CASE WESTERN RESERVE UNIVERSITY EST. 1826

EECS DEPARTMENT

MERO: A Statistical Approach for Hardware Trojan Detection

Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou and Swarup Bhunia

Department of Electrical Engineering and Computer Science

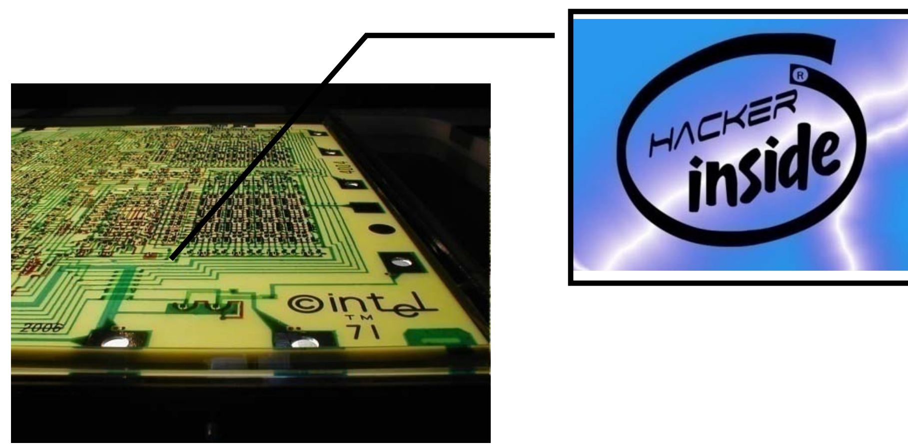
Case Western Reserve University

Cleveland, OH-44106, USA

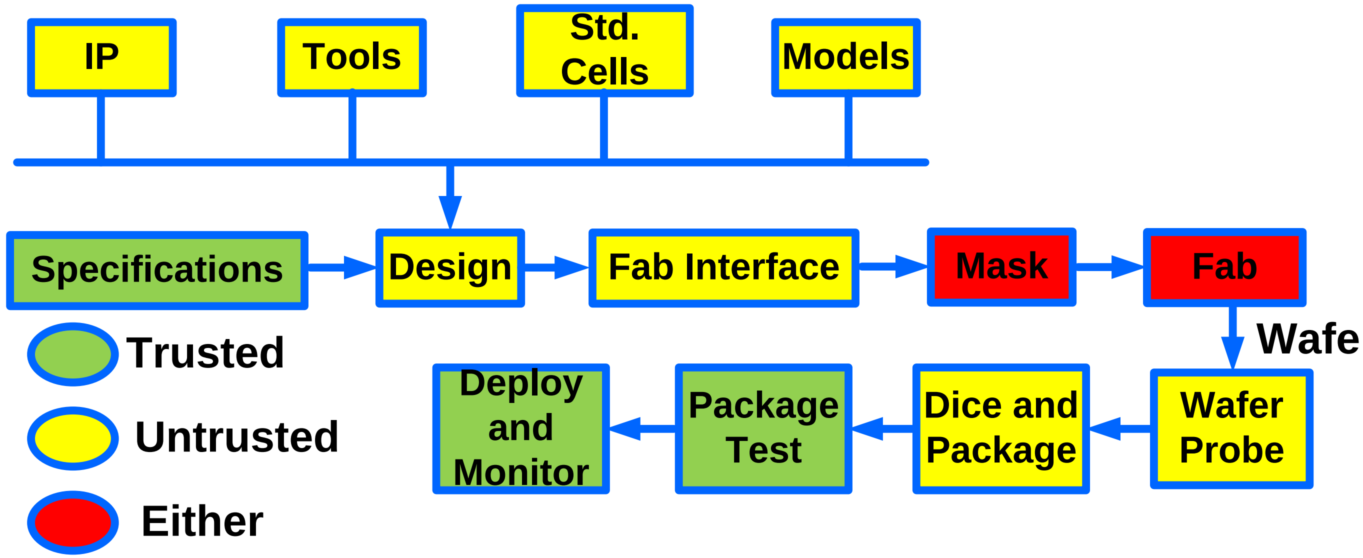
CHES-2009

Outline

- **Introduction**
- **Background and Motivation**
  - **Existing approaches of Trojan detection**
  - **Motivation for a statistical approach**
- **Proposed Technique**
  - **Overview**
  - ***MERO: Multiple Excitation of Rare Occurrence***
  - **Automation**
- **Results**
- **Conclusion**



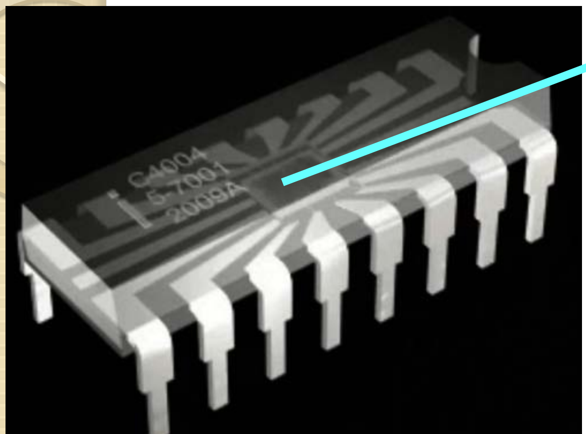
Modern IC Design & Manufacturing

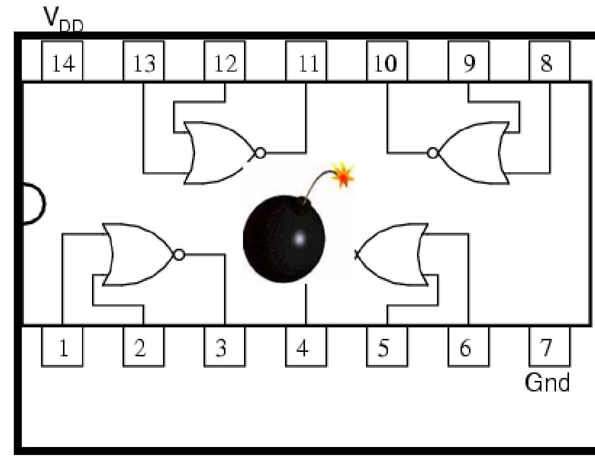


- **Economics of IC Design and Manufacturing:**
  - ***Intellectual Property*** **(IP) based designs**
  - ***Fabless*** **manufacturing model (trend on the rise)**
  - **Outsourcing of manufacturing to offshore *fabs***
  - **Loss of control over design and manufacture**
  - **Potentially untrusted parties getting involved**

