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)

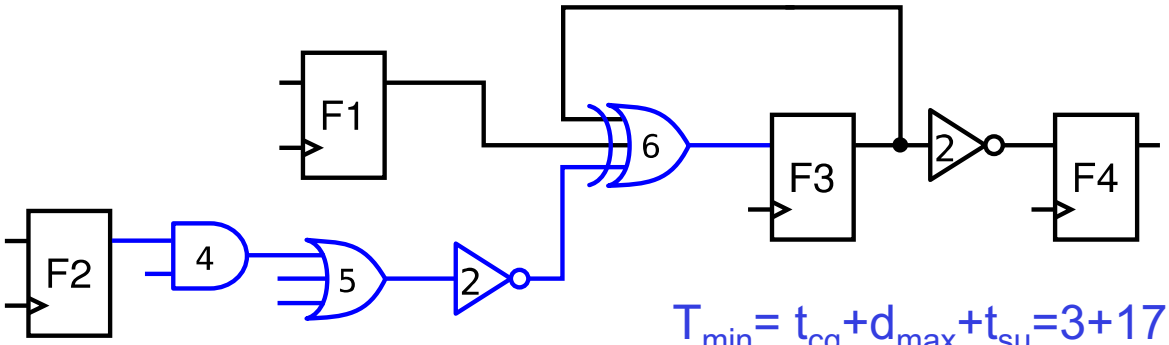
Overview

VirtualSync Timing Model

Timing Camouflage against Counterfeiting

Summary

The Traditional Timing Paradigm



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

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

- **Sequential components** such as flip-flops synchronize signal propagations.
- **Combinational gates** perform logic computations.

Reduce design effort

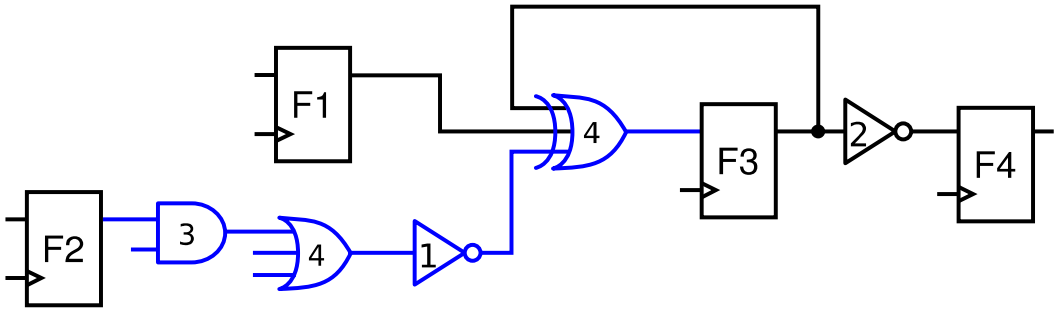
Disadvantages

Flip-flops have clock-to-q delays and impose setup time.

