TimingCamouflage: Improving Circuit Security against Counterfeiting by Unconventional Timing

Grace Li Zhang[1], Bing Li[1], Bei Yu[2], David Z. Pan[3] and Ulf Schlichtmann[1]

1 Chair of Electronic Design Automation
Technical University of Munich (TUM)

2 The Chinese University of Hong Kong

3 University of Texas at Austin

Overview

- Motivation
- Attack techniques and countermeasures
- Implementation of TimingCamouflage
- Experimental results
- Summary

Counterfeiting Digital Circuits

- **Counterfeiting Threat:** the production of illegal chips by a third party with a netlist recognized through **reverse engineering.**

Authentic chips are delayered and imaged

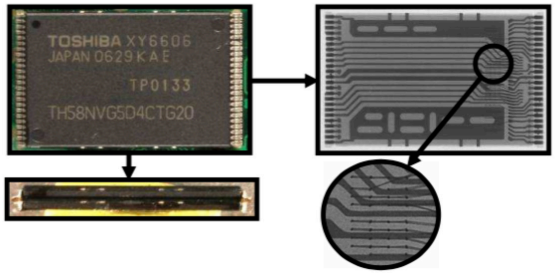
↓

Logic gates, flip-flops and their connections are identified

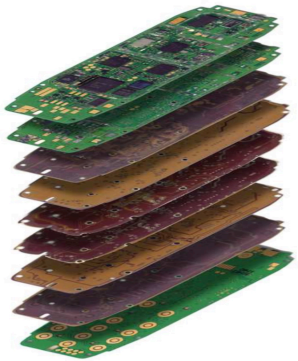
↓

