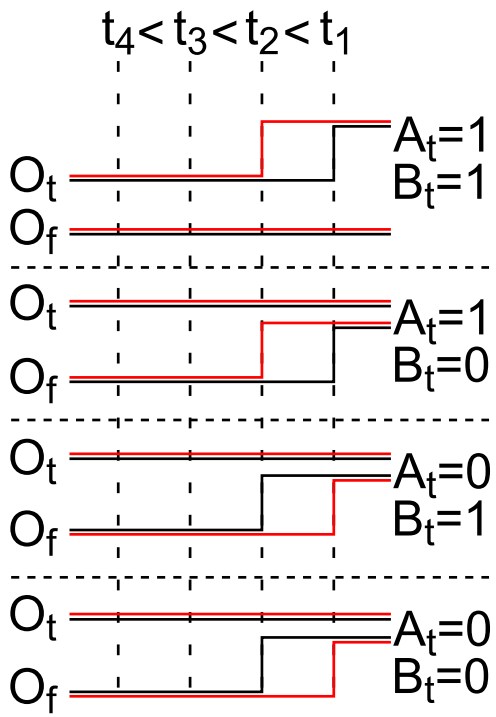



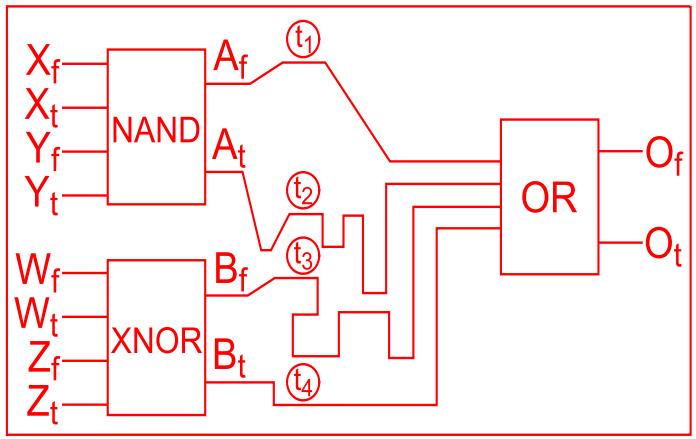
# Data-Dependent Time of Evaluation

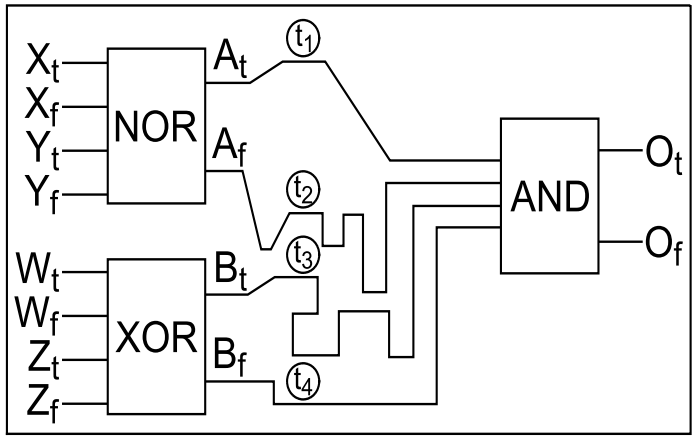


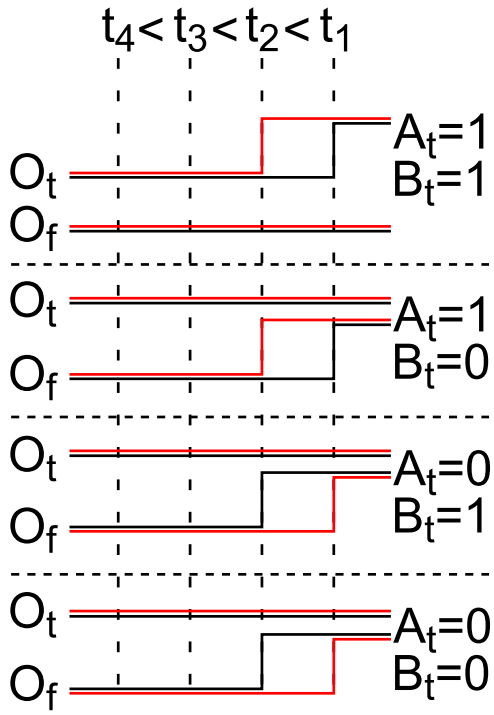