Delay imbalances between flip-flop stages degrade performance

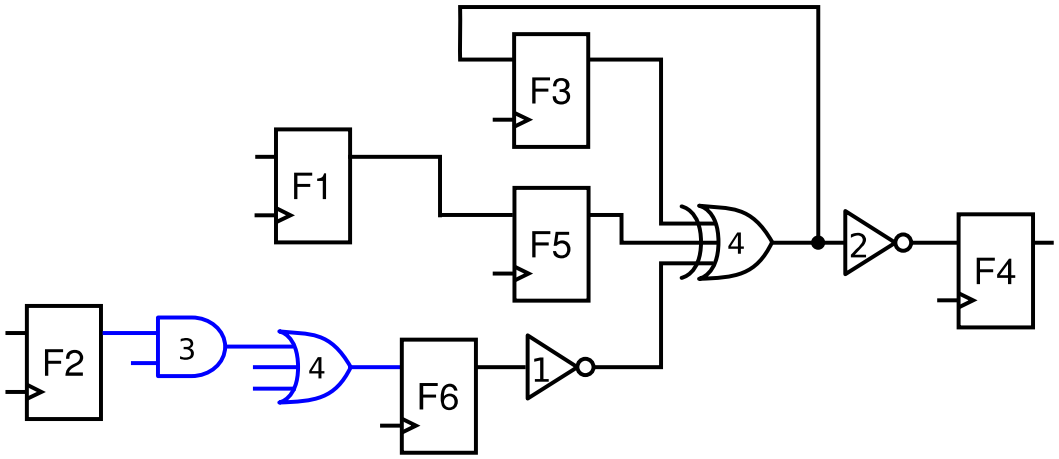
Timing Optimization Methods

Gate Sizing



T_{min}= 3+12+1=16

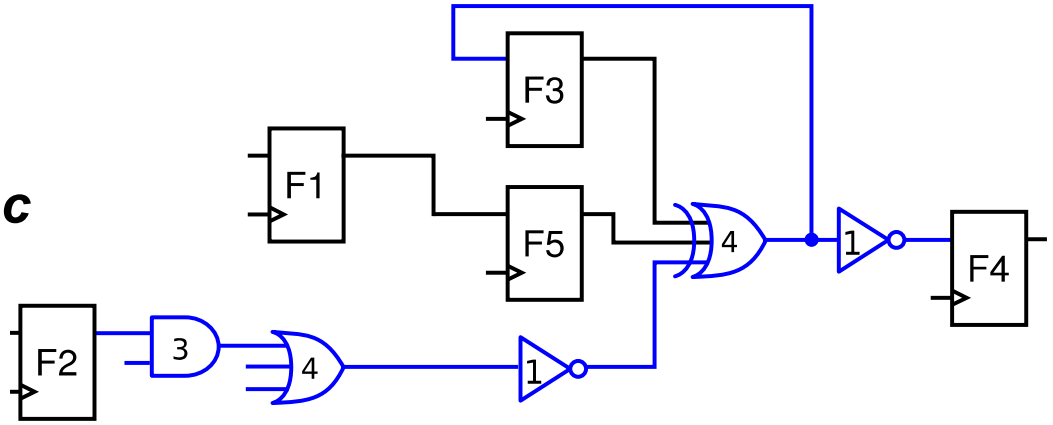
Retiming



T_{min}= 3+7+1=11

The limit in the traditional timing paradigm

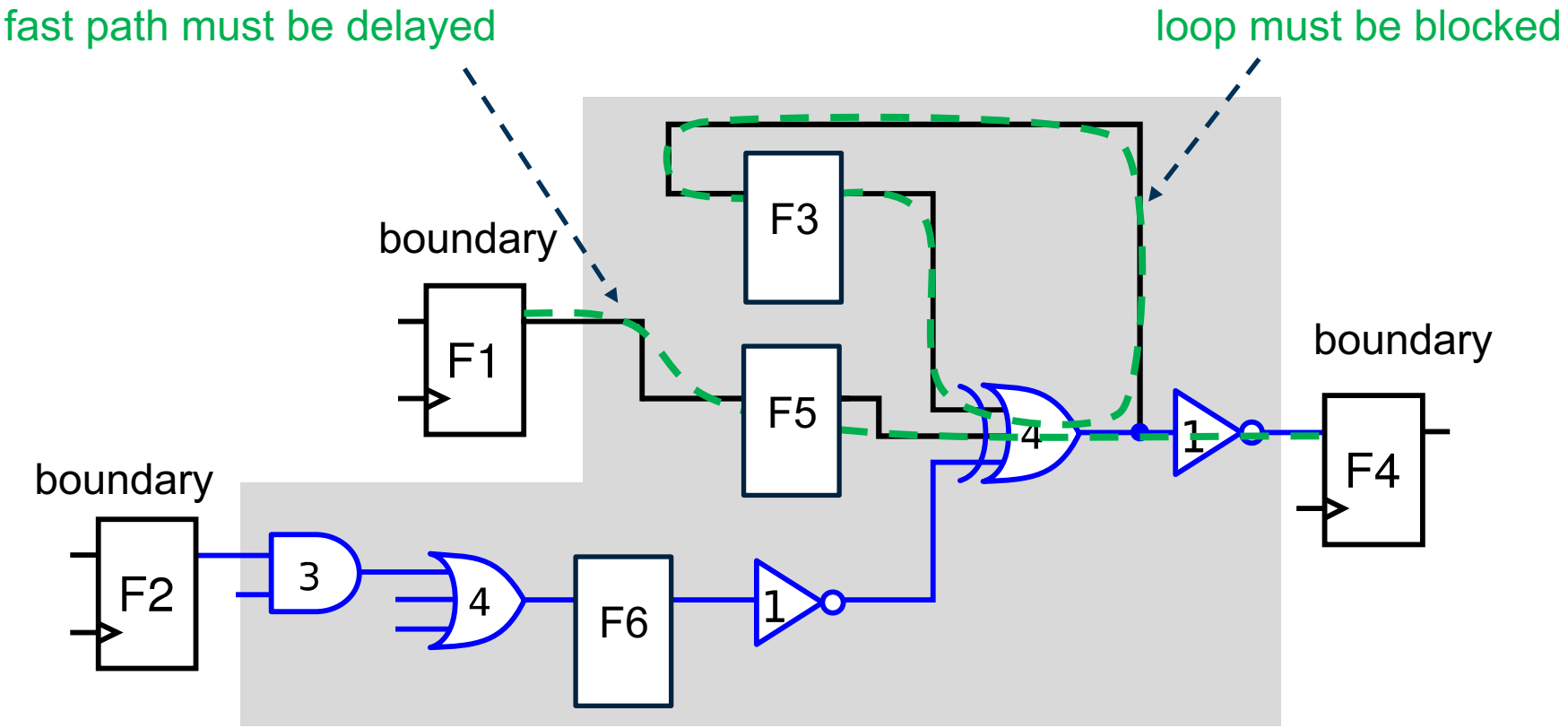
VirtualSync



T_{min}=(3+13+1)/2=8.5

22.7% reduction compared with retiming&sizing