The recognized netlist is processed with a standard IC design flow

optical and x-ray images of ICs

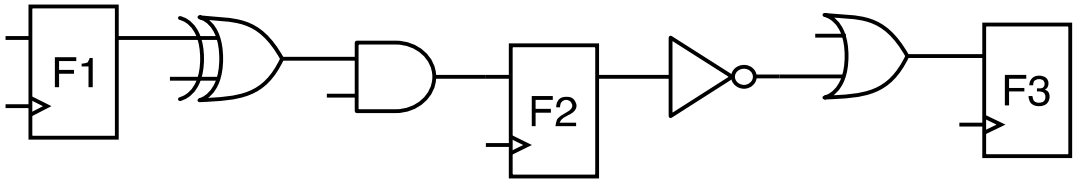


delayered nine-layer PCB from cellphone



R. Torrance et al., “Reverse Engineering in the Semiconductor Industry,” CICC, Sep, 2007

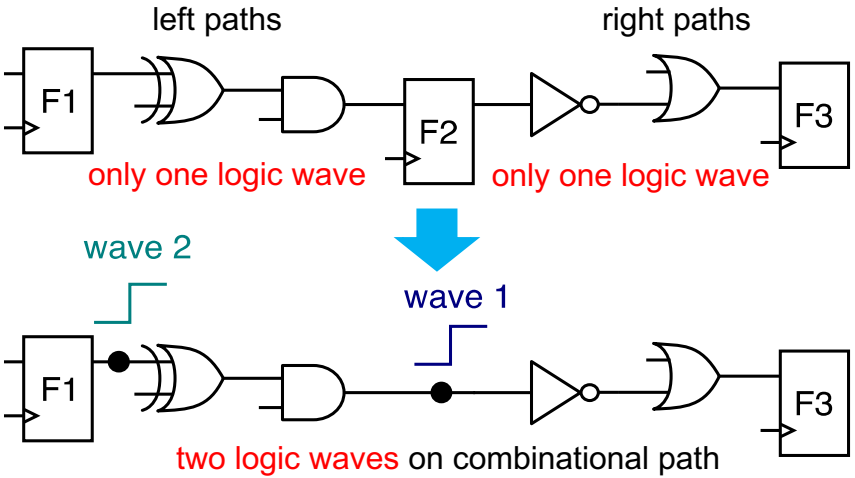
Counterfeiting with conventional timing

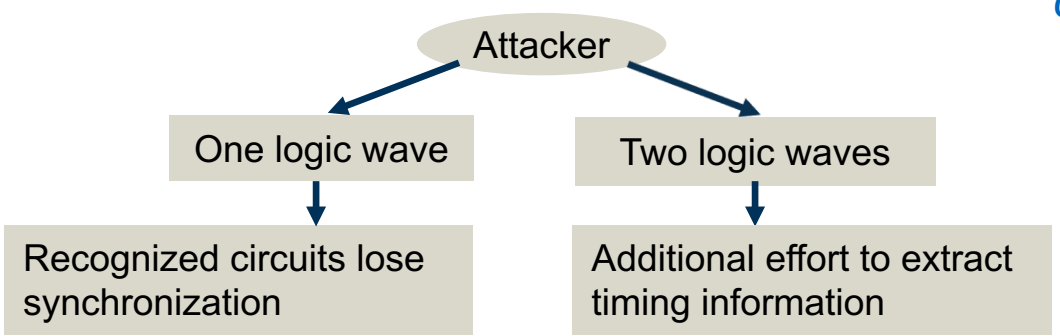


- Conventional timing model
  - All paths work within one clock period
  - Setup and hold time constraints are satisfied between pairs of flip-flops

A netlist is sufficient to reproduce a correctly working circuit!

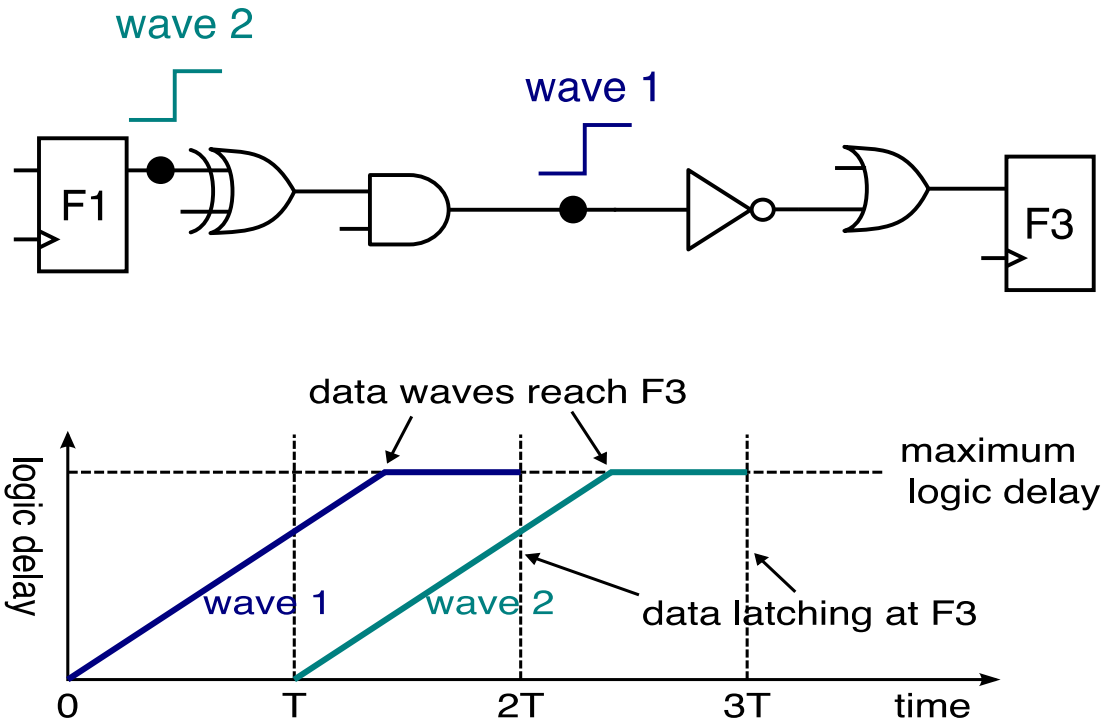
Counterfeiting with unconventional timing





With wave-pipelining, the function of a circuit depends on both its structure and the timing of combinational paths.