http://www.darpa.mil/MTO/solicitations/baa07-24/index.html

What are Hardware Trojans?

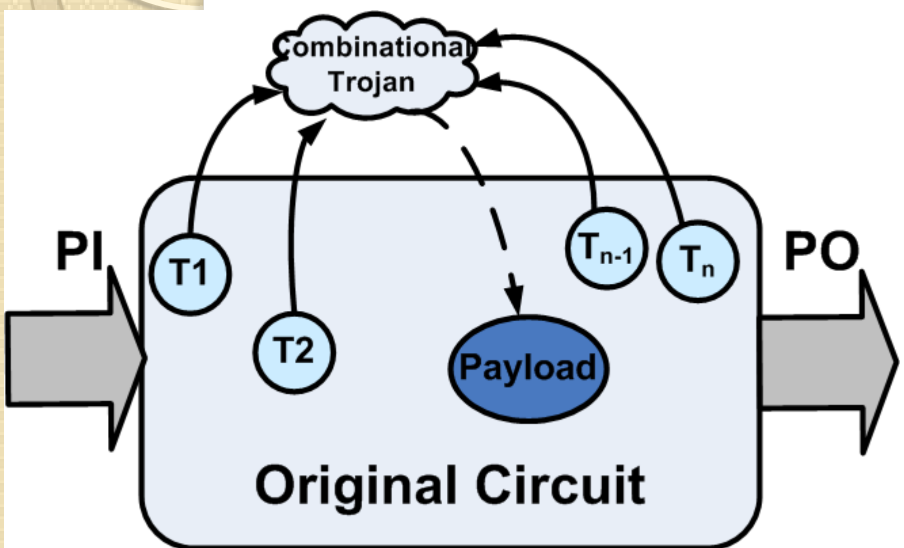




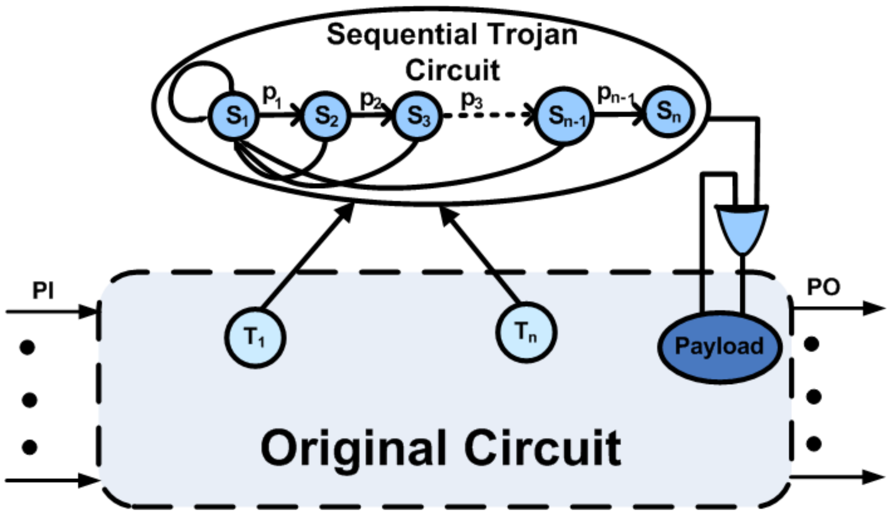
- **Malicious modifications to design**
  - **Causes IC to malfunction in-field**
  - **Can take place during design or fabrication**
  - **Inserted by an intelligent adversary**
  - ***Stealthy* => difficult to detect**
- **Results:**
  - **Potentially disastrous consequences in critical areas e.g. military installations, civilian infrastructures**

