OHM: Online Hardware Monitors

Dr. SREE RANJANI RAJENDRAN,
Postdoctoral Researcher, RISE Lab, IITM
email: sreeranjanirajendran@gmail.com

Introduction

Hardware security directly ensures the *integrated circuit* (IC) security, since hardware includes the interconnection of ICs. Globalization of the IC design flow is the main reason for hardware vulnerabilities.

*"**Outsourcing** the **fabrication** and **design** to **third parties** imputed to the huge scales of requirements and **economies involved**"*

HW Threats

Challenge

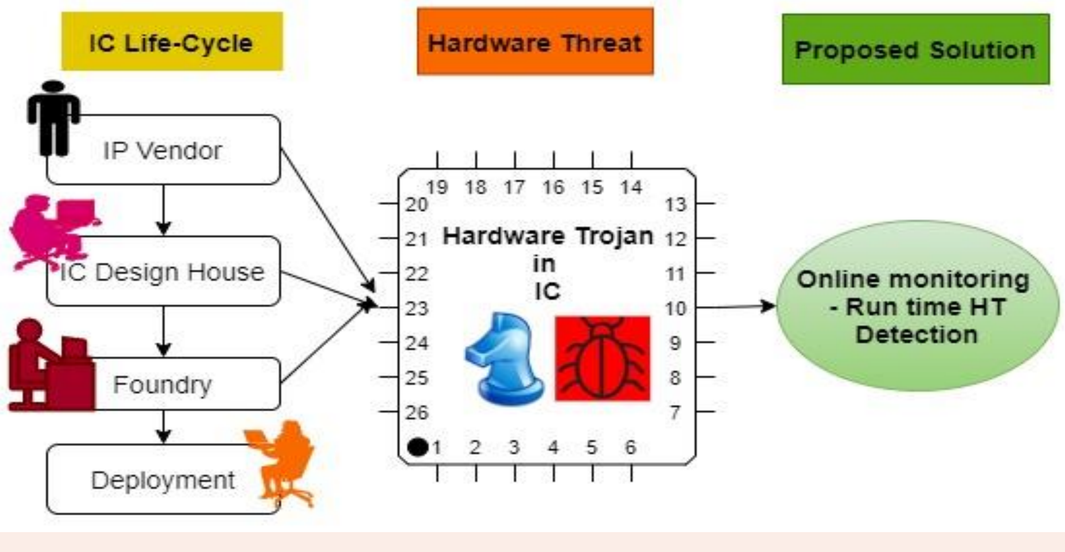
Is there any unique solution against the Hardware attack?

Threat Model

Scenario	IP Vendor	Design House	Foundry	End user
i	☺	☻	☻	☺

☻–*an attacker,* ☺–*an trustworthy entity*

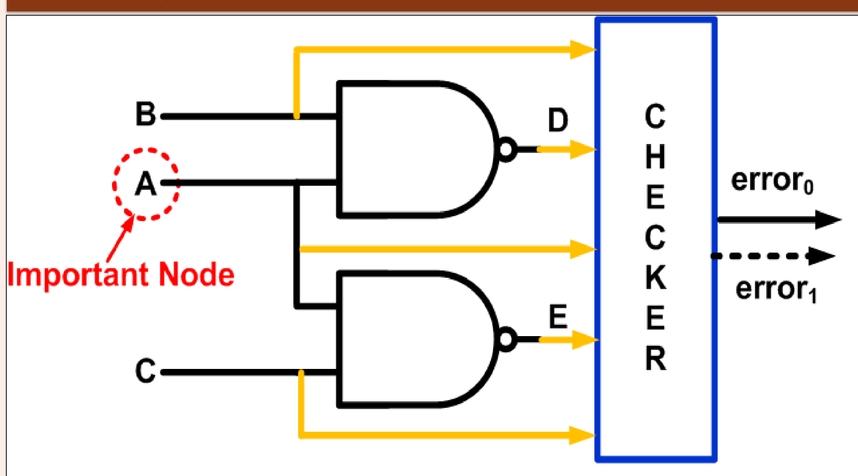
Proposed Countermeasure



Proposed an Automated Design Flow

- To the given netlist, the internal nodes are identified to which the HTs are inserted probably.
- Insert the low overhead checkers at a selected subset of internal nodes.
- The logic malfunctions are identified and reported by the online checkers.
- The number of checkers inserted are restricted to have a low hardware overhead with maximum HT detection accuracy.