VirtualSync Concept

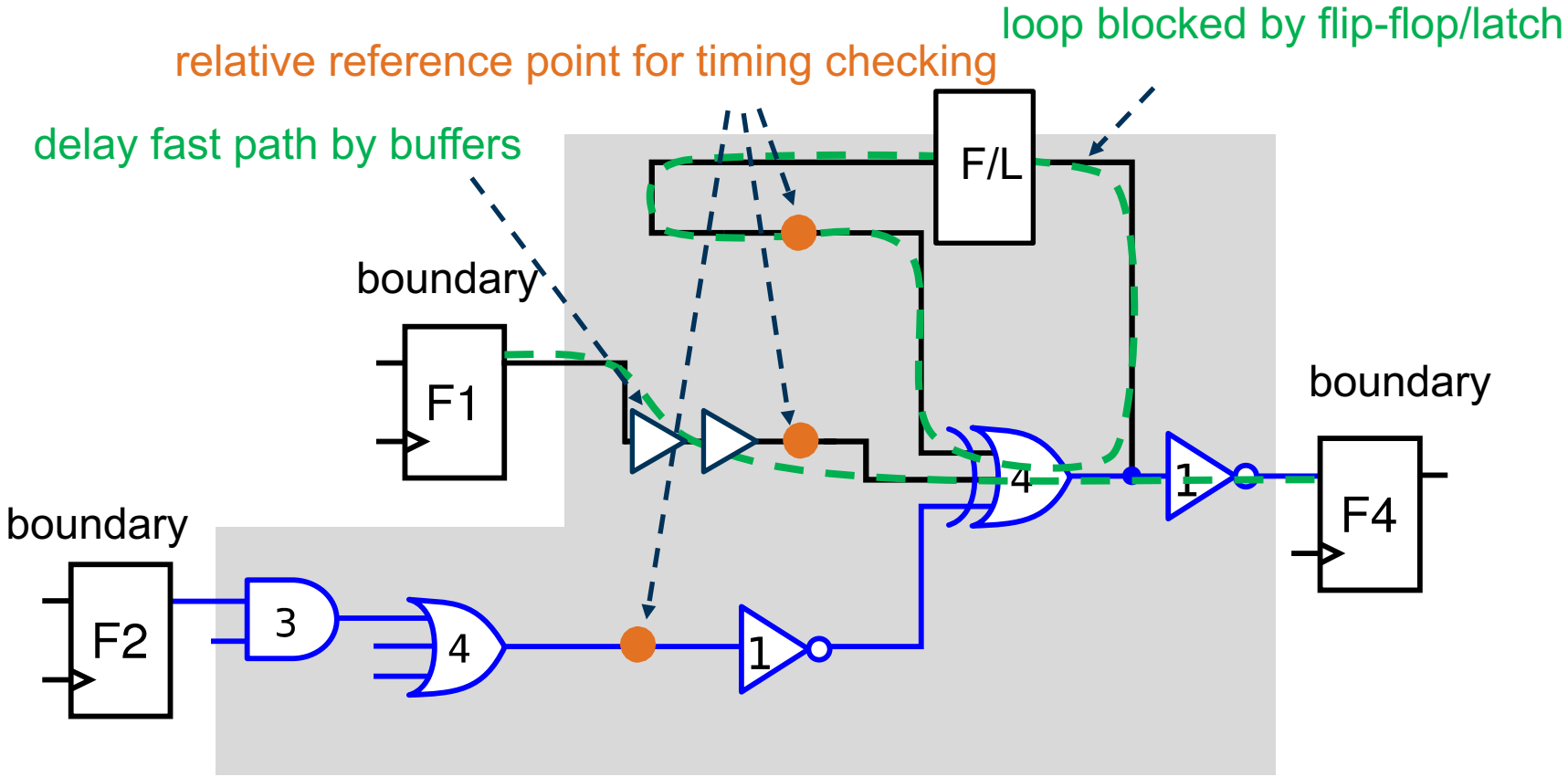


Circuit under optimization

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

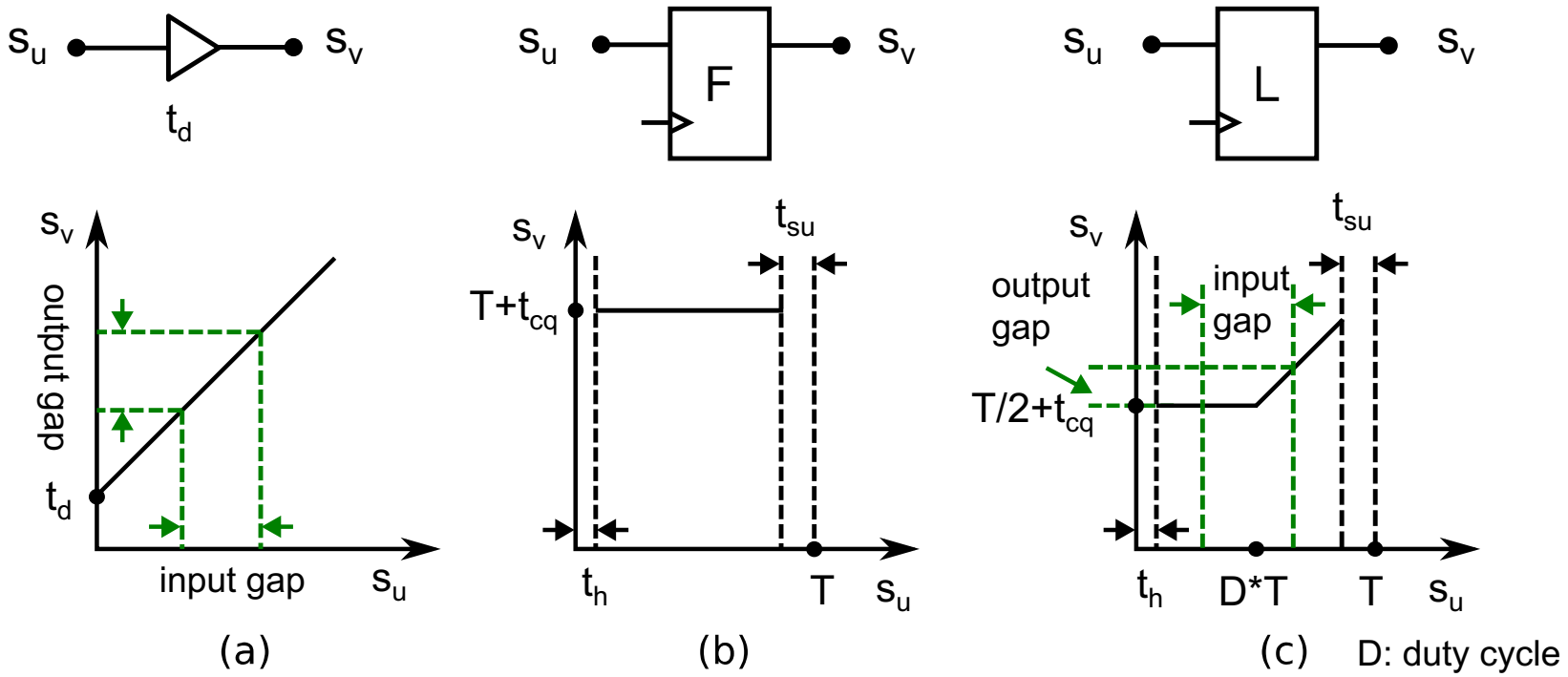
VirtualSync Concept



Circuit under optimization

- **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



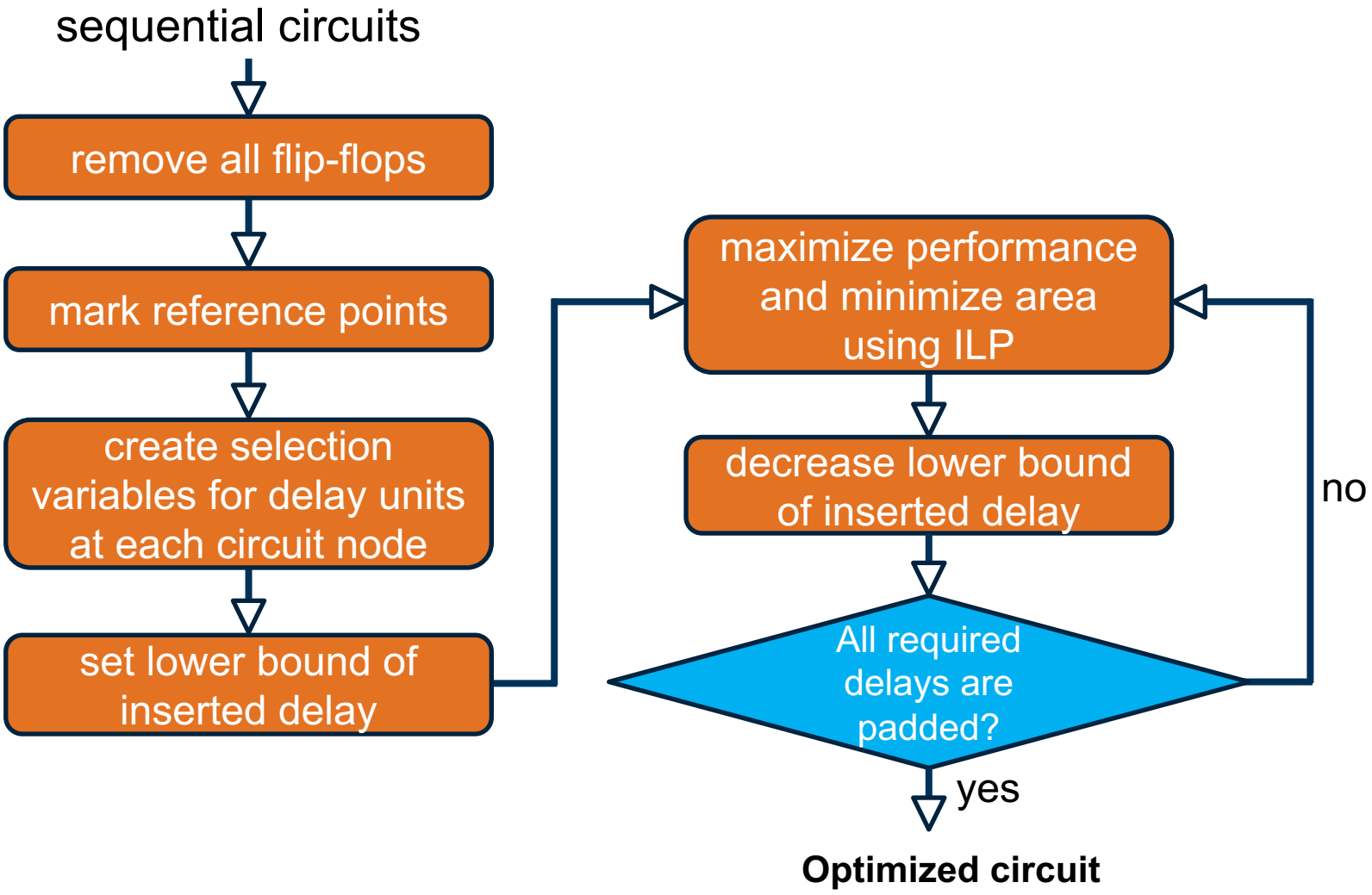
Linear delaying effect of a **combinational delay unit**