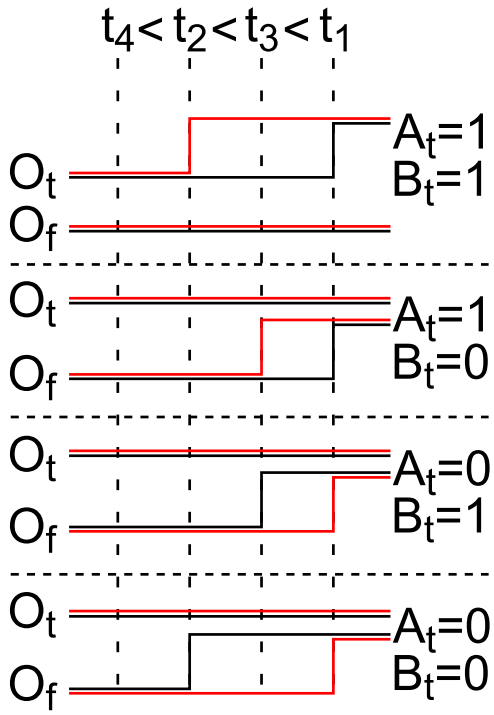



# Data-Dependent Time of Evaluation

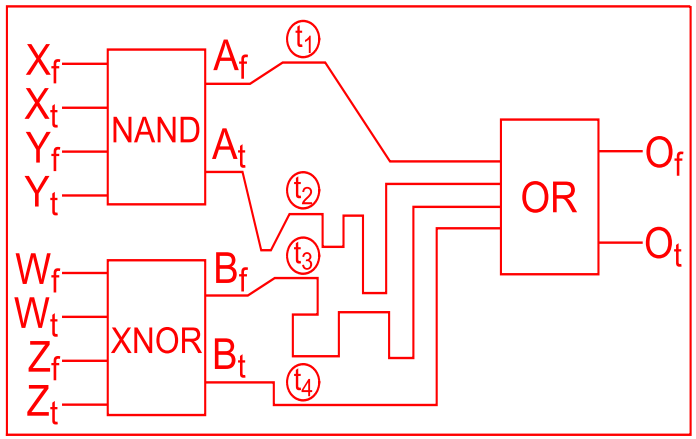


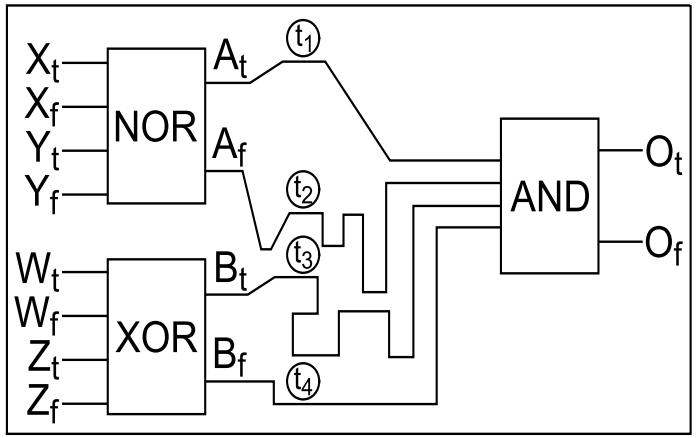



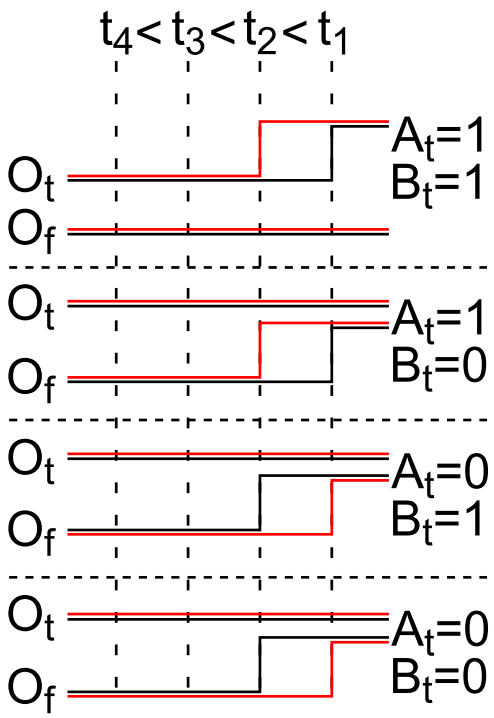



