Timing with Virtual Signal Synchronization for Circuit Performance and Netlist Security

Grace Li Zhang, Bing Li, Ulf Schlichtmann
Chair of Electronic Design Automation
Technical University of Munich (TUM)
Overview

VirtualSync Timing Model

Timing Camouflage against Counterfeiting

Summary
The Traditional Timing Paradigm

**Sequential components** such as flip-flops synchronize signal propagations.

**Combinational gates** perform logic computations.

- Clock-to-q delay $t_{cq}$: 3
- Setup time $t_{su}$: 1
- Hold time $t_h$: 1

Disadvantages:

- Flip-flops have clock-to-q delays and impose setup time.
- Delay imbalances between flip-flop stages degrade performance.

$$T_{min} = t_{cq} + d_{max} + t_{su} = 3 + 17 + 1 = 21$$
Timing Optimization Methods

Gate Sizing

- $T_{\text{min}} = 3 + 12 + 1 = 16$

Retiming

- $T_{\text{min}} = 3 + 7 + 1 = 11$
- The limit in the traditional timing paradigm

VirtualSync

- $T_{\text{min}} = (3 + 13 + 1) / 2 = 8.5$
- 22.7% reduction compared with retiming & sizing
VirtualSync Concept

fast path must be delayed

loop must be blocked

VirtualSync:
Step 1: Remove all flip-flops except those at the boundary of the module
Step 2: Block fast signals for timing synchronization, including
  • signals arriving at boundary flip-flops too earlier through fast paths
  • signals traveling across combinational loops

Circuit under optimization
VirtualSync Concept

- Delay units (logic gates, flip-flops and latches) are used to slow down signals on fast paths and loops.
- Relative Reference Points provide relative timing information.
Delay Units in VirtualSync

(a) Linear delaying effect of a combinational delay unit

(b) Constant delaying effect of a flip-flop

(c) Piecewise delaying effect of a latch

Input gap: the difference between arrival times of two signals at a delay unit
Output gap: the difference between their arrival times after they pass through the unit
Overall Flow of VirtualSync

1. Sequential circuits
2. Remove all flip-flops
3. Mark reference points
4. Create selection variables for delay units at each circuit node
5. Set lower bound of inserted delay
6. Maximize performance and minimize area using ILP
7. Decrease lower bound of inserted delay
8. All required delays are padded?
   - Yes: Optimized circuit
   - No: Repeat steps 2-7
Results of VirtualSync

Speed increase (%) and Area change (%)

Speed increase and area results compared with ideally balanced design.
Overview

VirtualSync Timing Model

Timing Camouflage against Counterfeiting

Summary
Counterfeiting Digital Circuits

**Counterfeiting threat:** Illegal production of chips by a third party with a netlist recognized through reverse engineering

- Authentic chips delayered and imaged
- Logic gates, flip-flops and their connections identified
- Recognized netlist processed with a standard IC design flow

Counterfeit chips

Optical and x-ray images of 64Gb Flash devices

Counterfeiting with Conventional Timing

- Conventional timing model
  - All paths defined with respect to one clock period
  - Setup and hold time constraints satisfied between pairs of flip-flops
- A netlist is sufficient to reproduce a circuit using a standard EDA flow.
Anti-Counterfeiting with Wave Pipelining

A camouflaged netlist is used to hide the synchronization of one logic wave. This requires an additional effort to extract timing information. The recognized circuit loses synchronization when using a single logic wave, whereas two logic waves are needed for the camouflaged netlist to function properly.
Counter Test Attack with False Paths

Delay measurement of constructed wave-pipelining false paths is challenging.

controlling signal always blocks one of the AND and OR gates.
Implementation of Timing Camouflage

Input: netlist, delay information, clock period T, delay recognition accuracy, required number of wave-pipelining paths

check paths incoming to and leaving from the next flip-flop

wave-pipelining false paths can be formed?

No

more paths required

Yes

construct wave-pipelining paths

Results of Constructing Wave-Pipelining Paths

To replicate chips, attackers need to recognize the constructed wave-pipelining false paths from the original paths.
Summary

- By viewing flip-flops and latches as delay units, circuit performance can be pushed even beyond the limit of the traditional timing paradigm.

- VirtualSync demonstrates a good potential for high-performance designs.

- The new timing camouflage technique invalidates the assumption that a netlist itself carries all design information.

- Timing Camouflage potentially opens up a new dimension of circuit security.
Thank you for your attention!
Relative Timing References in VirtualSync

- The location of the removed flip-flops such as F2 and F3 are called anchor points.
- The anchor points allow to relate timing information to boundary flip-flops. Every time when a signal passes an anchor point, its arrival time is converted by subtracting T.
- If F3 is removed, the arrival time $s_z$ becomes $-3 + 2 = -1$, violating the hold time constraint.