Timing constraints of wave-pipelining paths

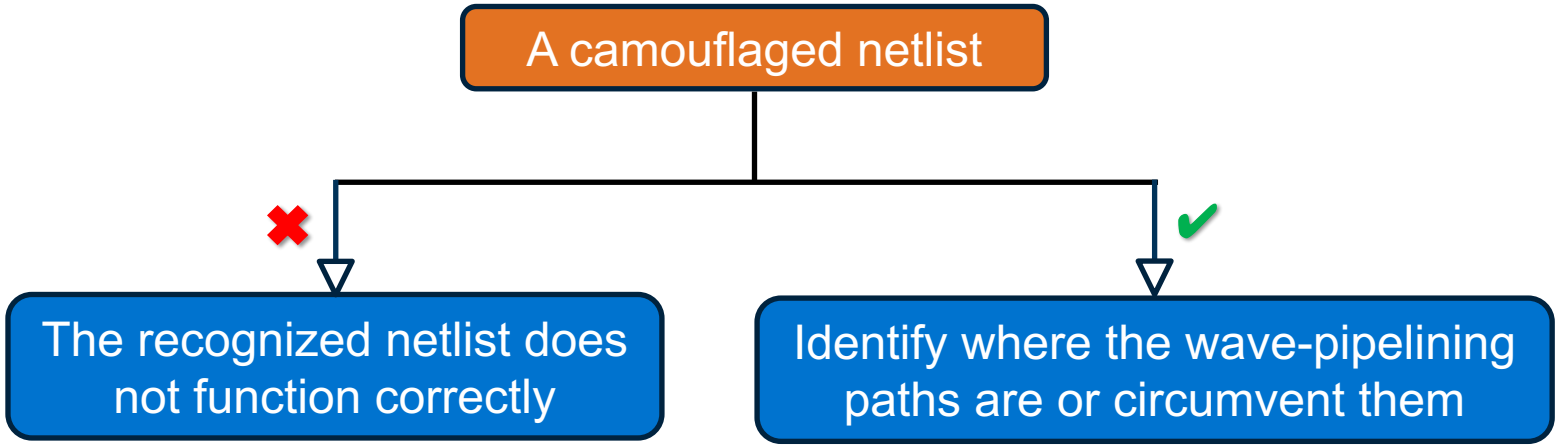


Wave-pipelining constraints

$$d_p \geq T + t_h, \forall p \in P$$

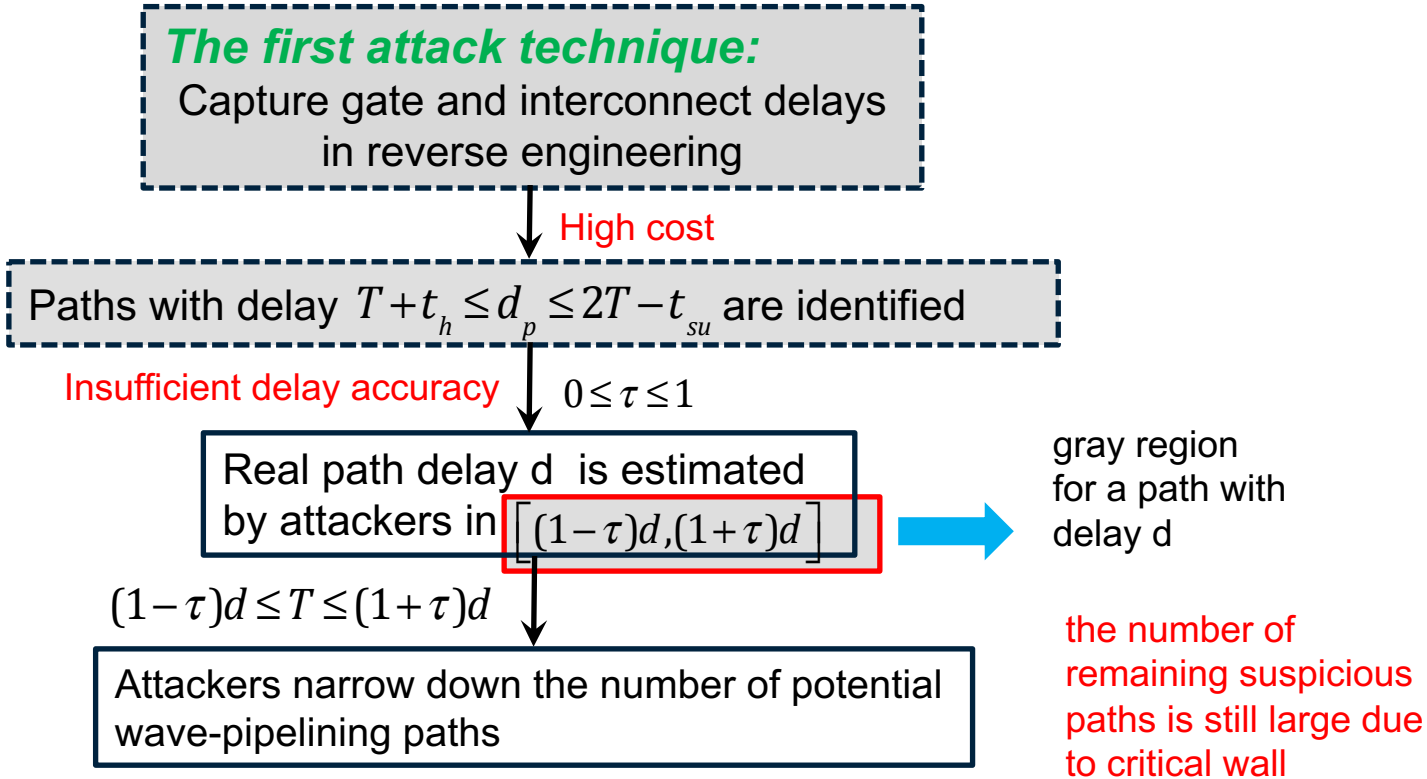
$$d_p \leq 2T - t_{su}, \forall p \in P$$