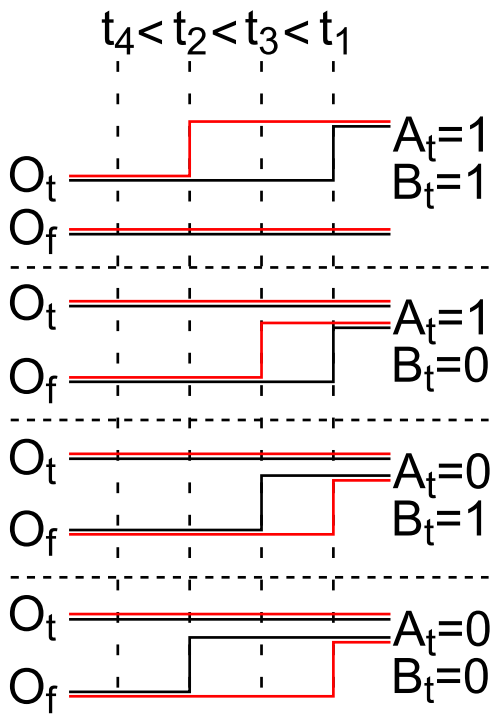



# Data-Dependent Time of Evaluation



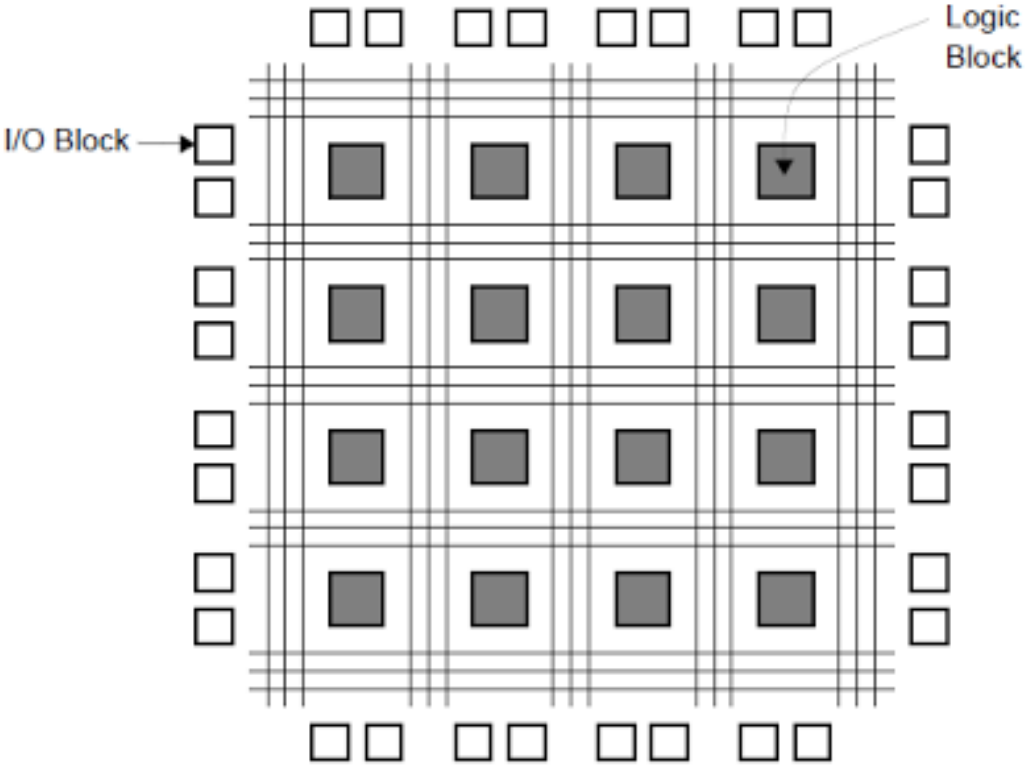



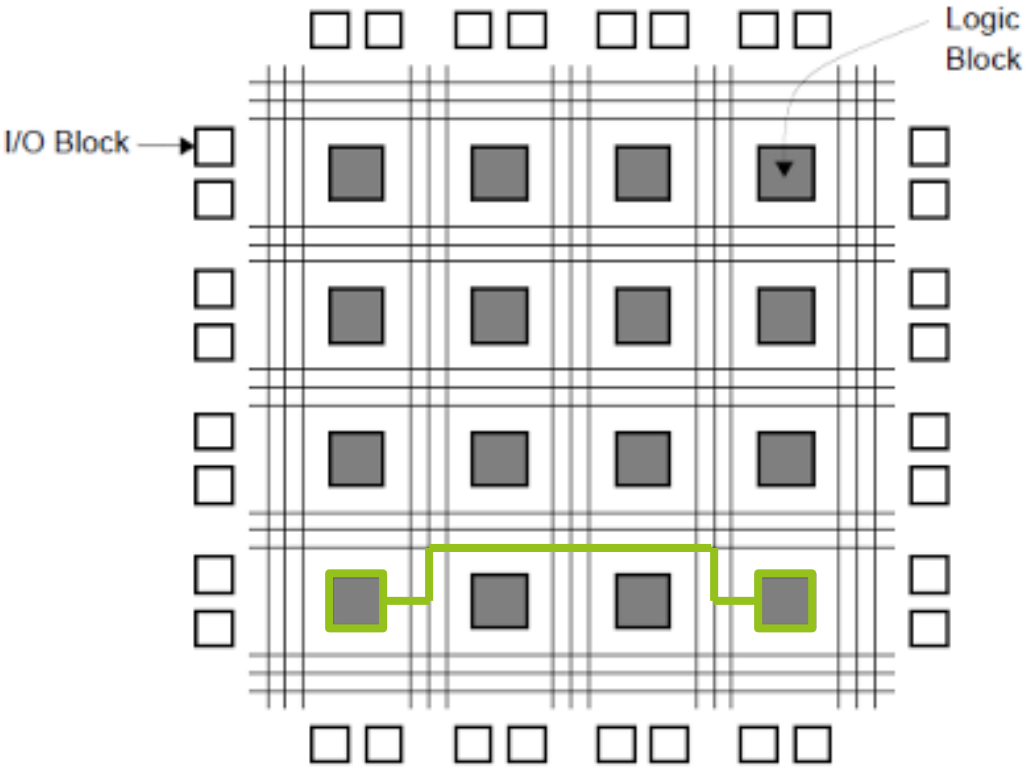
# How to Duplicate?

