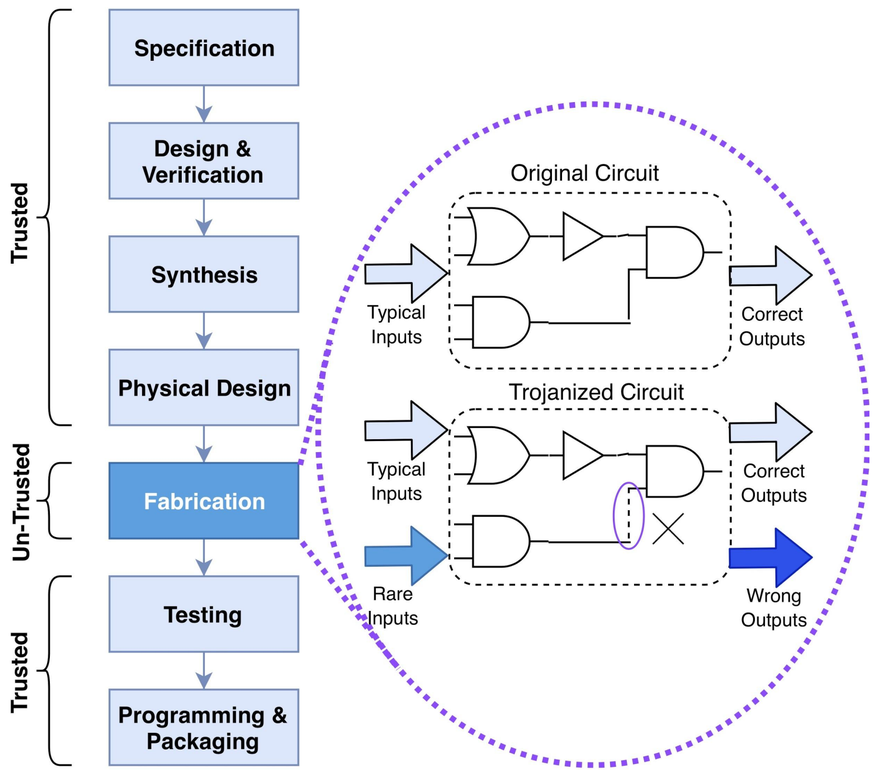
RSAC Security Scholar

Subtractive Hardware Trojans

Mohamed Tarek Ibn Ziad
Simha Sethumadhavan (Advisor)
Columbia University

COLUMBIA | ENGINEERING
The Fu Foundation School of Engineering and Applied Science

New Class of Hardware Trojans



- Removes (subtracts) a single wire from the gate-level netlist in order to trojanize the circuit.
- Prior work always adds extra logic gates or changes chemical composition.
  - Smallest additive Trojan is 1 capacitor and transistor (Analog backdoor).

Why Subtract?

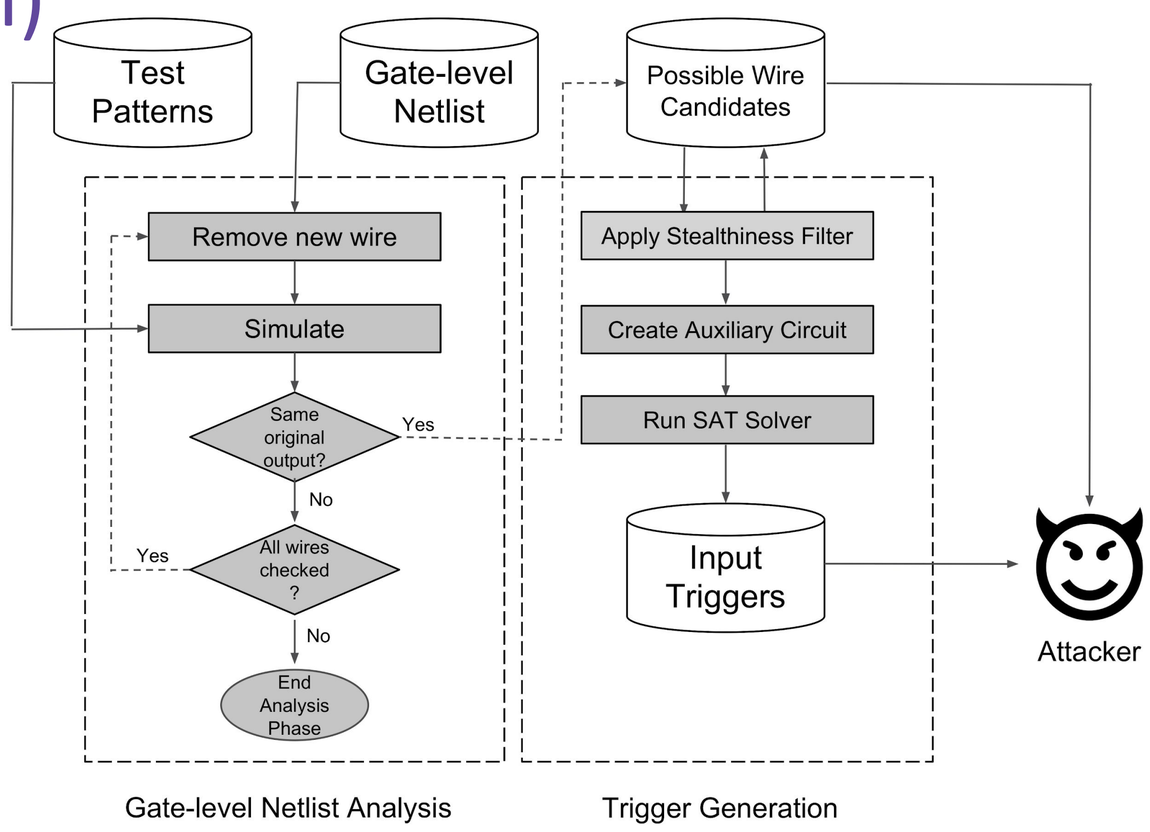
- Single wire edits are less likely to break complex fab design rule checks.
- So small that they can bypass post-silicon Trojan detection techniques.
  - Ex: functional testing, side channel analysis, and reverse engineering.

