Secure Split Manufacturing

JV Rajendran, UT Dallas, Email: jv.ee@utdallas.edu

Jiang Hu, Texas A&M, Email: jiang.hu@tamu.edu

Broader Research Goals

- How do we protect our design from an untrusted foundries against piracy attacks?
- How can we incorporate security features into IC design tools in a low-cost fashion?

Objective

- Hardware is prone to supply-chain attacks
- Most attacks originate from untrusted foundry
- Avoid giving complete designs to the untrusted foundry
- Solution: Split manufacturing
  - Manufacture front-end-of-line at untrusted foundry
  - Manufacture back-end-of-line at trusted foundry

Threat Model

- Attacker is in the FEOL foundry; no access to BEOL
- Attacker can generate gate-level netlist from GDSII
- Resulting netlist contains gates and unknown input-output (IO) connections
- Attacker does not know the IO relationship of the original design

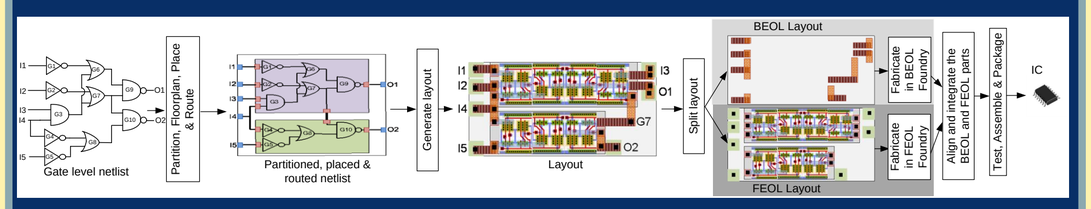
Problem

Trojans

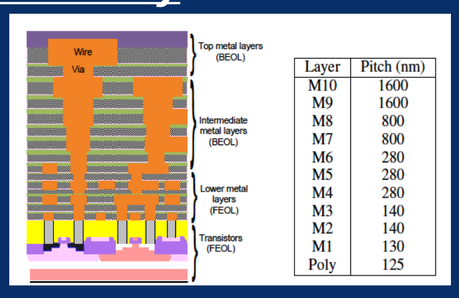
Counterfeit

Piracy & Overbuilding

Solution: Split manufacturing



Feasibility



Layer	Pitch (nm)
M10	1600
M9	1600
M8	800
M7	800
M6	280
M5	280
M4	280
M3	140
M2	140
M1	130
Poly	125

Different requirements in manufacturing FEOL and BEOL

↓

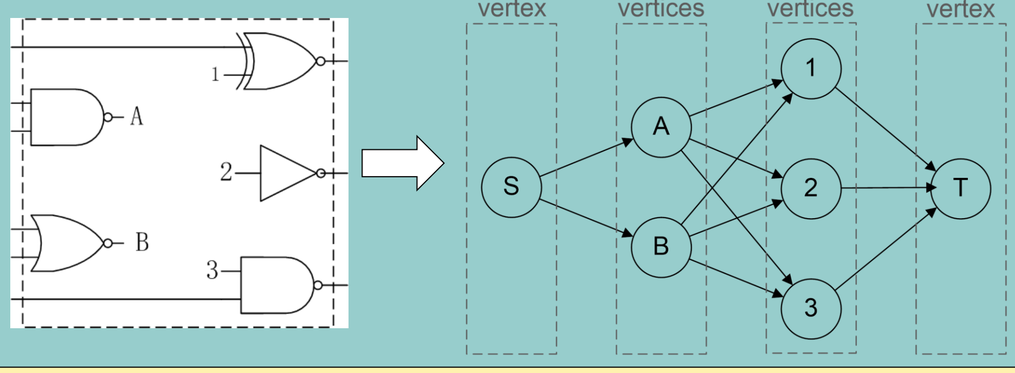
Leverage for security

Approach: Exploit heuristics of physical-design tools to attack

Hints for an attacker

- Acyclic combinational logic circuit
- Physical proximity
- Load capacitance constraint
- Timing constraint
- Directionality of dangling wires

Problem formulation: Min-cost n/w flow



Defense: Placement Perturbation

Input : a design after global routing and wire layer assignment

↓

Extract tree from circuit (DAG)

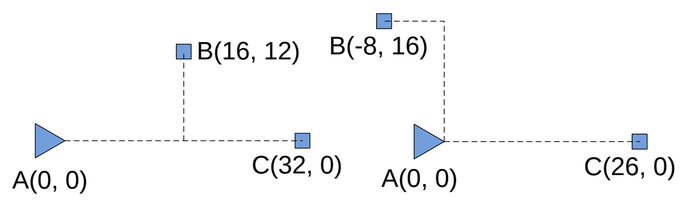
↓

Do placement from leaf to root of the tree

↓

Output : layout with placement

- Pareto optimization
- Two dimensions:
  - ♢ Pin distance (Overhead)
  - ♢ Perturbation (Security)



$$\pi_{A,B}^{x} = 2 \cdot |-8 - 16| = 48$$

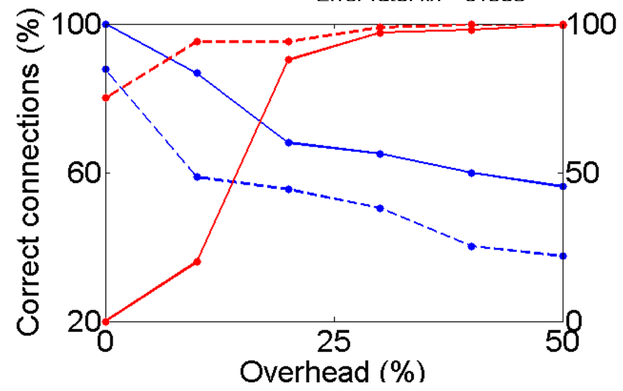
$$\pi_{A,B}^{y} = 1 \cdot |16 - 12| = 4$$

$$\pi_{A,C}^{x} = 0 \cdot |26 - 32| = 0$$

$$\pi_{A} = \pi_{A,B}^{x} + \pi_{A,B}^{y} + \pi_{A,C}^{x} = 52$$

Results

- Benchmark circuits: ISCAS85, ITC99
- Layout generated with Cadence tool
- Attack recovers 84% of missing wires
- Defense with 5% overhead increases error rate to 82%



Security vs. overhead tradeoff

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan 9-11, 2017
Arlington, VA

UT DALLAS
TEXAS A&M UNIVERSITY