- FPGA is organized in a grid.
- Xilinx Design Language (XDL)
- Components/PIPs are addressable via X and Y coordinates.
- Reinstantiate components/PIPs with modified coordinates.
- Change component configuration.
- Original circuit: placement constraints
- Compementary circuit: prohibit contraint



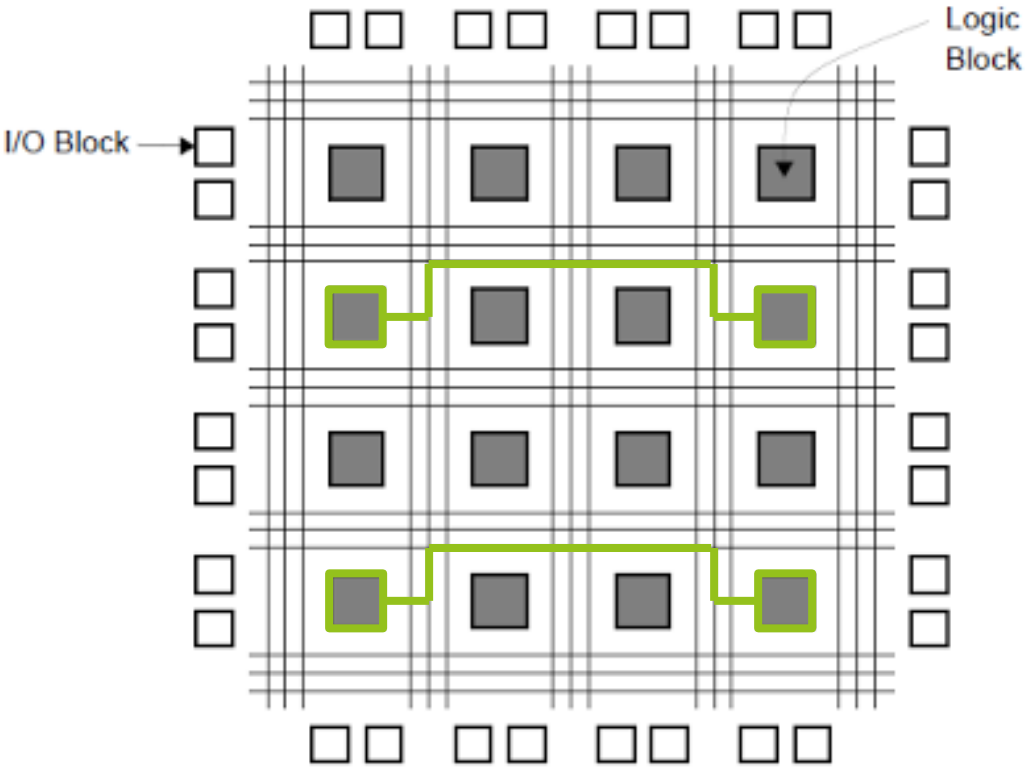
# How to Duplicate?

- FPGA is organized in a grid.
- Xilinx Design Language (XDL)
- Components/PIPs are addressable via X and Y coordinates.
- Reinstantiate components/PIPs with modified coordinates.
- Change component configuration.
- Original circuit: placement constraints
- Compementary circuit: prohibit contraint



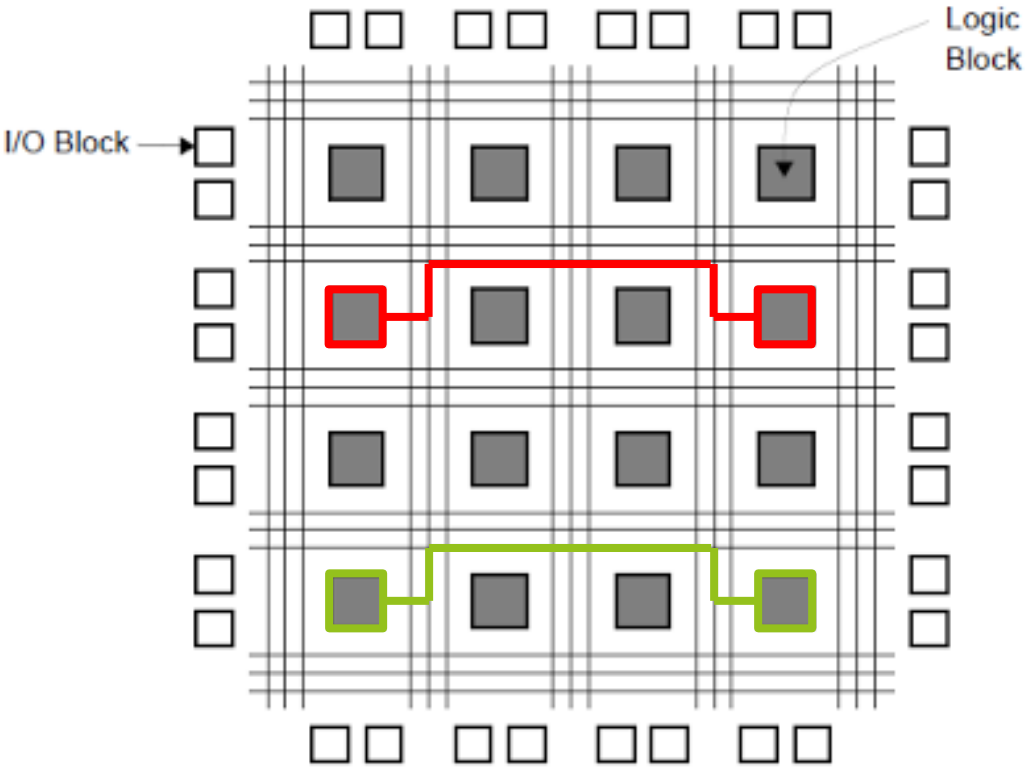
# How to Duplicate?