Single-rail and Double-rail Checker



Single-Rail Checker Logic

```
if (A == 1)
  error0 = (D^~B) | (E^~C);
else if (A == 0)
  error0 = ({D,E} != 2'b11);
```

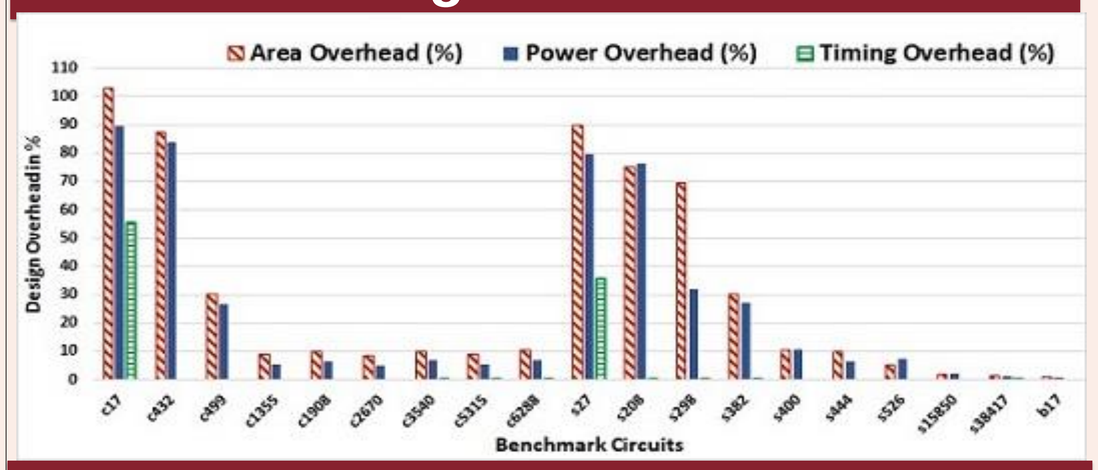
Two-Rail Checker Logic

```
if (A == 1)
  {error0, error1 } = ((D^~B) | (E^~C)) ? 2'b10 : 2'b01;
else if (A == 0)
  {error0, error1} = ({D,E} != 2'b11) ? 2'b10 : 2'b01;
```

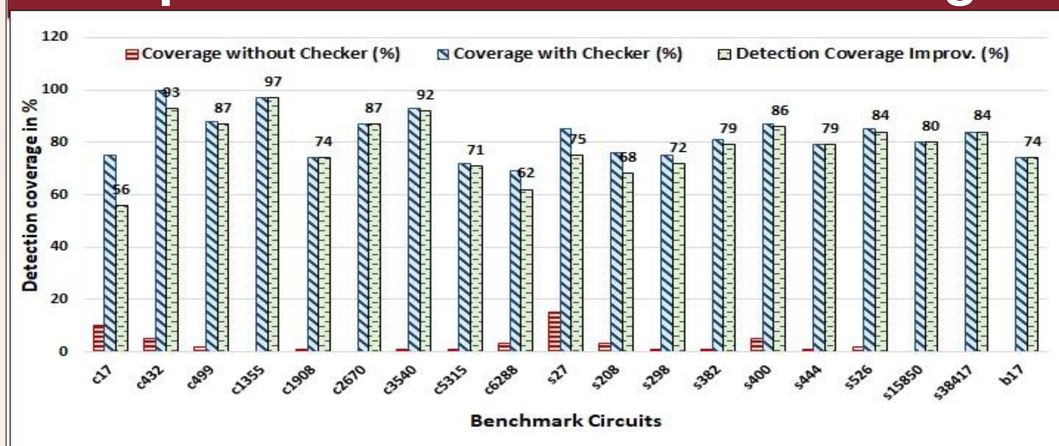
HT Detection Metrics

- Detection Coverage
- Design Overhead

Design Overhead



Improved HT Detection Coverage



Conclusions

- 100% detection coverage with controlled design overhead of 10%.
- Avoids the functionality change of the original circuit due to the checker module, since the checker module is functionally free circuit.
- Resistant to cell replacement attack, since reverse-engineering is not possible
- Extended easily to secure the system designed.

References

1. R. S. Chakraborty, S. Pagliarini, J. Mathew, **R. Sree. Ranjani**, and M. N. Devi, "A flexible online checking technique to enhance hardware Trojan horse detectability by reliability analysis," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 2, pp. 260–270, 2017.
2. **R. Sree Ranjani** "Online monitoring technique to build a Trusted Hardware Design", VLSID 2016 (PhD Forum).
3. **R. Sree Ranjani** "Online monitoring based Design-for-Trust technique to Design a Trusted Hardware Design", VLSID 2020 (User Design Track).