Attack techniques and countermeasures

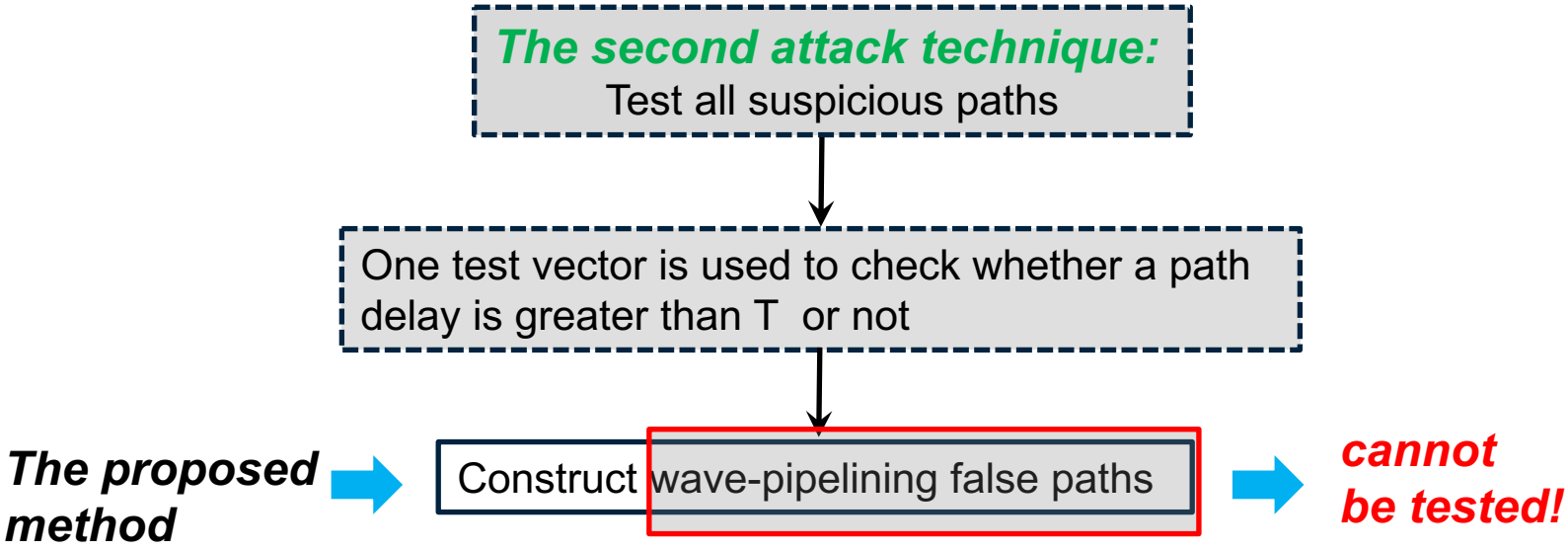


- Attack model
  - A netlist recognized by reverse engineering
  - Estimated delays of logic gates and interconnects with an inaccuracy factor τ
- Attack objective
  - Identify the locations of wave-pipelining paths in the netlist