- FPGA is organized in a grid.
- Xilinx Design Language (XDL)
- Components/PIPs are addressable via X and Y coordinates.
- Reinstantiate components/PIPs with modified coordinates.
- Change component configuration.
- Original circuit: placement constraints
- Compementary circuit: prohibit contraint

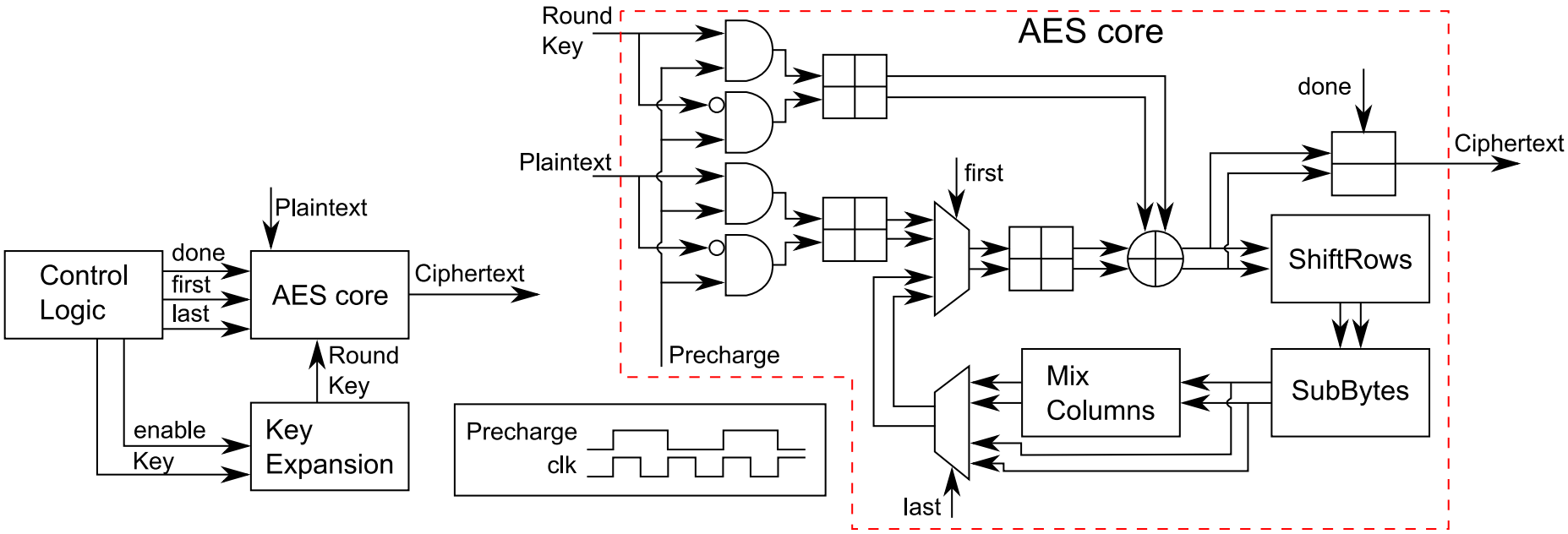


# How to Duplicate?

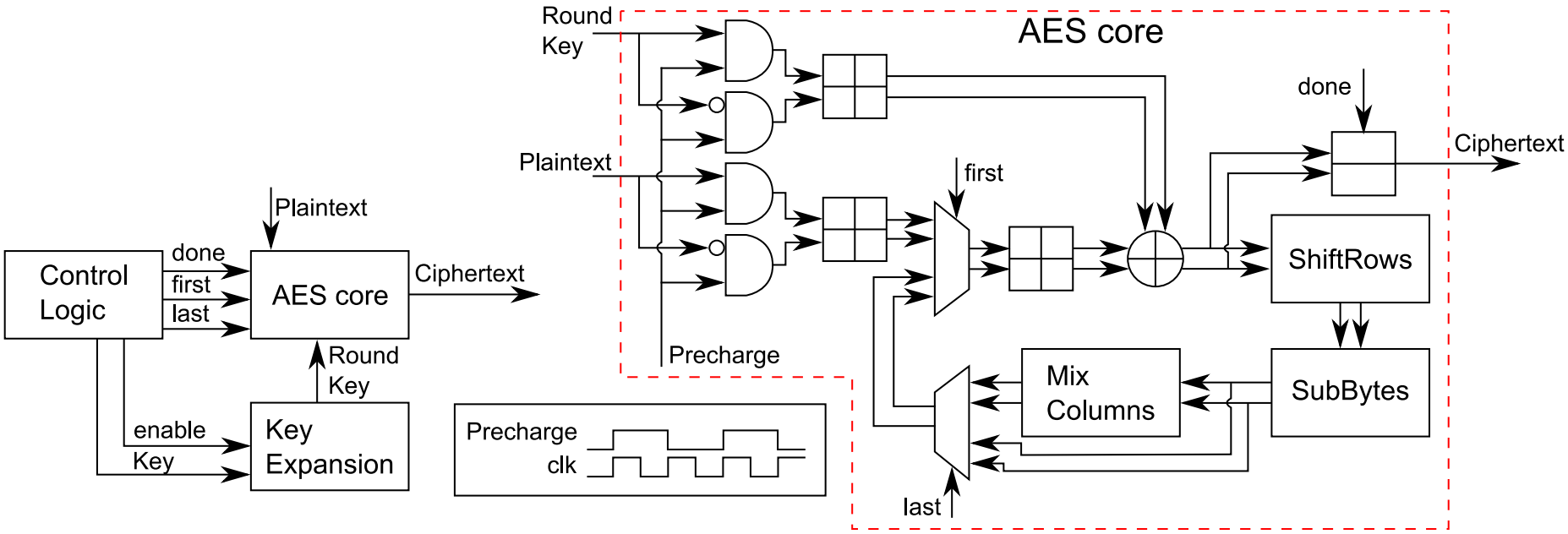
- FPGA is organized in a grid.
- Xilinx Design Language (XDL)