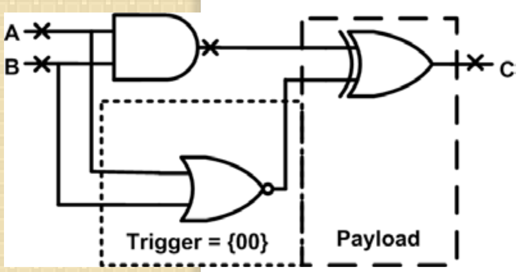
Hardware Trojan: Examples

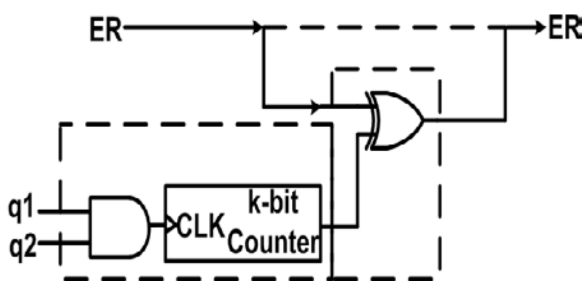
Combinational Trojan model

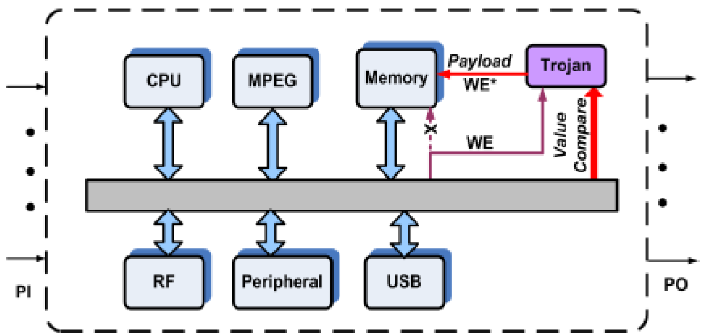


Sequential Trojan Model







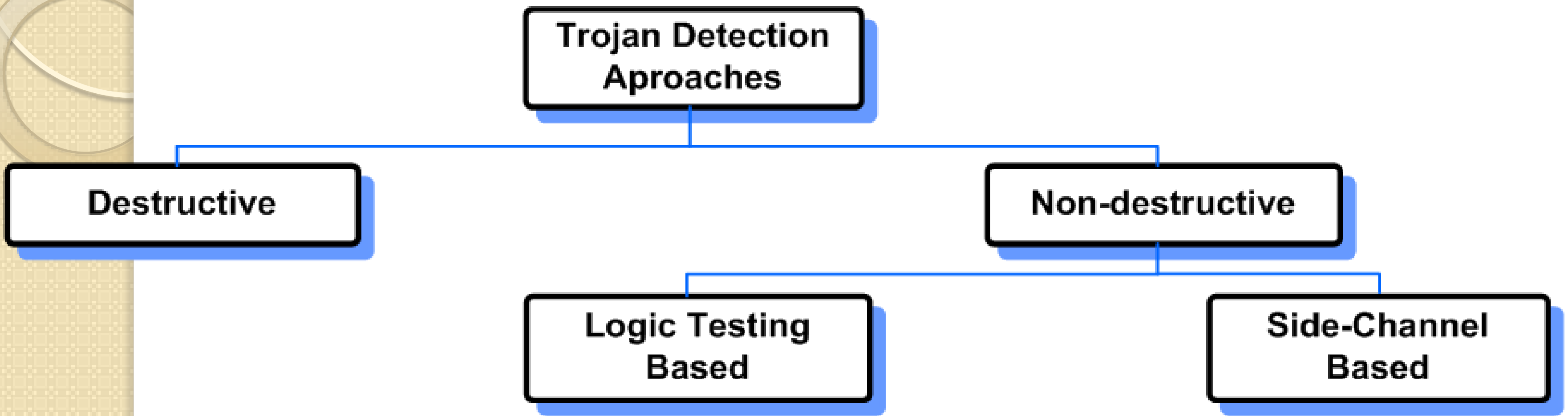


Comb Trojan Example

Seq Trojan (time-bomb) Example

System level view

Hardware Trojan Detection



	Logic Testing Approach	Side-Channel Analysis Approach
Pros	• Robust under process noise • Effective for ultra-small Trojans	• Effective for large Trojans • Easy to generate test vectors
Cons	• Difficult to generate test vectors • Large Trojan detection challenging	• Vulnerable to process noise • Ultra-small Trojan detection challenging

The proposed approach target both logic testing & side-channel analysis!

Chakraborty et al, HOST 2008

Wolff et al, DATE 2008

Why Statistical Approach?

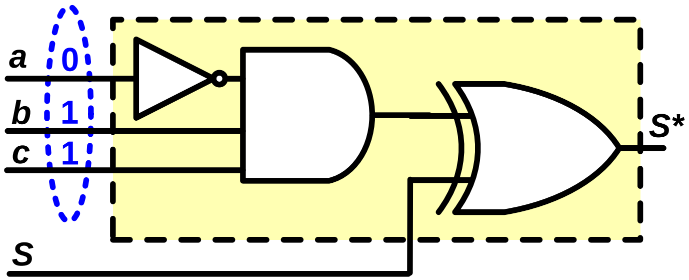
- **Feasible Trojan search space is inordinately large!**
  - **Combinatorial function of number of circuit nodes**
  - **Exhaustive enumeration impossible**
  - ***Deterministic* test generation computationally infeasible**
  - **Adversary likely to choose rarely triggered/observed Trojans**

- **A Statistical Approach for Trojan Detection**
  - **Finds the rare events in the circuit**
  - **Generates test vectors to trigger each trigger node multiple times**
  - **Provides high confidence about the *quality of testset***

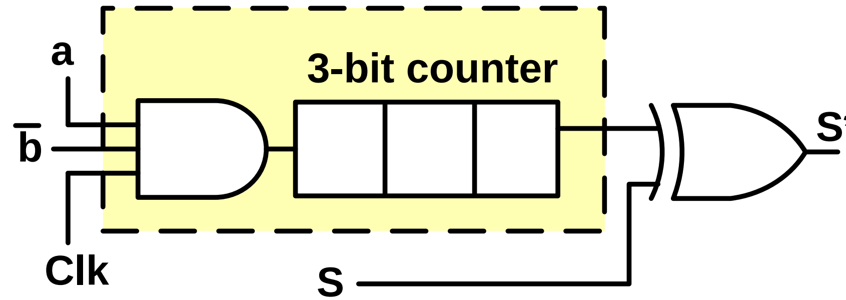
Multiple Excitation of Rare Occurrences (MERO) Approach

- **Assumptions:**
  - **An inserted Trojan has a small but non-zero activation probability**
  - **Can be combinational/sequential consisting of *q* trigger nodes**
- **Method:**
  - **Apply test vectors that trigger each node to its rare value at least *N* times**
- **Main inferences of analysis:**
  - **Expected number of times of Trojan getting triggered proportional to *N***
  - **Trojan triggering probability decreases as number of trigger nodes (*q*) increase**
  - **Trojan triggering probability increases if trigger probability of individual trigger nodes (θ) increases**