Attack techniques and countermeasures



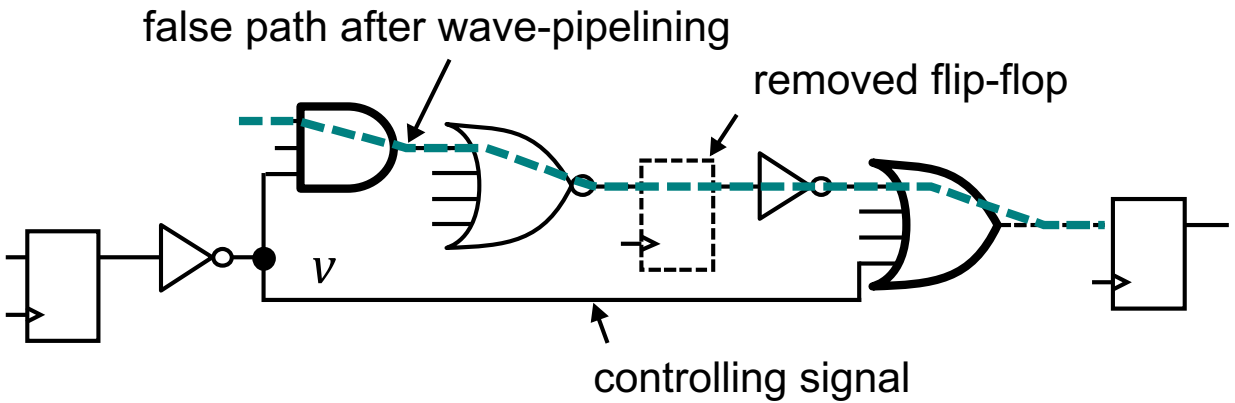
Attack techniques and countermeasures



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.



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

↓

Size logic gates of all false paths to meet the gray region.

Difficult to find a solution

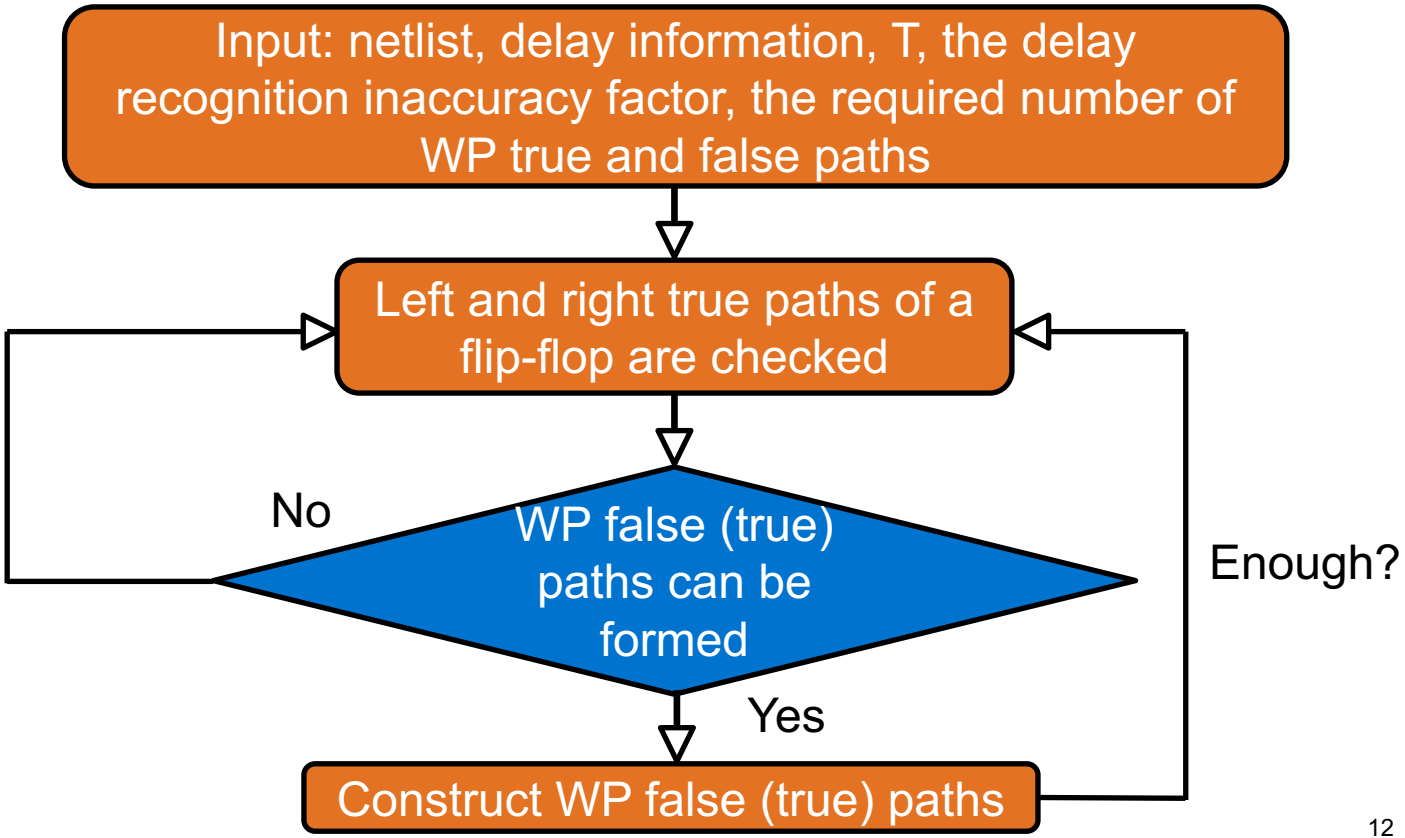
The fifth attack technique:
Calculate all gate delays from tested path