- Components/PIPs are addressable via X and Y coordinates.
- Reinstantiate components/PIPs with modified coordinates.
- Change component configuration.
- Original circuit: placement constraints
- Compementary circuit: prohibit contraint



# Case Study

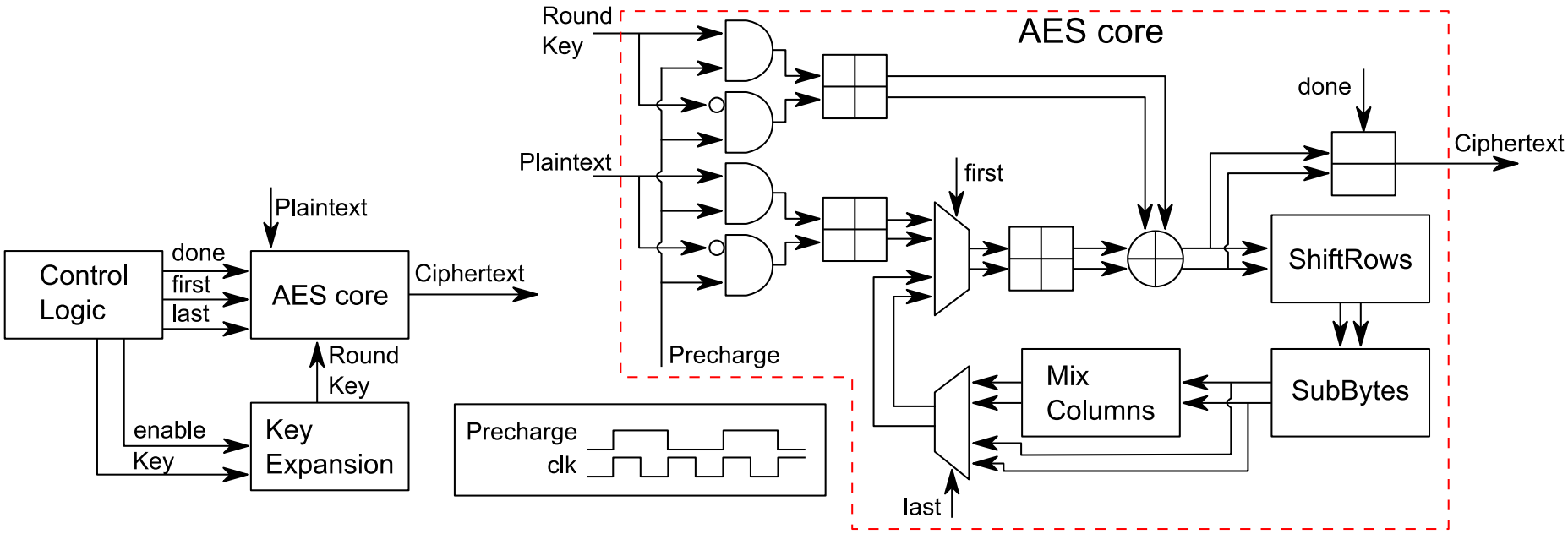

Round Key
Plaintext
AES core
done
Ciphertext
first
ShiftRows
Precharge
Mix Columns
SubBytes
last
Plaintext
Control Logic
done
first
last
AES core
Ciphertext
Round Key
enable Key
Key Expansion
Precharge
clk