Constant delaying effect of a **flip-flop**

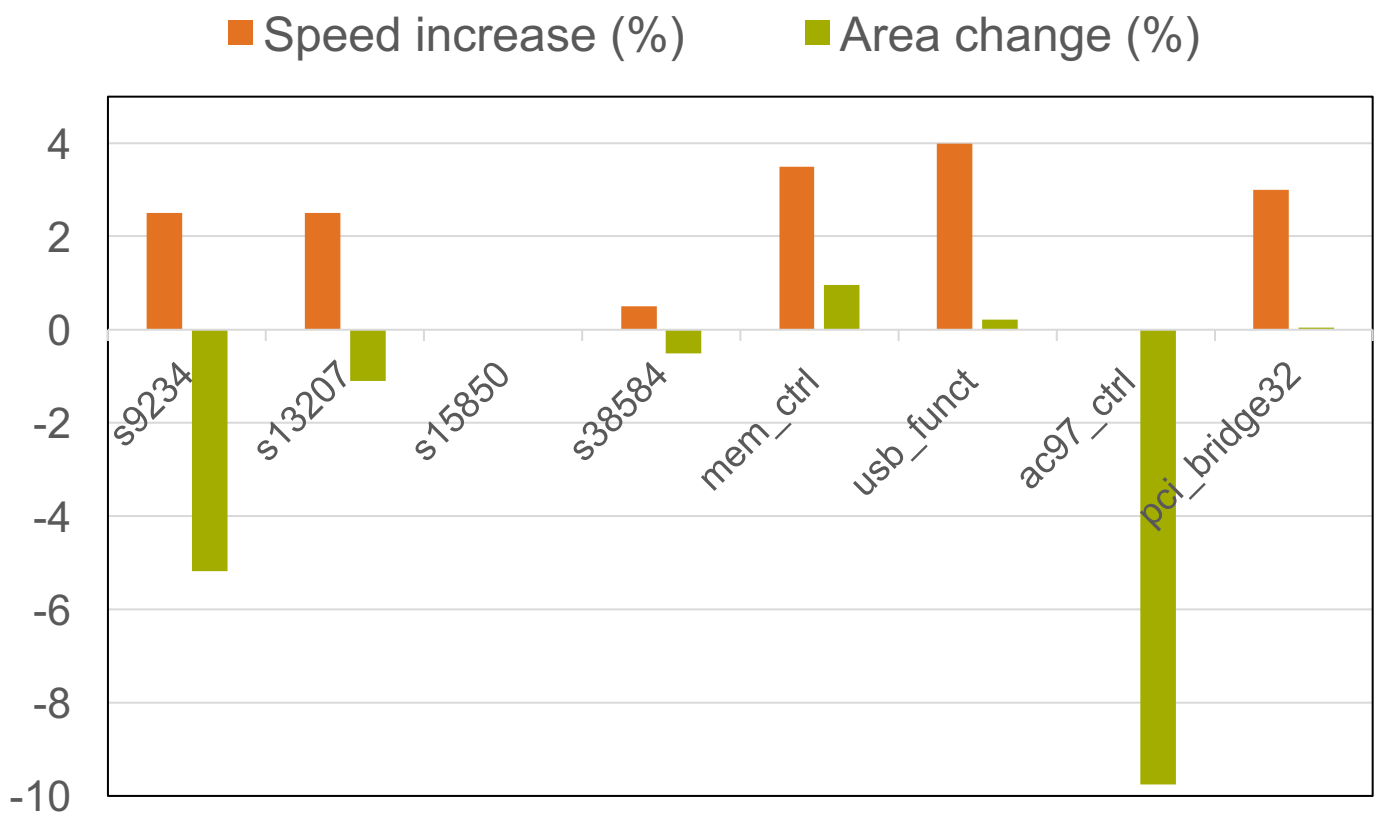
Piecewise delaying effect of a **latch**

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



Results of VirtualSync



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

↓

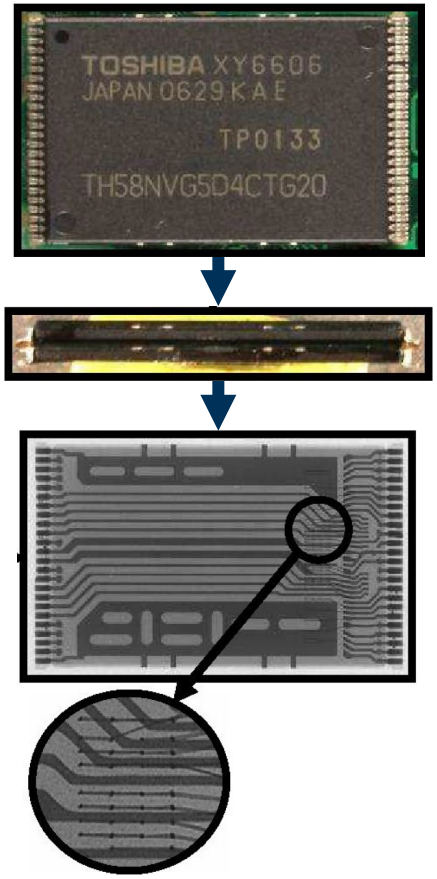
Logic gates, flip-flops and their connections identified

↓

Recognized netlist processed with a standard IC design flow

↓

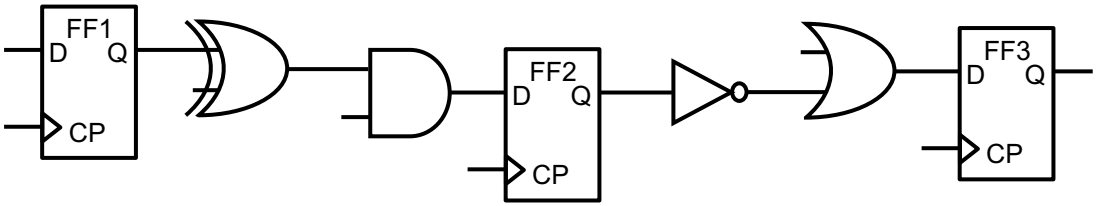
Counterfeit chips



Optical and x-ray images of 64Gb Flash devices

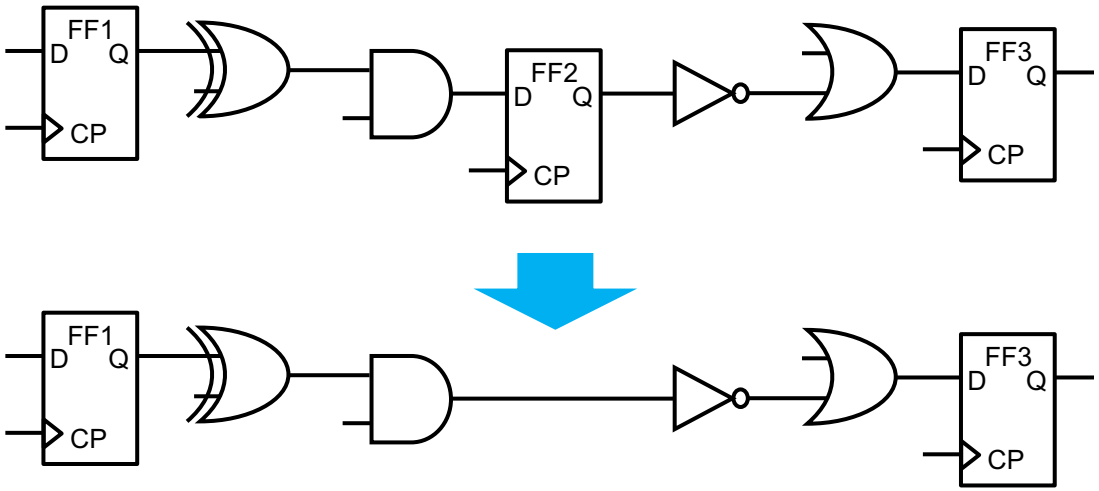
[R. Torrance et al., "Reverse Engineering in the Semiconductor Industry," CICC, Sep, 2007]