Rules of the Game (Threat Model)

- Defenders will be running Automatic Test Pattern Generation (ATPG) tests.
- Attackers will have access to ATPG tests.

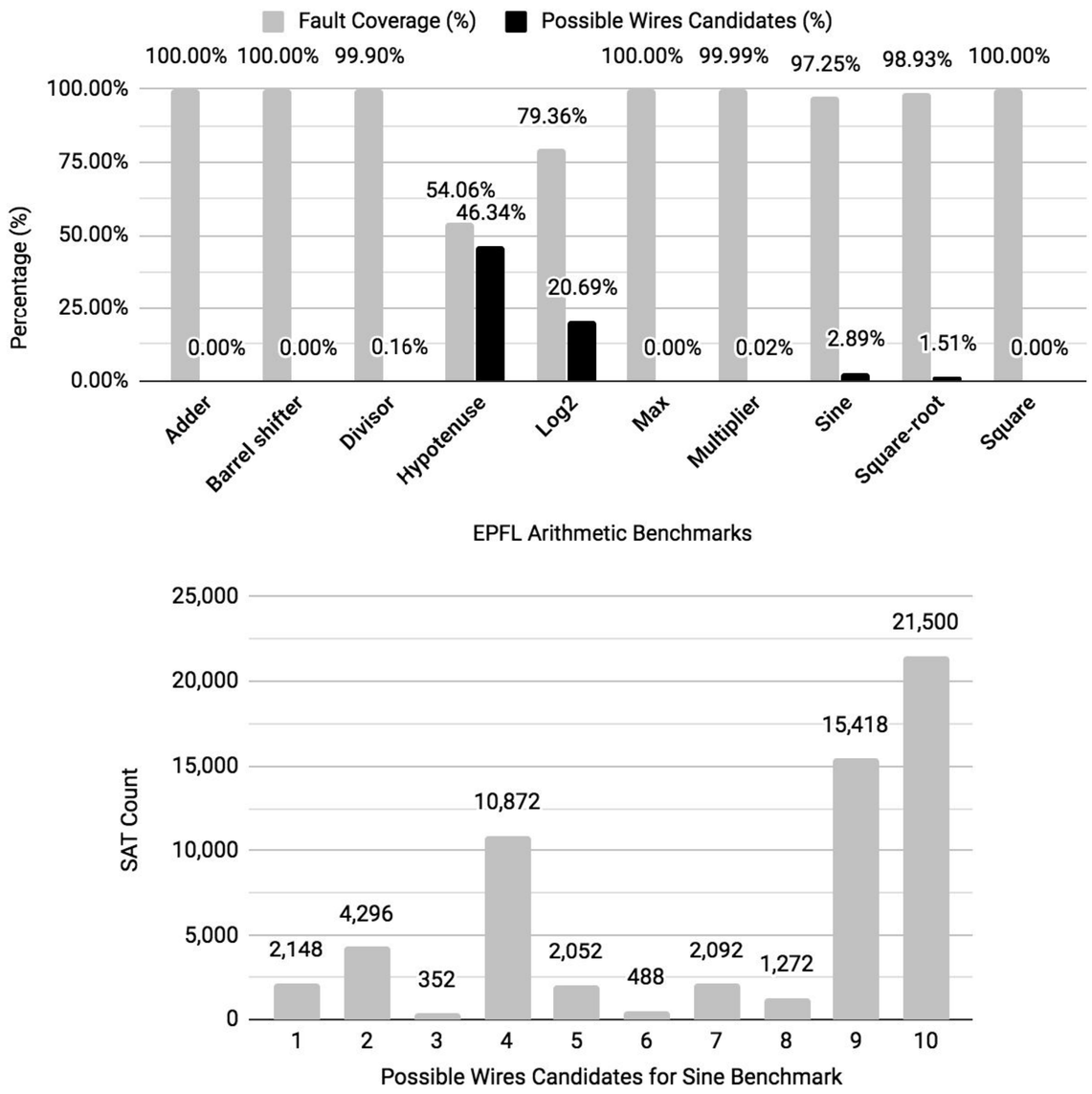
Strategy:

1. Find a circuit that passes all ATPG tests.
2. Make it so that circuit has exactly one less wire.
3. Find a trigger for that circuit using Boolean Satisfiability (SAT) solver.



Results

- We applied our framework on EPFL and ISCAS-85 benchmark suites.
  - Vulnerability to Subtractive Trojans increases with the increase of **circuit size** and **logic depth**.
- We compared the side-channel overheads of Subtractive Trojans vs. traditional Trojans from Trust-Hub.
  - Our Subtractive Trojans are more stealthy, while having almost zero area and power overheads.



Future Work

- Develop new methods for detecting Subtractive Hardware Trojans.