Circuit Example



(i) Combinational Trojan



(ii) Sequential Trojan

- **Trojan Trigger Condition:**

  (i) a=0, b=1, c=1 ***(ii) a=1, b=0***
- **Generate vectors to satisfy each of these conditions multiple (*N*) times**
- **Probability of Trojan activation increases with *N***
- **The concept is similar to *N-Detect Tests****

** I. Pomeranz and S.M. Reddy, 2004.*

MERO Steps

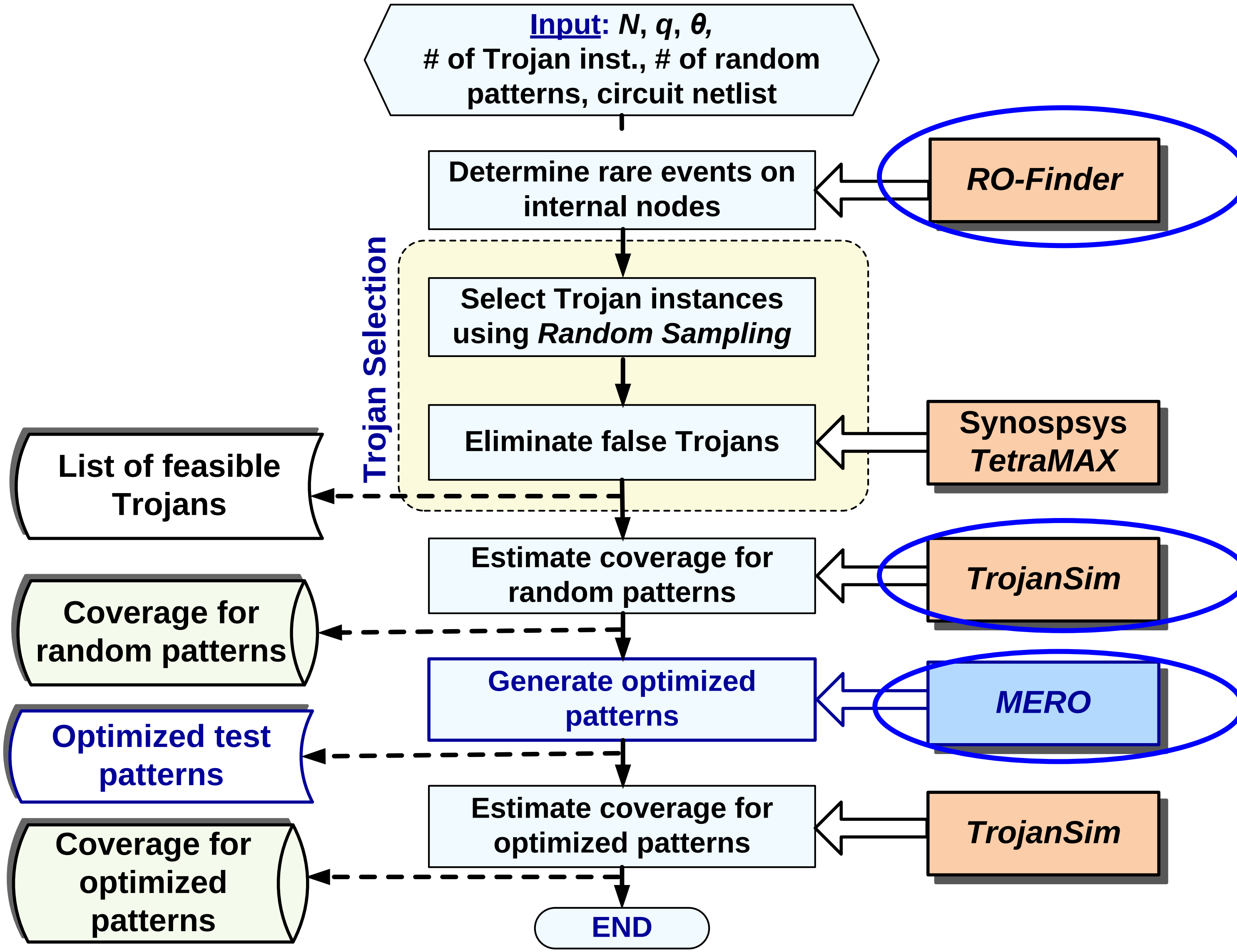
Test Generation Steps

- **Determine *rare nodes* and associated *rare values***
- **Generate random vectors**
- **Rank vectors with decreasing rare node trigger probability (*r*)**
- **For each vector in the ranked list**
  - **Perturb one/two bit(s) at a time**
  - **Retain the perturbation if *r* improves**
- **Stop if all rare nodes are excited to their rare values *N* times**

Trojan Coverage Steps

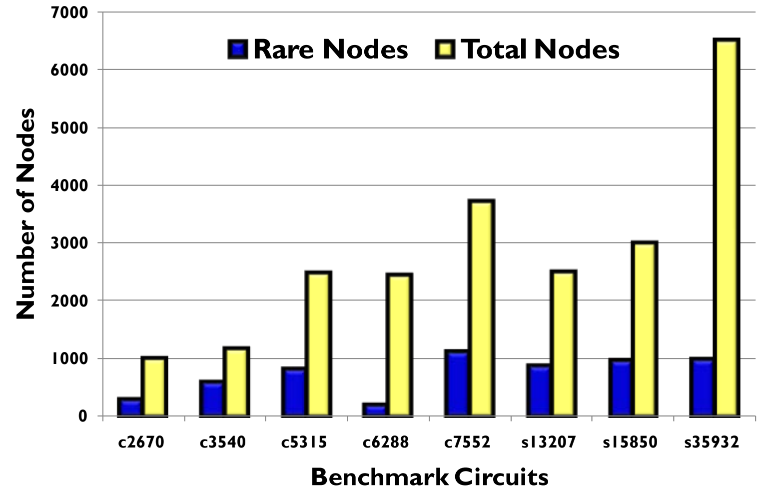
- **Create Trojans with trigger node probability < *θ* *(trigger-threshold)***
- **Perform *Random Sampling* over Trojan space**
- **Eliminate *False Trojans* (by justification)**
- **Perform functional simulation for an input testset**

