Compass: Navigating the Design Space of Taint Schemes for RTL Security Verification

Yuheng Yang* (MIT), Qinhan Tan* (Princeton), Thomas Bourgeat (EPFL), Sharad Malik (Princeton), Mengjia Yan (MIT)

I. Overview

Hardware Security Problems:

- Side channel attacks
- Spectre attacks
- TEEs root-of-trust key leakage

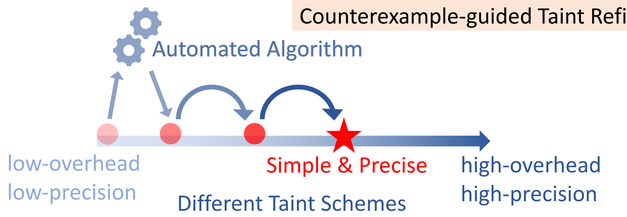
Violations of **Information Flow Property**

We verify them with **Taint Analysis**

Our Work:

- Observation: There is a large design space of taint schemes
- Goal: Find taint schemes that are simple and precise
- Solution: An automated, iterative approach to find efficient taint schemes

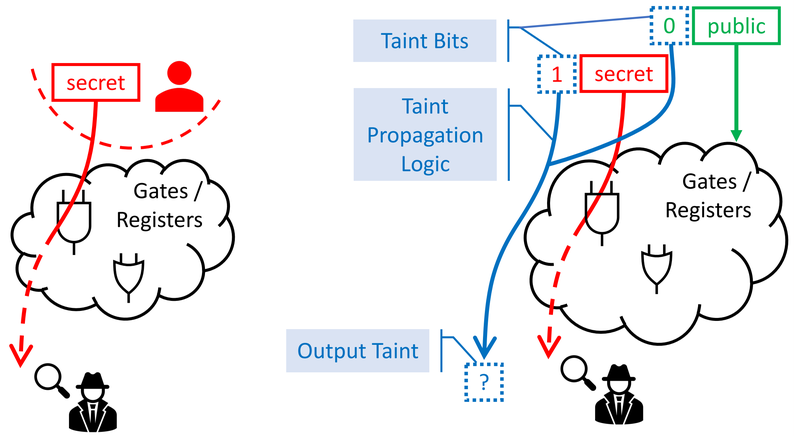
Technique:
Counterexample-guided Taint Refinement



II. Background

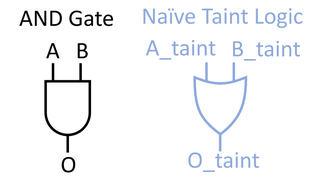
Information flow property
checks whether a secret can influence the value of attacker observable signals

Taint analysis
over-approximates information flow using taint bits and logic



III. Design Taint Schemes

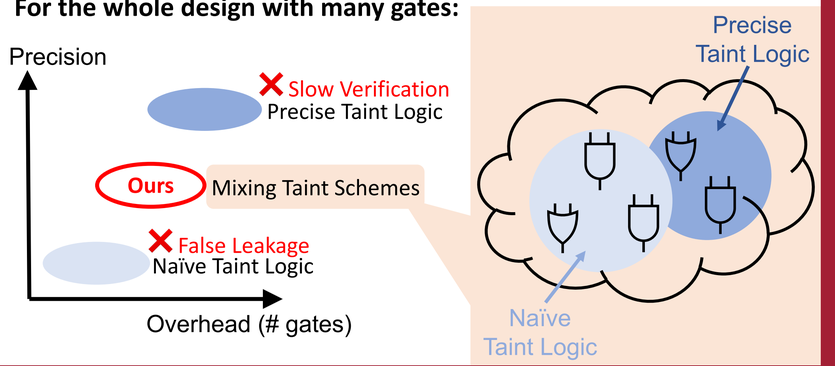
For a single AND gate:



Naïve taint logic introduces false flow

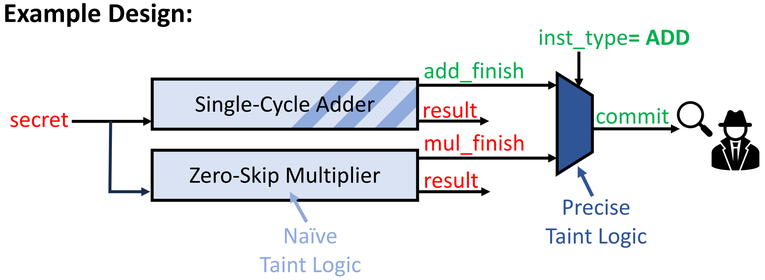
A	B	O	Leakage ?	O_taint
0	0	0	No	1
1	0	0		

For the whole design with many gates:



IV. Advantage of Mixing Taint Schemes

Example Design:

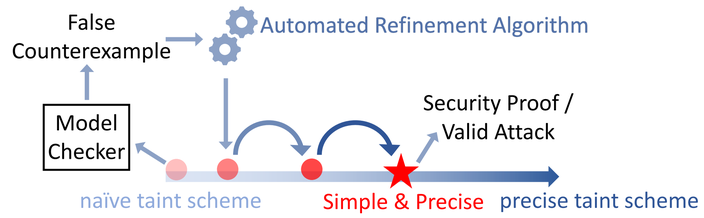


Property: Prove that if `inst_type==ADD`, then `commit_taint==0`

Challenge:
How to automatically discover gates that need precise taint logic?

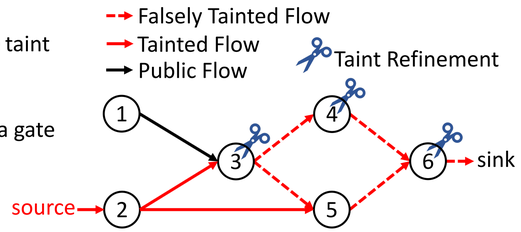
V. Compass Framework

Automated Counterexample-Guided Taint Refinement:



Refinement Algorithm:

- View circuit as a graph
- Color edges based on the taint propagation in the false counterexample
- View taint refinement of a gate as a "cut" on graph



VI. Evaluation Results

Setup:

- Processors Designs: Sodor, Rocket, BOOM (with Spectre defense), ProSpeCT
- Security Property: Secure speculation (software-hardware sandboxing contract)
- Baseline: CellIFT (generates precise taint logic for the whole design)

Result 1: 84% fewer taint gates, 85% fewer taint bits
Result 2: 32% less simulation time
Result 3: Faster model checking

- Unbounded Proof:

	CellIFT	Compass	
	Proof Time	Proof Time	Time to Find Taint Scheme
Sodor	2 h	10 s	5 min

- Bounded Proof:

	CellIFT	Compass	
	Bound with 7 days	Bound with 24 h	Time to Find Taint Scheme
Rocket	41	159	1 h
BOOM	26	28	31 h
ProSpeCT	29	29	35 h