The timing constraints at the boundary flip-flops force the usage of the internal sequential delay units!
Iterative Relaxation in VirtualSync

- Emulation of sequential delay units with different padding delays for long and short paths
- Model approximation with clock/data-to-q delays
  - Yes
  - Different padding delays are needed?
  - No
  - Model legalization using accurate delay models
  - Different padding delays are needed?
    - Yes
    - Buffer replacement using sequential units and delay discretization
    - Optimized circuit
## Runtime of VirtualSync

<table>
<thead>
<tr>
<th>Circuit</th>
<th>$T_r$(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>s5378</td>
<td>121.6</td>
</tr>
<tr>
<td>s9234</td>
<td>7251.1</td>
</tr>
<tr>
<td>s13207</td>
<td>3121.6</td>
</tr>
<tr>
<td>s15850</td>
<td>289.97</td>
</tr>
<tr>
<td>s38584</td>
<td>1142.3</td>
</tr>
<tr>
<td>systemcdes</td>
<td>7310.5</td>
</tr>
<tr>
<td>mem_ctrl</td>
<td>3750.1</td>
</tr>
<tr>
<td>usb_funct</td>
<td>1211.7</td>
</tr>
<tr>
<td>ac97_ctrl</td>
<td>2936.8</td>
</tr>
<tr>
<td>pci_bridge</td>
<td>7418.5</td>
</tr>
</tbody>
</table>
## Results of VirtualSync

<table>
<thead>
<tr>
<th>Circuit</th>
<th>Critical part</th>
<th>Optimized circuit</th>
<th>Comparison</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#flip-flop</td>
<td>#gates</td>
<td>#flip-flop</td>
</tr>
<tr>
<td>s5378</td>
<td>35</td>
<td>1877</td>
<td>11</td>
</tr>
<tr>
<td>s9234</td>
<td>91</td>
<td>3981</td>
<td>58</td>
</tr>
<tr>
<td>s13207</td>
<td>191</td>
<td>3483</td>
<td>95</td>
</tr>
<tr>
<td>s15850</td>
<td>71</td>
<td>3847</td>
<td>72</td>
</tr>
<tr>
<td>s38584</td>
<td>126</td>
<td>9498</td>
<td>62</td>
</tr>
<tr>
<td>systemcdes</td>
<td>92</td>
<td>3232</td>
<td>90</td>
</tr>
<tr>
<td>mem_ctrl</td>
<td>136</td>
<td>7500</td>
<td>101</td>
</tr>
<tr>
<td>usb_funct</td>
<td>138</td>
<td>5378</td>
<td>123</td>
</tr>
<tr>
<td>ac97_ctrl</td>
<td>237</td>
<td>4873</td>
<td>42</td>
</tr>
<tr>
<td>pci_bridge</td>
<td>239</td>
<td>9510</td>
<td>188</td>
</tr>
</tbody>
</table>

The comparison was made with extreme retiming and sizing, with which the timing performance has reached the limit in the traditional timing paradigm.
**Attack techniques and countermeasures**

**The first attack technique:**
Capture gate and interconnect delays in reverse engineering

Paths with delay $T + t_{h} \leq d_{p} \leq 2T - t_{su}$ are identified

Real path delay $d$ is estimated by attackers in

$$[ (1 - \tau)d, (1 + \tau)d ]$$

High cost

Insufficient delay accuracy $0 \leq \tau \leq 1$

Attacker narrow down the number of potential wave-pipelining paths

Gray region for a path with delay $d$

The number of remaining suspicious paths is still large due to critical wall
Attack techniques and countermeasures

The second attack technique:
Test all suspicious paths

A test vector is used to check whether a path delay is greater than T or not

Construct wave-pipelining false paths
Attack techniques and countermeasures

The third attack technique:
Simulate all possible wave-pipelining cases

Each false path is assumed to be a real false path once and a wave-pipelining path once.

# of paths: n
# of simulations: 2^n

The fourth attack technique:
Size all false paths as wave-pipelining

Violations of timing constraints in single-period clocking need to be avoided.

Difficult to find a solution

The fifth attack technique:
Calculate all gate delays from tested paths

Measured path delays can be used to calculate gate delays with linear algebra.

At-speed testing of path delays inaccurate
Attack techniques and countermeasures

- False path: A combinational path which cannot be activated in functional mode or test due to controlling signals from other paths.

- Wave-pipelining false path (WP false path): A combinational path with wave-pipelining that is a false path when viewed with the conventional single-period clocking.
Implementation of Timing Camouflage

Objective:
(1) Minimize the number of buffers
(2) Maximize the connection with the original circuits

Try to connect the input pins of gates to the original gates

Only keep necessary gates

Delays of wave-pipelining constraints

(a)

(b)