MERO Implementation & Validation

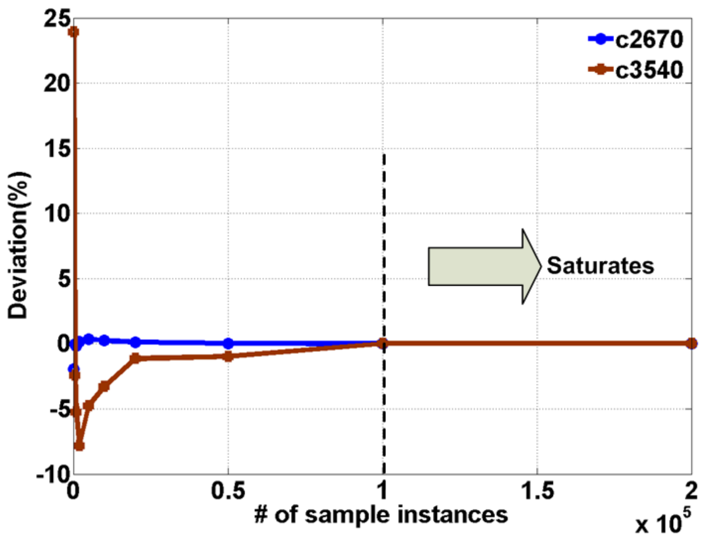


Simulation Results

- **ISCAS'85 and ISCAS'89 ckts**
  - **Comb/seq Trojans**
  - **# of trigger nodes (*q*) set to 2 or 4**
  - ***Θ* set to 0.2**