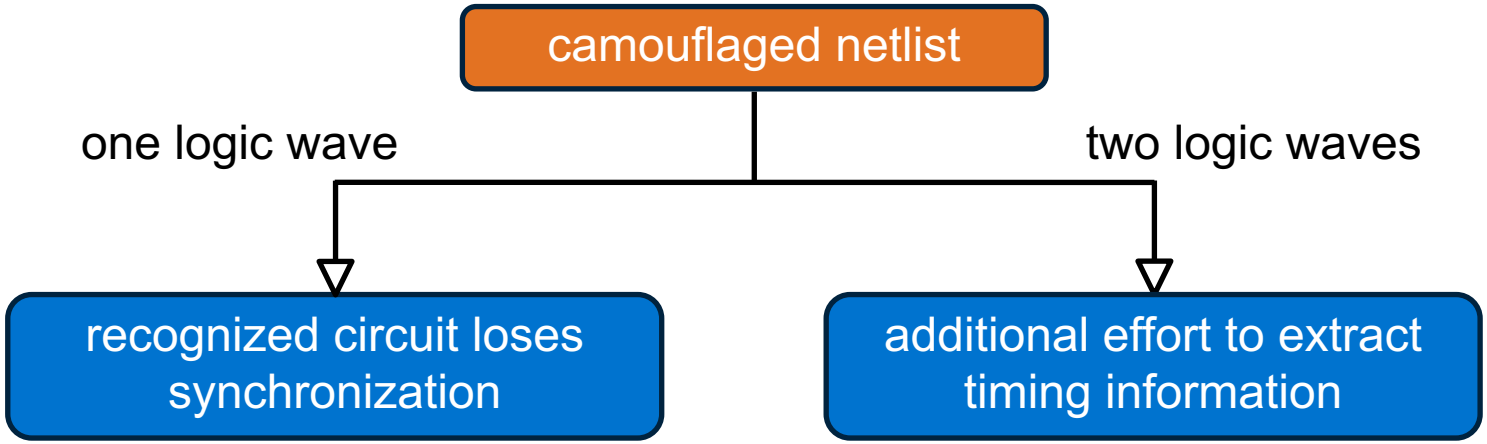
Counterfeiting with Conventional Timing



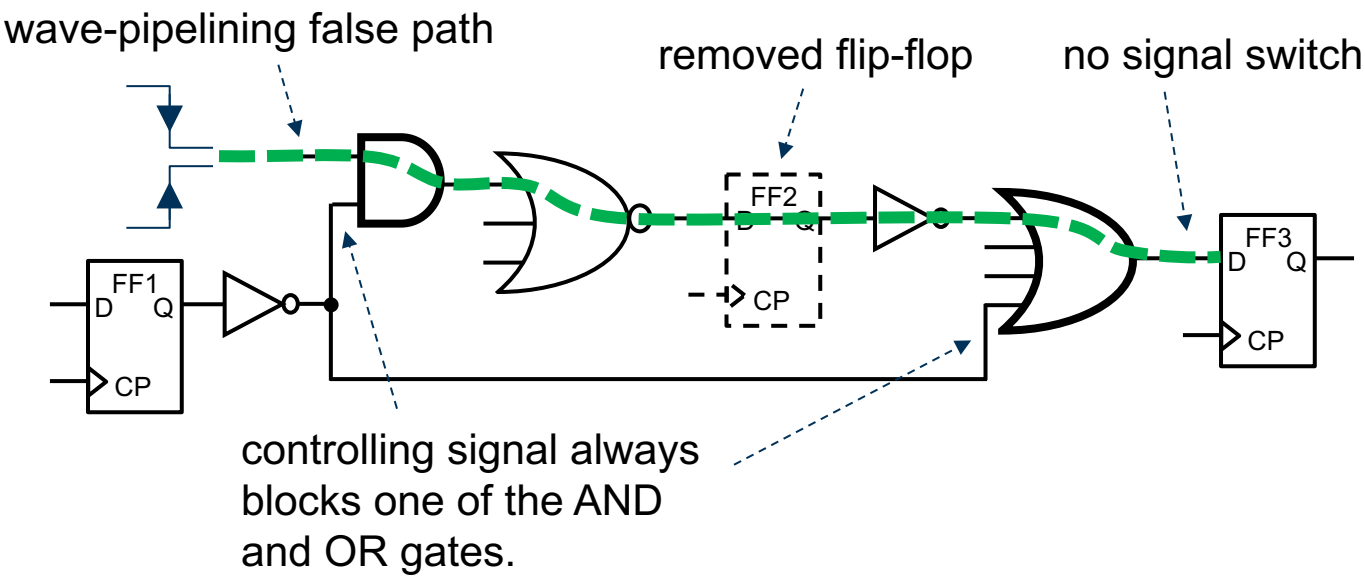
- Conventional timing model
  - All paths defined with respect to one clock period
  - Setup and hold time constraints satisfied between pairs of flip-flops
- A netlist is sufficient to reproduce a circuit using a standard EDA flow.