# Case Study




- Round-based architecture
  - WDDL => DWDDL
  - DPL-noEE => DDPL-noEE
  - AWDDL => DAWDDL

# Case Study

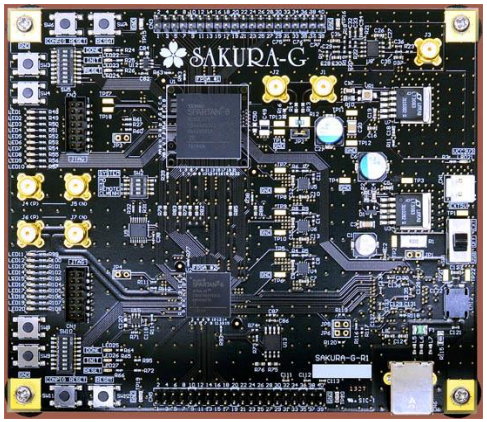



- Round-based architecture
  - WDDL => DWDDL
  - DPL-noEE => DDPL-noEE
  - AWDDL => DAWDDL

| Logic Style | LUT | FF |
|---|---|---|
| WDDL | 8,154 | 1,672 |
| DWDDL | 16,308 | 3,344 |
| DPL-noEE | 3,834 | 1,672 |
| DDPL-noEE | 7,668 | 3,344 |
| AWDDL | 7,146 | 1,672 |
| DAWDDL | 14,292 | 3,344 |

# Setup

- SAKURA-G (Xilinx Spartan 6)
- 1Ω Resistor at Vdd
- 1 GS/s, 20MHz Bandwidth
- 3 MHz Clock
- 1M Traces

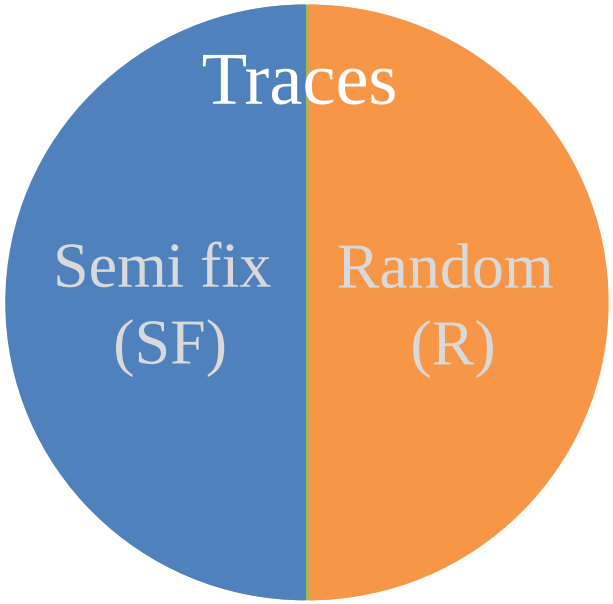



# Evaluation

## Welch's T-Test

**Semi fix vs. random:**

- 1024 plaintexts
- First 64 bits of round 5 are NULL
- Randomly picked




$N_{SF}$ = Size of SF
$X_{SF}$ = Mean of SF
$S_{SF}$ = Std. deviation of SF

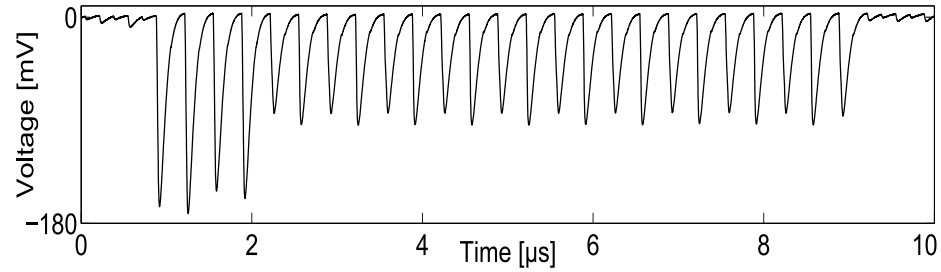
$N_R$ = Size of R
$X_R$ = Mean of R
$S_R$ = Std. deviation of R

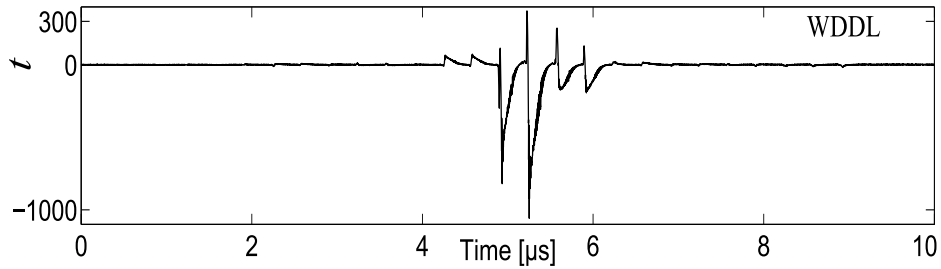
$$T = \frac{X_{SF} - X_R}{\sqrt{\frac{S_{SF}^2}{N_{SF}} + \frac{S_R^2}{N_R}}}$$

