Evaluating the Duplication of Dual-Rail Logics on FPGAs

Alexander Wild, Amir Moradi, Tim Güneysu

April 13, 2015
Motivation
Dual-rail precharge logic
Motivation
Dual-rail precharge logic

Dual-rail logic

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

<table>
<thead>
<tr>
<th>Gate</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gate</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Motivation
Dual-rail precharge logic

Dual-rail logic

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

<table>
<thead>
<tr>
<th>Gate</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
</table>

Precharge logic

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Gate</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ \]
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

\[ t_4 < t_3 < t_2 < t_1 \]

\[ \begin{array}{c}
A_t = 1 \\
B_t = 1 \\
\hline
A_t = 1 \\
B_t = 0 \\
\hline
A_t = 0 \\
B_t = 1 \\
\hline
A_t = 0 \\
B_t = 0 \\
\end{array} \]
Data-Dependent Time of Evaluation
Data-Dependent Time of Evaluation

![Diagram showing data-dependent time of evaluation with logic gates and timing diagrams.]

- Timing diagrams indicating different scenarios for the evaluation of logic functions with data-dependent times.
- The diagrams show the output responses for various input combinations, illustrating the correctness of the logic operations.

---

Evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs | Wild | COSADE - Berlin | APRIL 13, 2015
Data-Dependent Time of Evaluation

Diagram showing the logic gates and timing diagrams for evaluating the Duplication of Dual-Rail Precharge Logics on FPGAs.
How to Duplicate?

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

![Diagram of AES encryption process]

**Control Logic**
- done
- first
- last
- enable
- Key

**AES core**
- Round Key
- Plaintext
- Precharge
- first
- last

**Key Expansion**
- Precharge
- clk

**AES Core**
- ShiftRows
- Mix Columns
- SubBytes
- done
- Ciphertext
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

<table>
<thead>
<tr>
<th>Logic Style</th>
<th>LUT</th>
<th>FF</th>
</tr>
</thead>
<tbody>
<tr>
<td>WDDL</td>
<td>8,154</td>
<td>1,672</td>
</tr>
<tr>
<td>DWDDL</td>
<td>16,308</td>
<td>3,344</td>
</tr>
<tr>
<td>DPL-noEE</td>
<td>3,834</td>
<td>1,672</td>
</tr>
<tr>
<td>DDPL-noEE</td>
<td>7,668</td>
<td>3,344</td>
</tr>
<tr>
<td>AWDDL</td>
<td>7,146</td>
<td>1,672</td>
</tr>
<tr>
<td>DAWDDL</td>
<td>14,292</td>
<td>3,344</td>
</tr>
</tbody>
</table>
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

\[ T = \frac{X_{SF} - X_R}{\sqrt{\frac{S^2_{SF}}{N_{SF}} + \frac{S^2_R}{N_R}}} \]

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)
- Doupllication 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?