Anti-Counterfeiting with Wave Pipelining



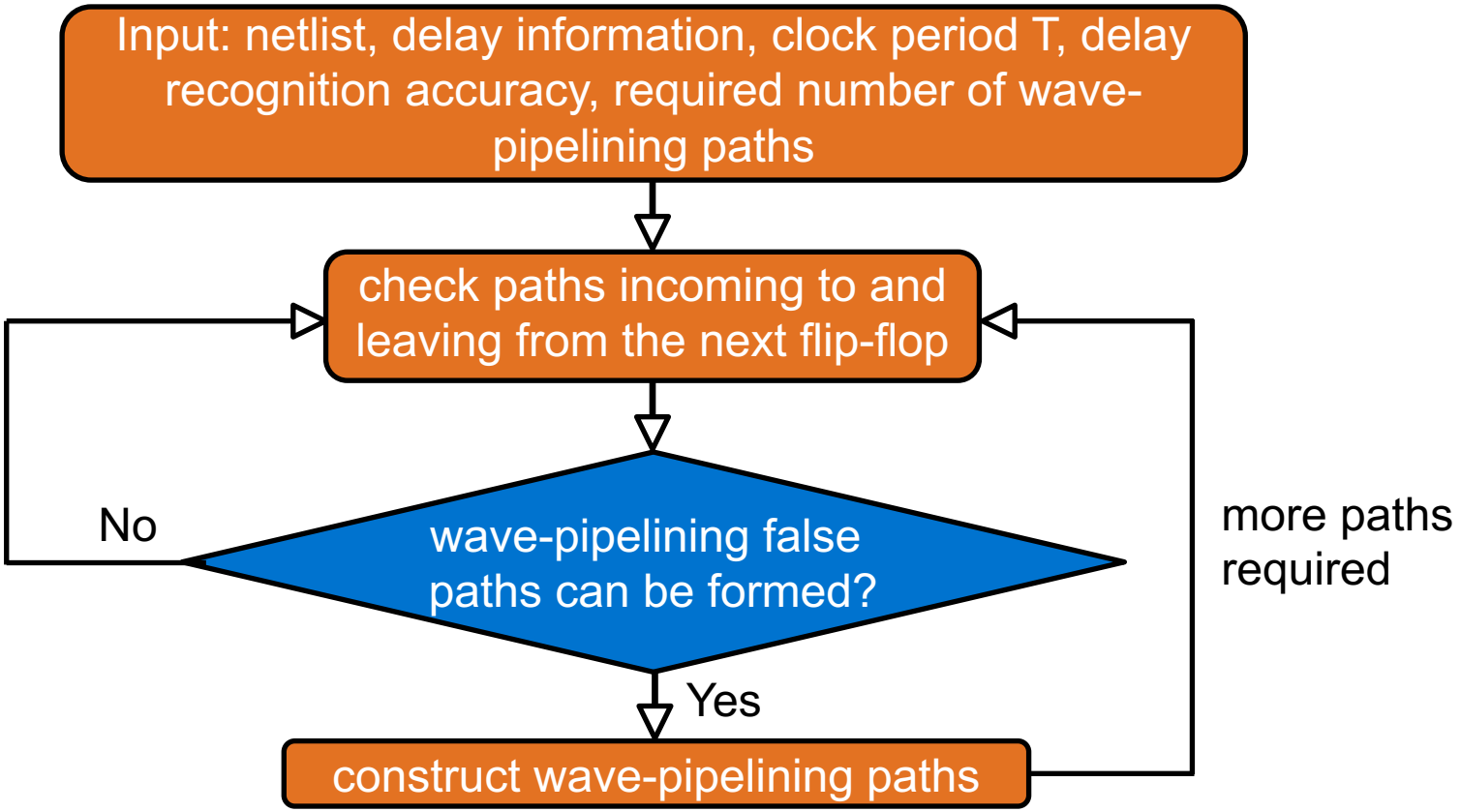


Counter Test Attack with False Paths



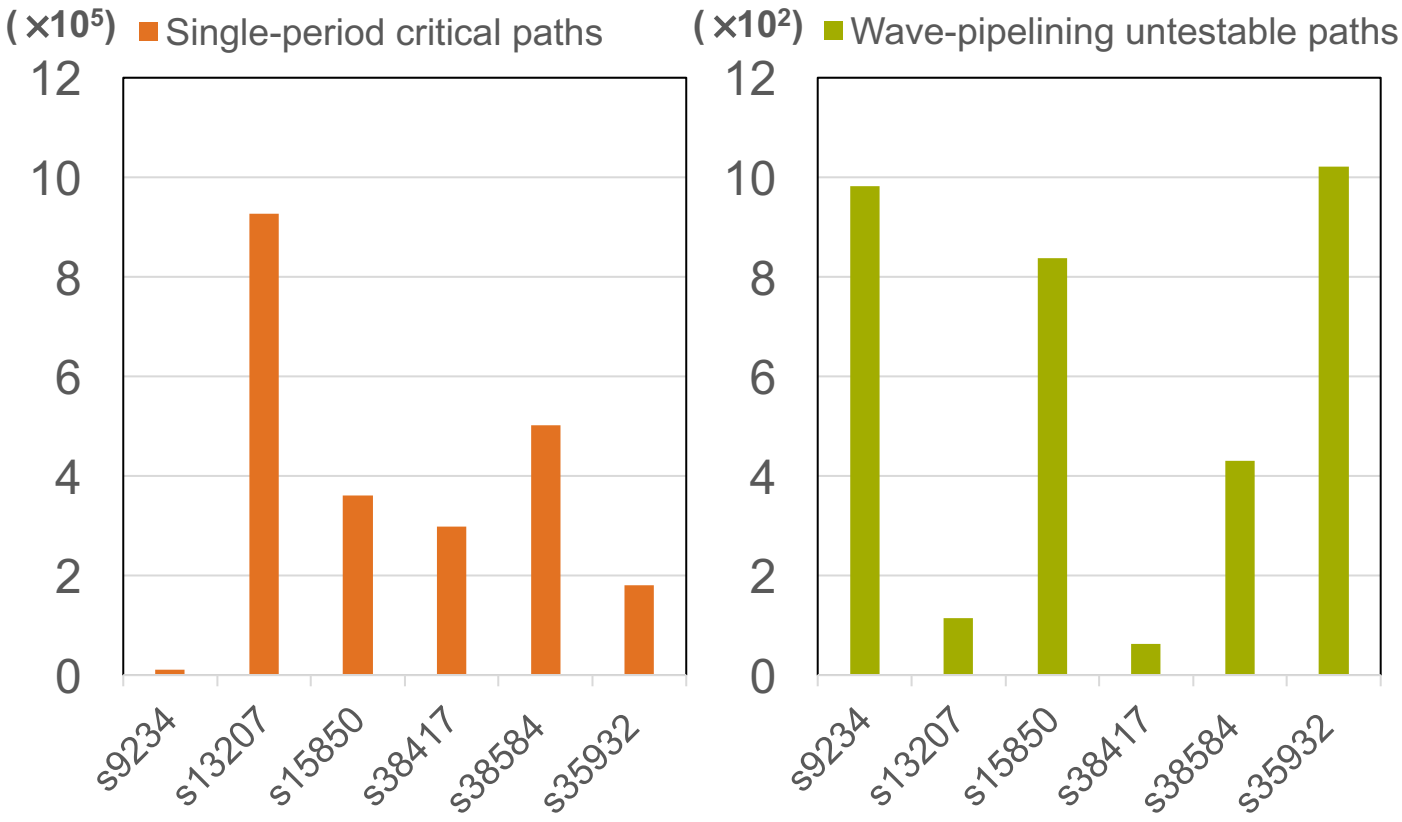
Delay measurement of constructed wave-pipelining false paths is challenging.

Implementation of Timing Camouflage



Grace Li Zhang, Bing Li, Bei Yu, David Z. Pan, Ulf Schlichtmann, "TimingCamouflage: Improving Circuit Security against Counterfeiting by Unconventional Timing", Design, Automation and Test in Europe (DATE), March 2018

Results of Constructing Wave-Pipelining Paths



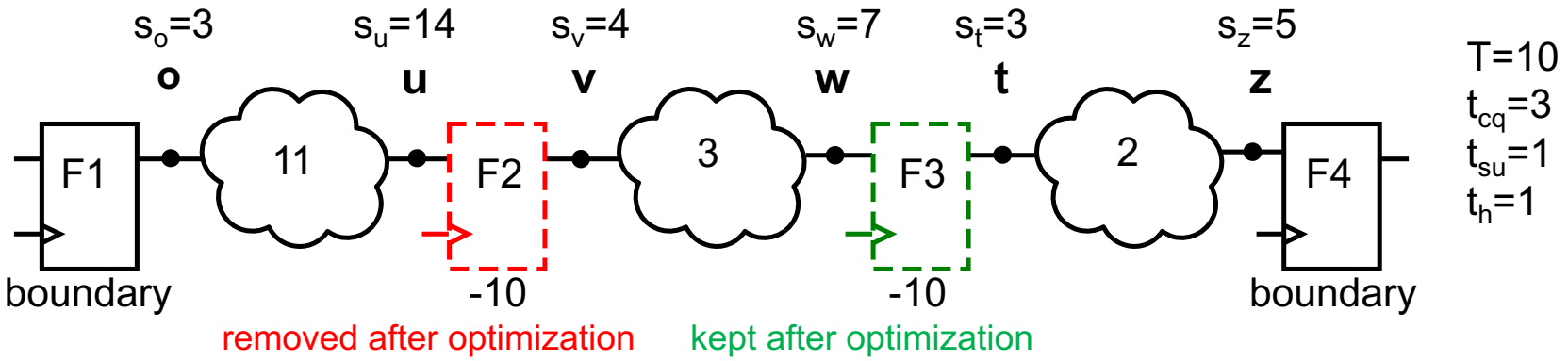
To replicate chips, attackers need to recognize the constructed wave-pipelining false paths from the original paths.