↓

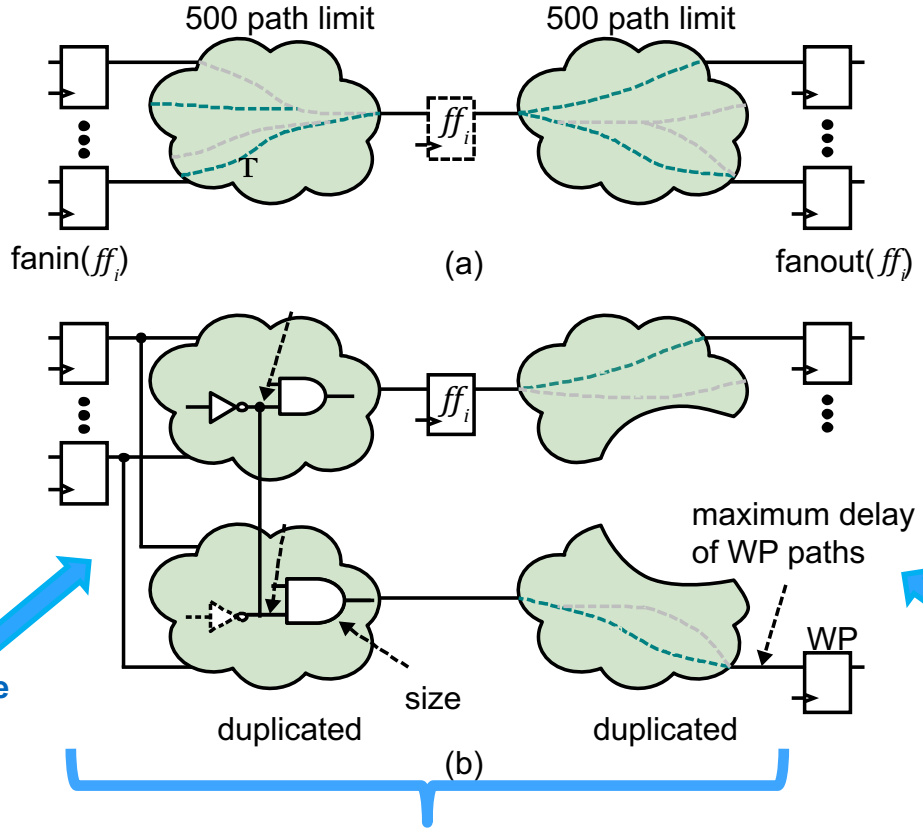
Measured path delays can be used to calculate gate delays with linear algebra.