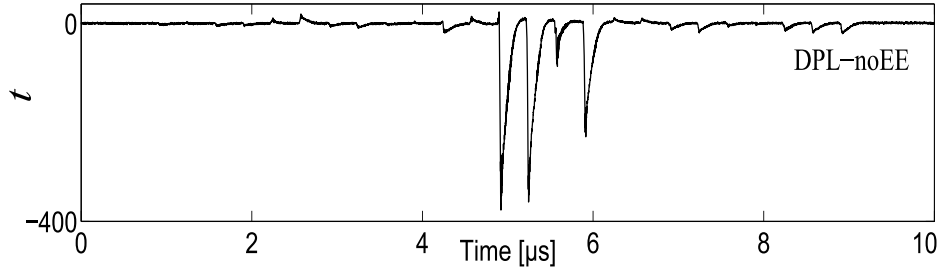
**Fail/Pass Criteria:** If there is any point in time for which the t-statistic trace exceeds a threshold +/- 4.5 the device under test fails.

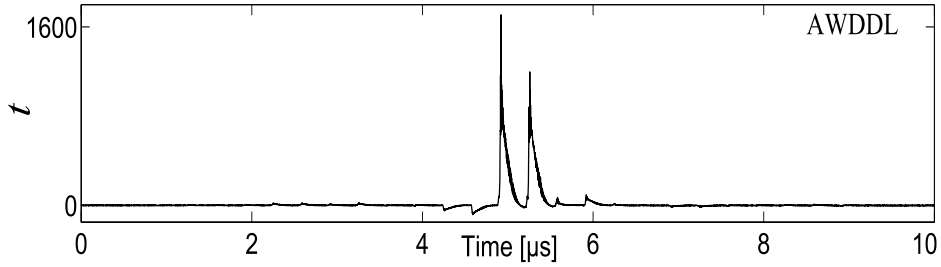
# Evaluation

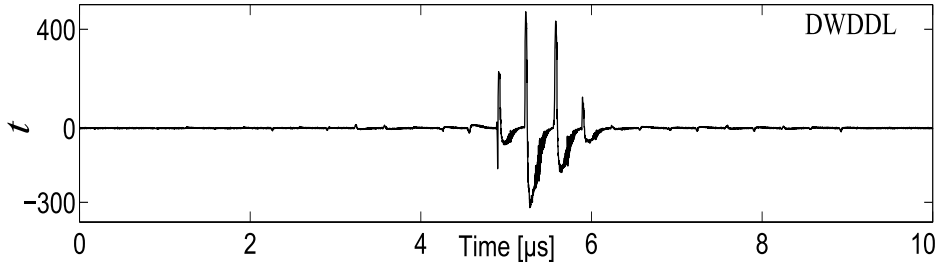
## Results

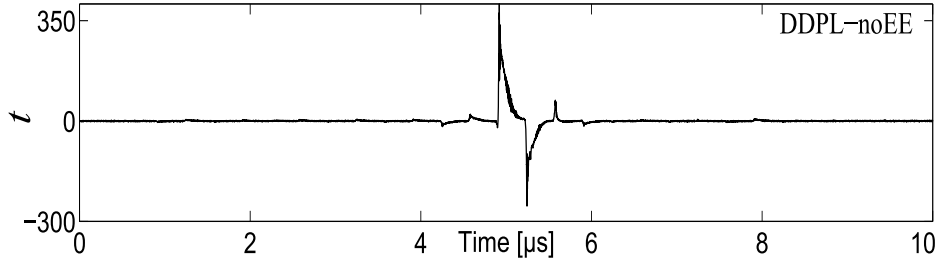


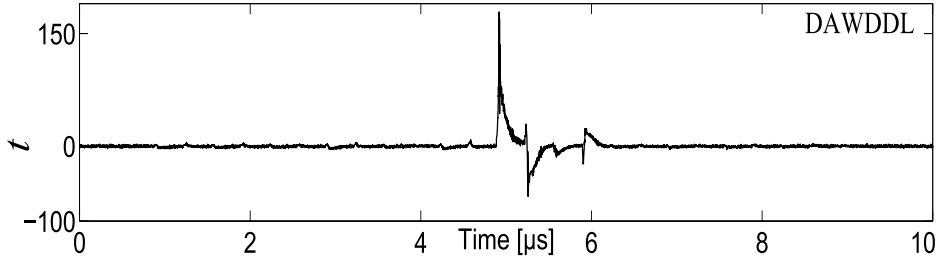



# Conclusions

- Dual-rail routuing does not work well on FPGA (CHES 2014)
- Douplication show a data dependent time of evaluation.
  - still detectable leakage
- Not a clear future for dual-rail pre-charge logic on FPGAs

- follow-up work: (seems to be a suitable solution)
  - **GliFreD: Glitch-Free Duplication - Towards Power-Equalized Circuits on FPGAs** (ePrint 2015/124)

# Thank you for Listening!

*Any Questions?*