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

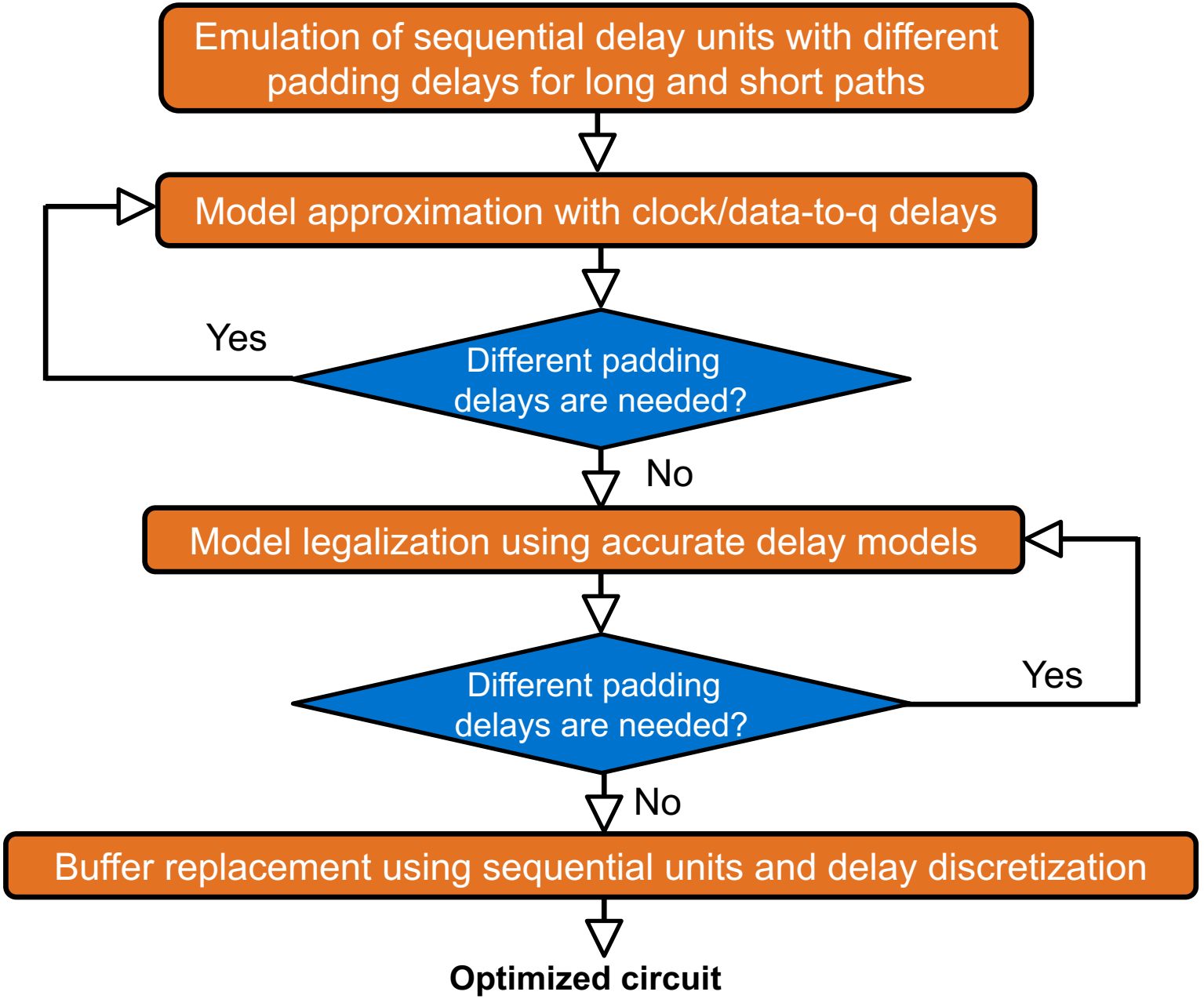


$$s_z + t_{su} \le T \qquad\qquad s'_z \ge t_h$$

- 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



Runtime of VirtualSync

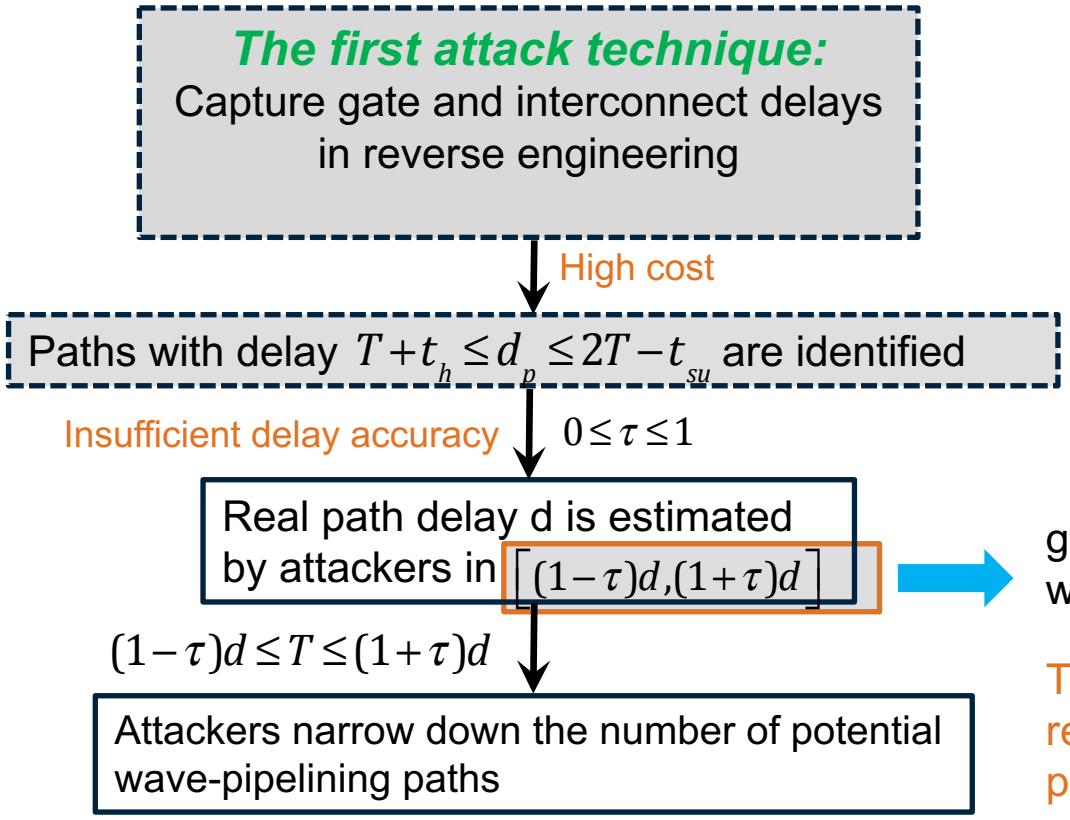
Circuit	T_r(s)
s5378	121.6
s9234	7251.1
s13207	3121.6
s15850	289.97
s38584	1142.3
systemcdes	7310.5
mem_ctrl	3750.1
usb_funct	1211.7
ac97_ctrl	2936.8
pci_bridge	7418.5