At-speed testing of path delays inaccurate

Implementation of TimingCamouflage



Implementation of TimingCamouflage



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 flip-flops

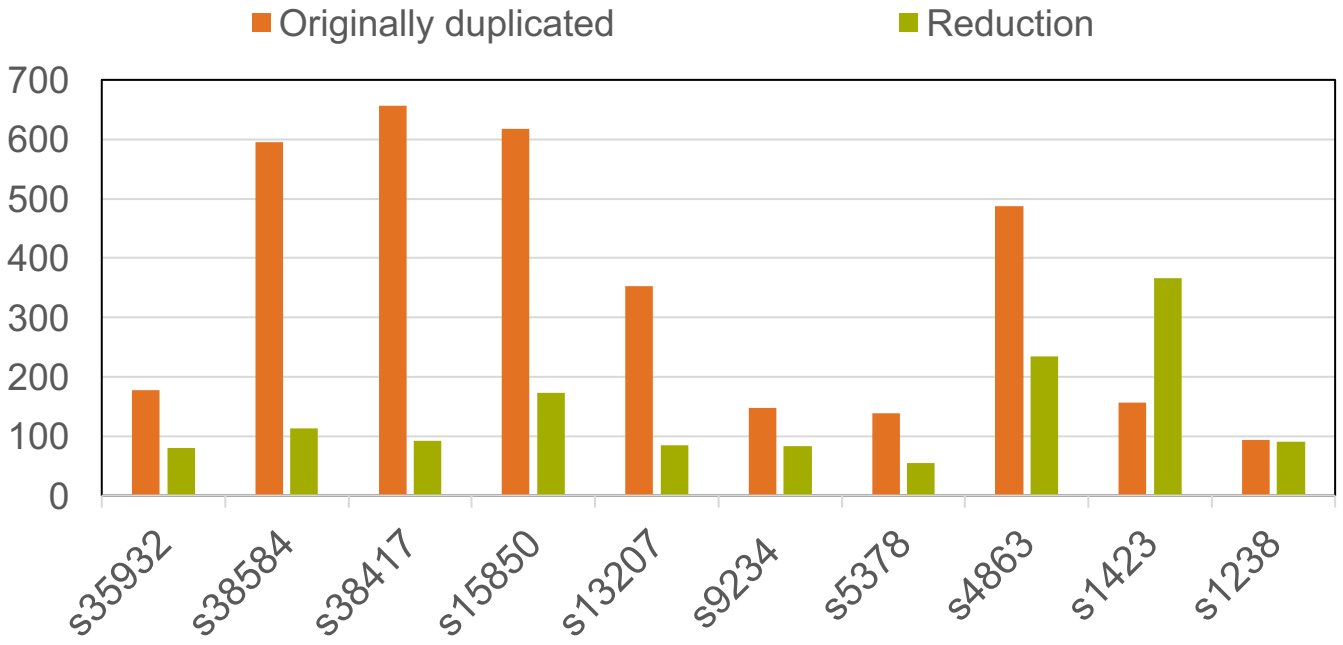
Delays of wave-pipelining constraints

Results of constructing WP paths

Circuit	number of single-period true paths	number of WP true paths	number of WP false paths	number of duplicated gates	number of inserted buffer
s35932	180039	20	1022	178	80
s38584	502561	48	431	130	117
s38417	298922	82	63	321	65
s15850	361544	20	838	186	141
s13207	927424	20	115	152	74
s9234	10922	20	983	148	83
s5378	10143	401	78	139	55
s4863	4140	680	0	184	77
s1423	8506	450	12	75	213
s1238	15	3	4	94	90

WP false and true paths can be constructed successfully

Results of duplicated number of gates



The number of logic gates in duplicated circuit is reduced significantly

Summary

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

- The difficulty of attack has been increased significantly by
  - additional test costs
  - wave-pipelining false paths

- Our ongoing work includes incorporating gate delay camouflage by doping modification to further decouple gate delays from layout.

Thank you for your attention!

Runtime

Circuit	T_r(s)
s35932	625.29
s38584	3685.88
s38417	1711.01
s15850	3018.06
s13207	446.17
s9234	291.45
s5378	266.022
s4863	3766.98
s1423	1170.71
s1238	2.07

Wave-pipelining false paths in test cases

Circuit	n_f	$\tau = 0.2$	$\tau = 0.1$
s5378	122757	80386	4845
s4863	0	0	0
s1423	2331927	58992	37312
s1238	392	0	0