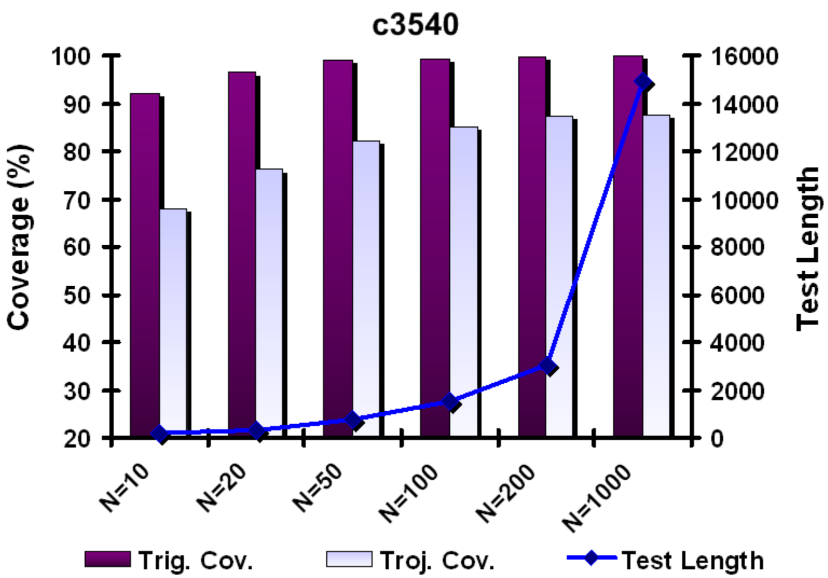


Effect of Sample Size on Coverage



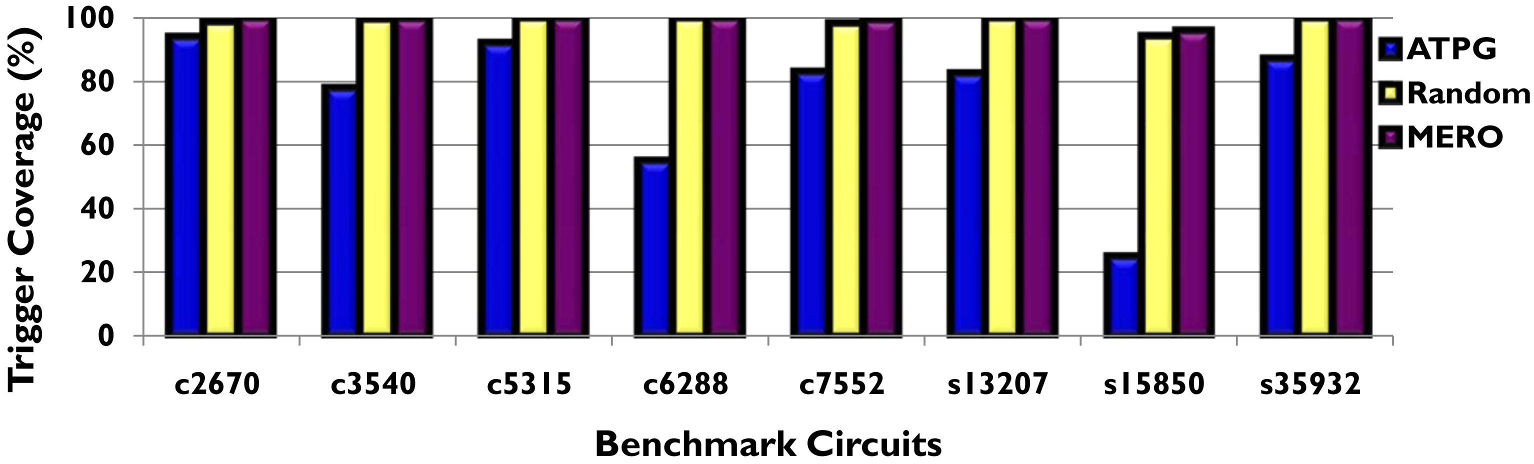
Sample size = 100,000

Effect of *N* on coverage

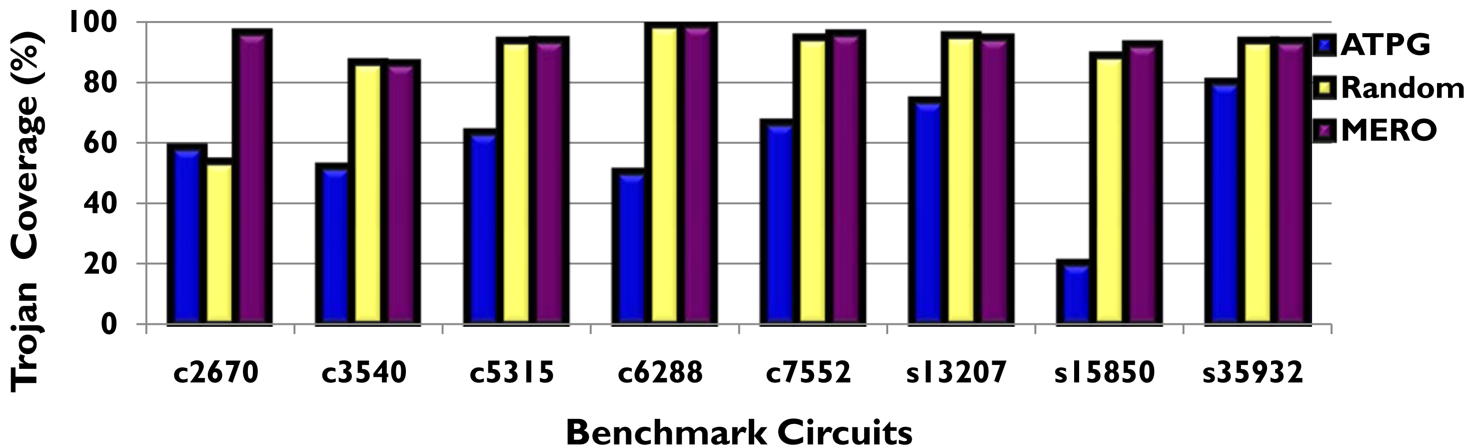


***N* = 1000**

Simulation Results: Coverage (q=2)