Results of VirtualSync

Circuit	Critical part		Optimized circuit			Comparison	
	#flip-flop	#gates	#flip-flop	#latch	#buffer	clock period reduction	area increase
s5378	35	1877	11	14	94	**11.5%**	2.84%
s9234	91	3981	58	45	91	2.5%	-5.17%
s13207	191	3483	95	73	52	2.5%	-1.09%
s15850	71	3847	72	18	26	0%	6.01%
s38584	126	9498	62	75	46	0.5%	-0.5%
systemcdes	92	3232	90	81	227	3.5%	2.43%
mem_ctrl	136	7500	101	39	140	3.5%	0.97%
usb_funct	138	5378	123	37	60	4%	0.21%
ac97_ctrl	237	4873	42	172	218	0%	-9.76%
pci_bridge	239	9510	188	68	338	3%	0.05%

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

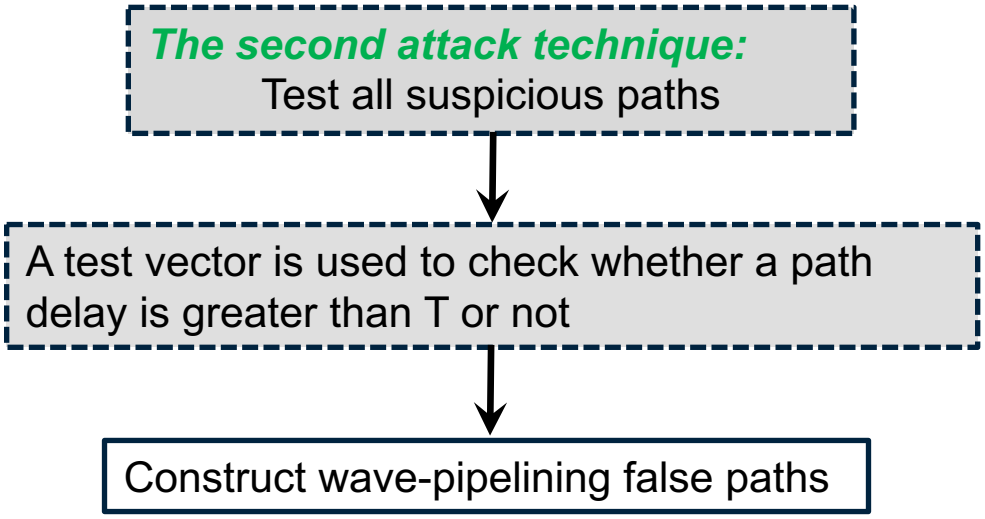
Attack techniques and countermeasures



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



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

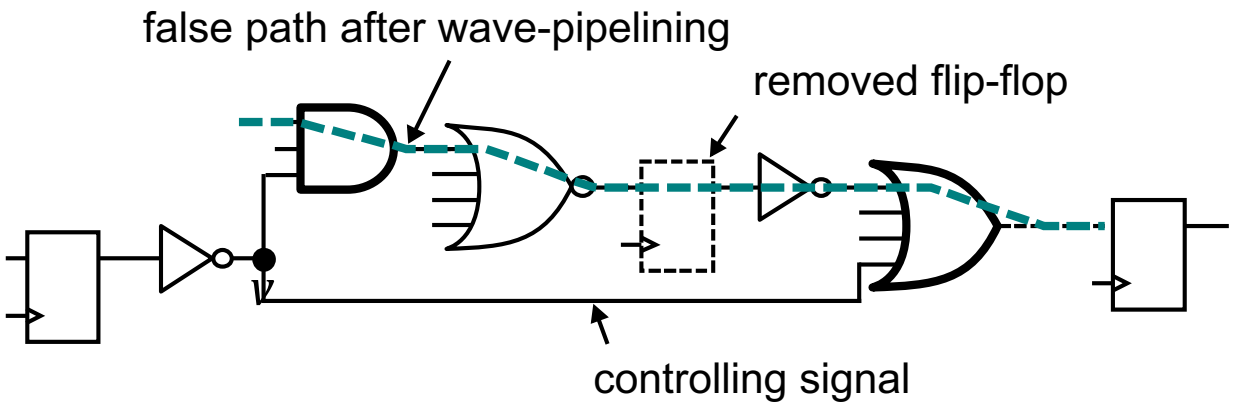
The fifth attack technique:
Calculate all gate delays from tested paths

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

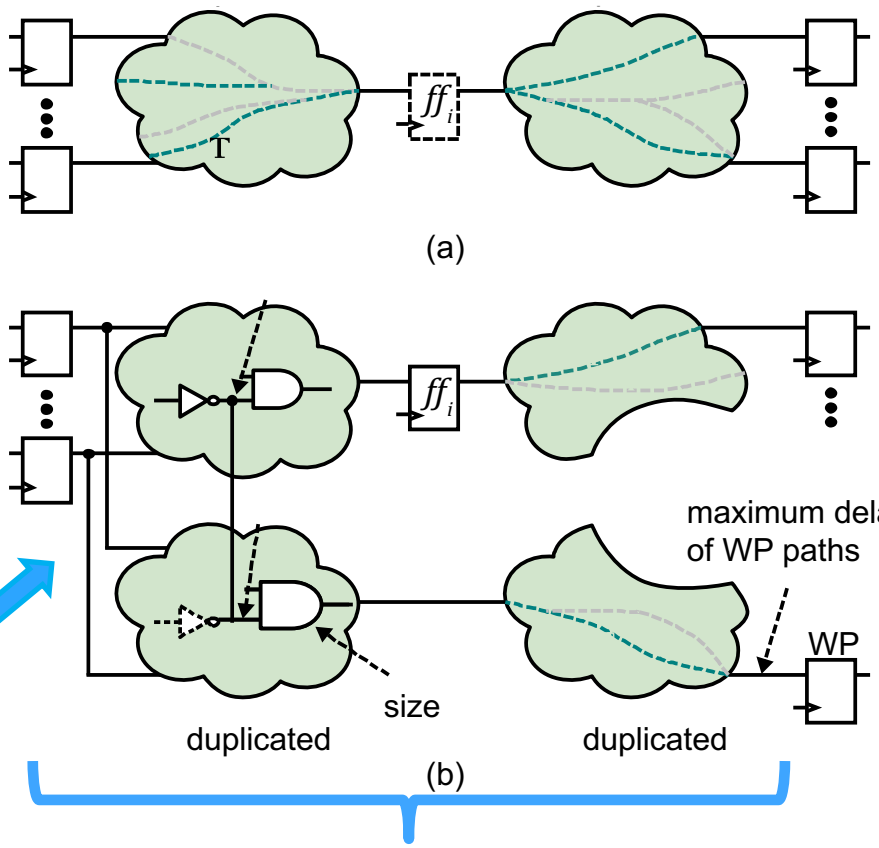
At-speed testing of path delays inaccurate

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