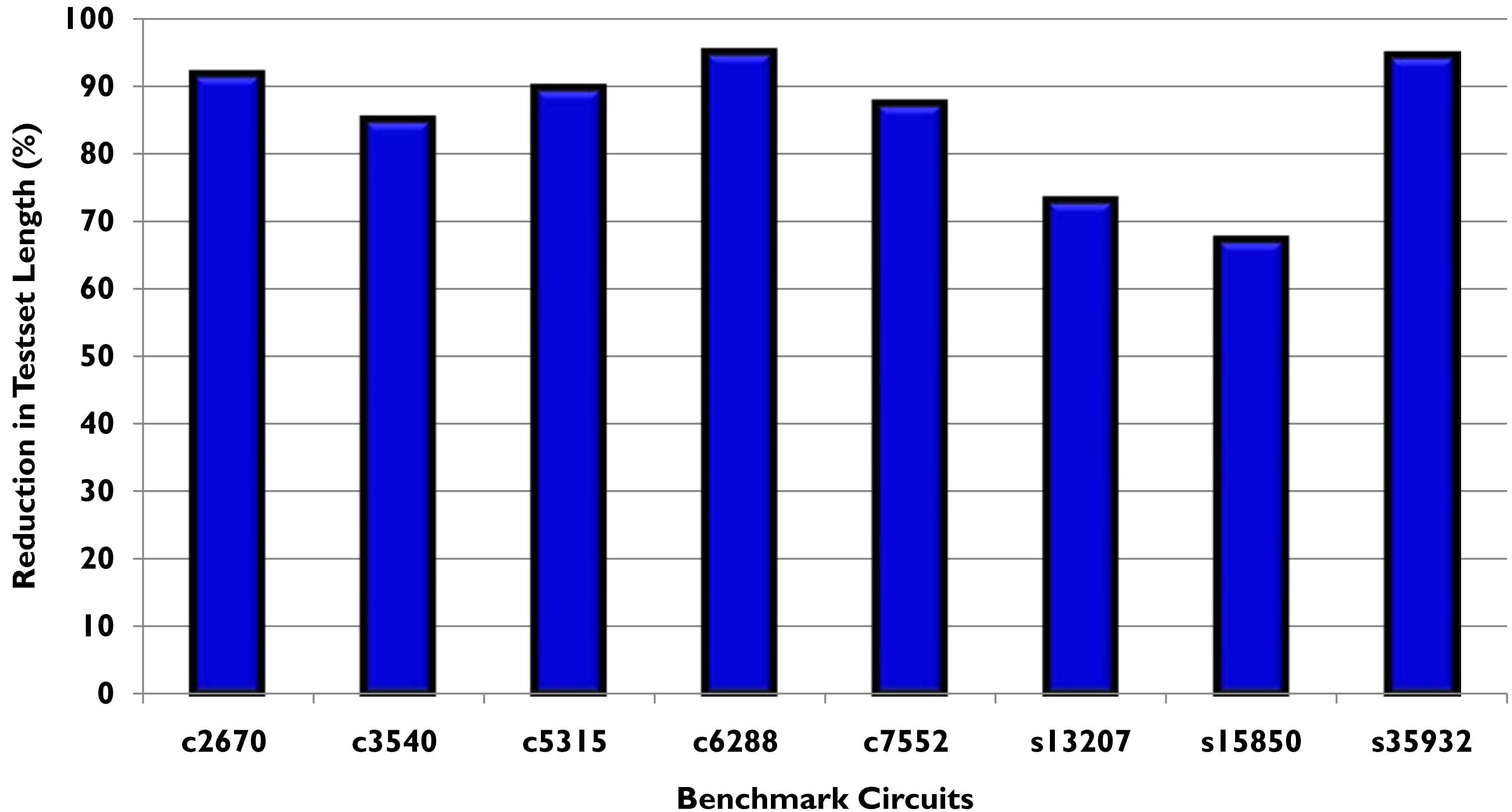
Trigger Coverage



Trojan Coverage

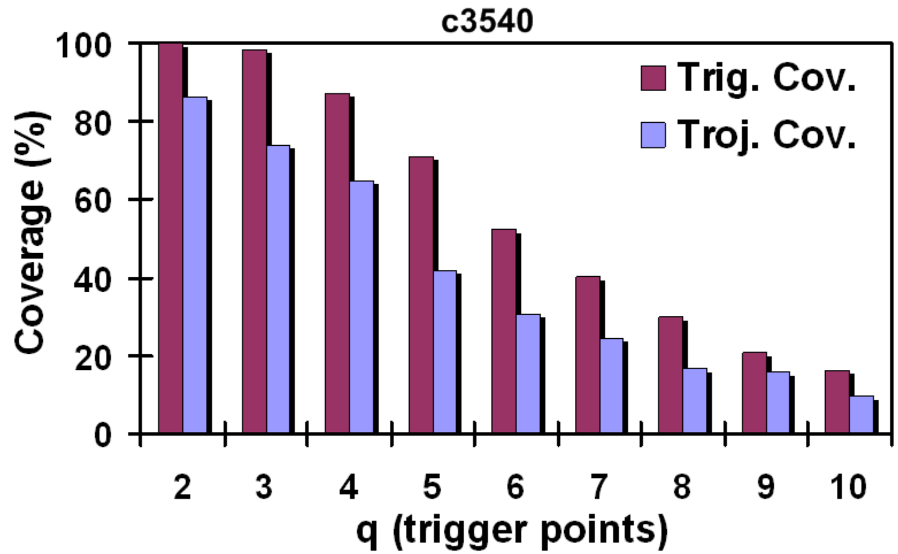
Trigger Coverage is inferior to Trojan Coverage!

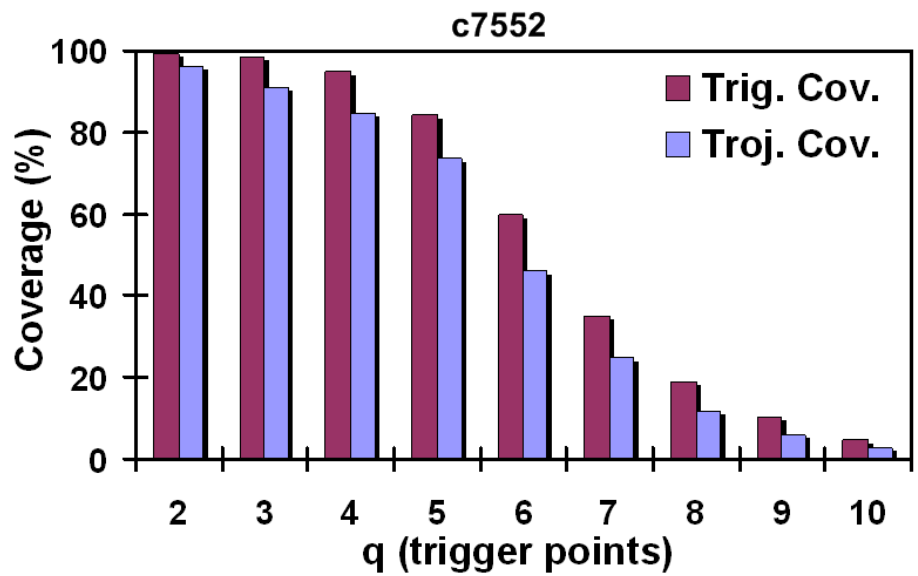
Simulation Results: Test Length



% Reduction in Test length compared to weighted random patterns (average: ~85%)

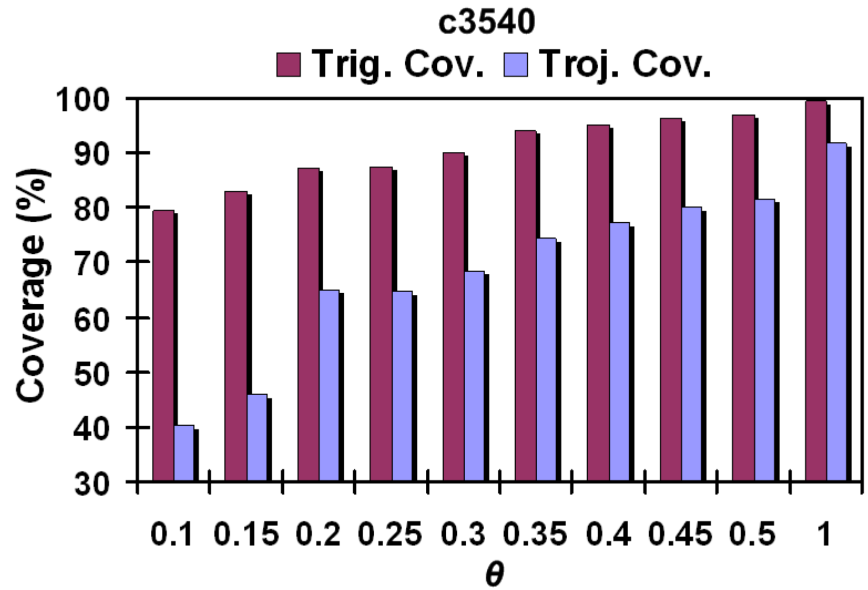
Simulation Results: Effect of *q*

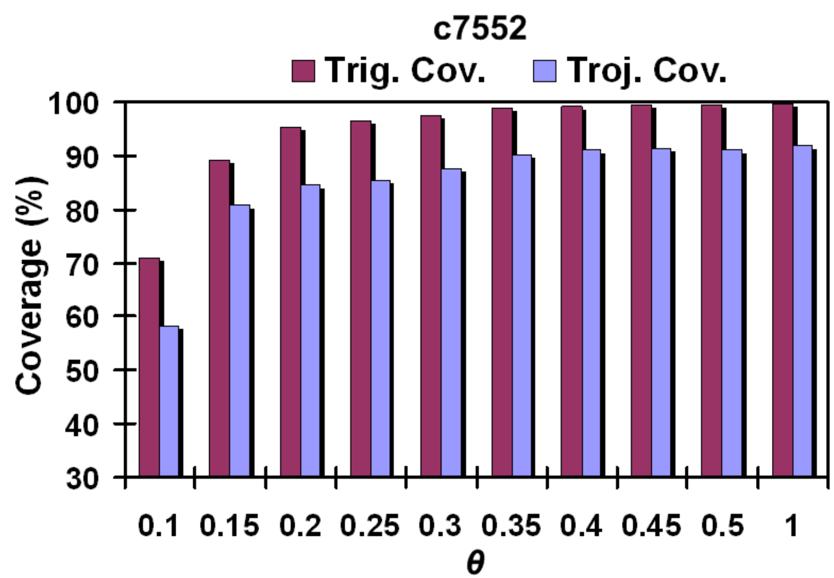




Coverage Decreases with *q*!

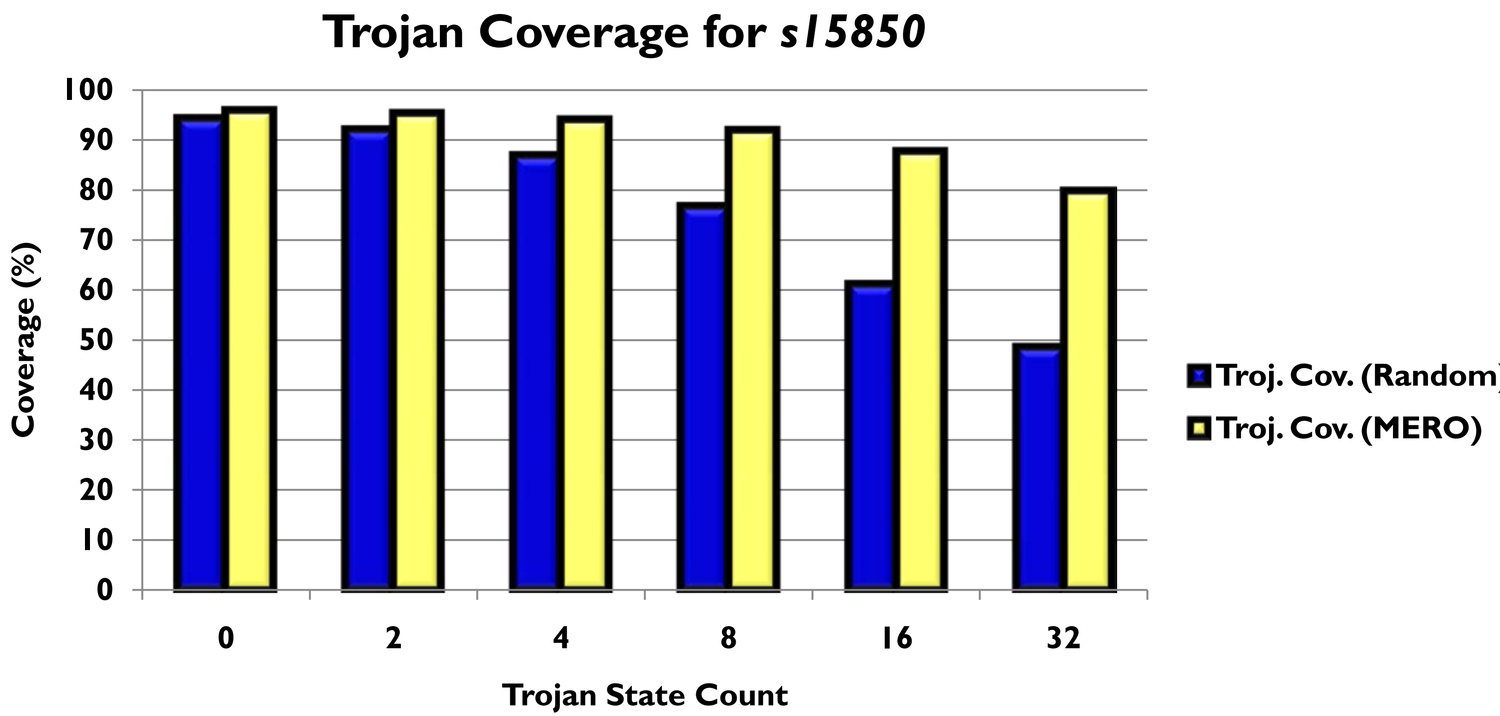
Simulation Results: Effect of ϑ





Coverage Improves with *θ*!

Sequential Trojan Coverage



- ***Counter-like Trojans triggered by internal node conditions (q = 2)***
- ***MERO patterns provide better coverage***
- ***Coverage Better for Smaller Trojans***

Conclusions

- **We have presented a *statistical approach* for hardware Trojan Detection**
  - **Provides superior coverage compared to random or ATPG vectors**
  - **~85% reduction in testset length**
  - **Effective for both *combinational* and *sequential* Trojans**
  - **High trigger coverage facilitates side-channel analysis**

- **Future Work**
  - ***Integration of logic testing and side-channel analysis in MERO framework***
  - **Blind testing**