IPTrust: Validation of IP Security and Trust

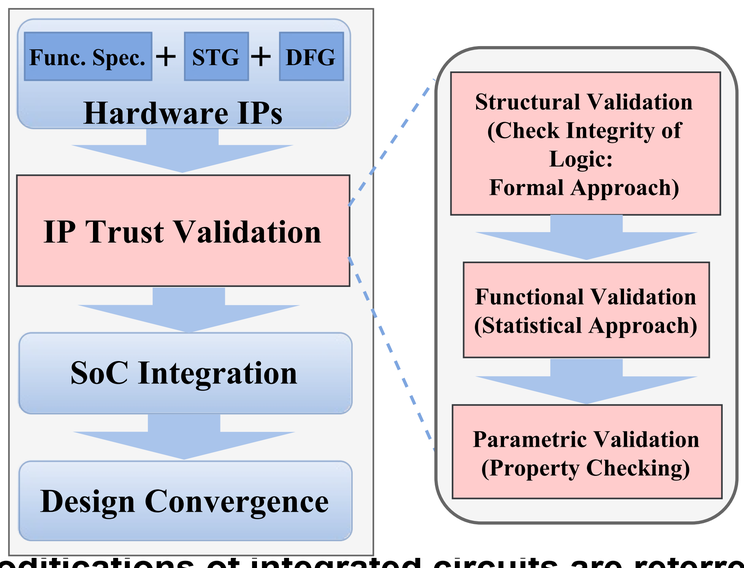
PIs: Prabhat Mishra and Swarup Bhunia, University of Florida

http://esl.cise.ufl.edu/trust.html

The purpose of the project includes:

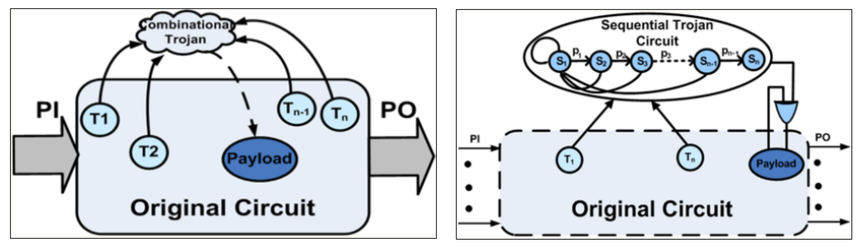
(1) to investigate diverse integrity and trust issues in hardware Intellectual Properties (IPs);

(2) to develop a scalable trust validation framework to verify IP trust and security from the perspective of functional, structural and parametric verification approaches.



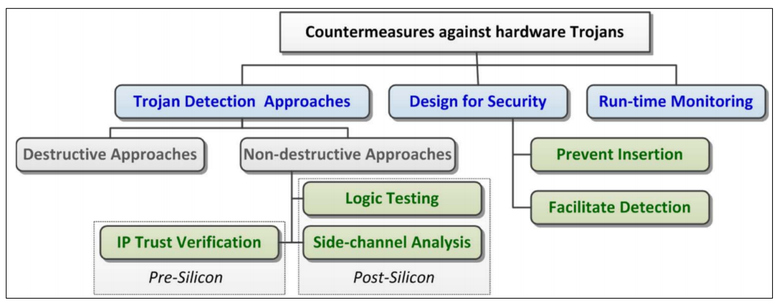
Malicious modifications of integrated circuits are referred as *Hardware Trojans.* **In an untrusted design or fabrication facility an adversary can alter the original design to:**

- **Change the functionality**
- **Leak secret information**
- **Disable the circuit**



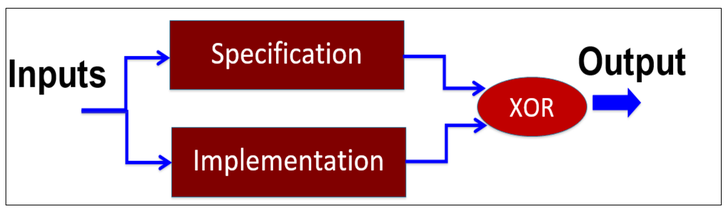
Model of combinational and sequential hardware Trojans

Existing countermeasures against hardware Trojans:



Security Validation using Symbolic Algebra

Traditional equivalence checking using SAT solver lead to state space explosion when Large IP blocks are involved.

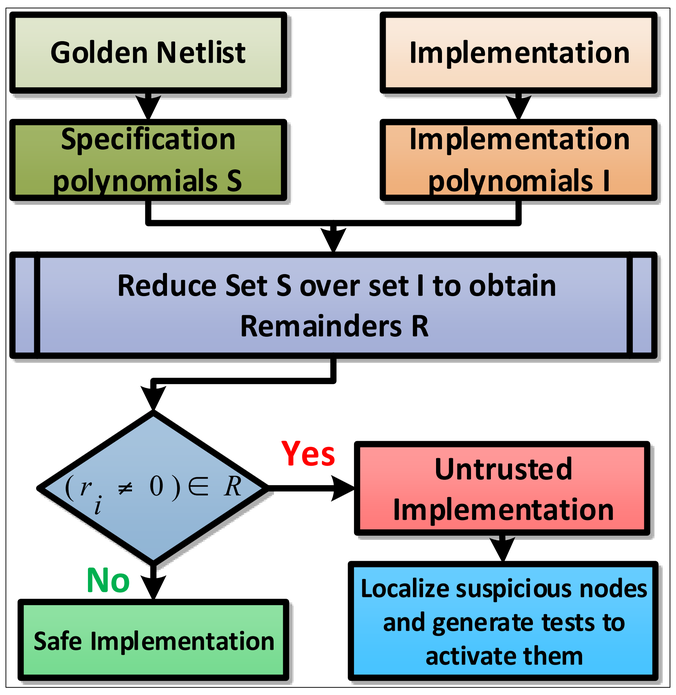


- **We propose a equivalence checking and Trojan localization method based on the Gröbner basis.**
- **Specification polynomials are obtained as:**

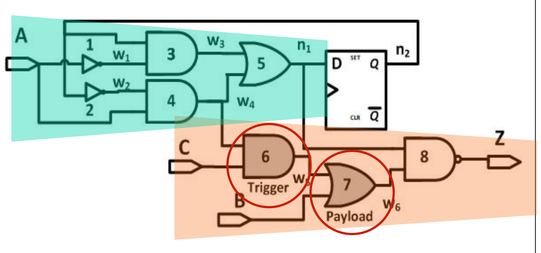
$$S=\{f_{spec\_1}, f_{spec\_2}, \ldots, f_{spec\_n}\}$$

- **Gate level circuit C converted to polynomials:**

$$F=\{f_{imp\_1}, f_{imp\_2}, \ldots, f_{imp\_s}\}$$



- **Specification polynomials**
  - f_{spec1}: $n_1 - (A+n_2-2*A*n_2)=0$
  - f_{spec2}: $Z - (n_1*B)=0$
- **Implementation polynomials**
  - f_{imp1}: $n_1 - (n_2*w_4*A - n_2*w_4 + w_4 - n_2*A)=0$
  - f_{imp2}: $w_4 - (A - n_2*A)=0$
  - f_{imp3}: $Z - (n_1*w_4*C*B - n_1*w_4*C - n_1*B+1)=0$



- **Trojan gates can be identified by analyzing remainder after reduction.**

Equivalence checking and Trojan localization

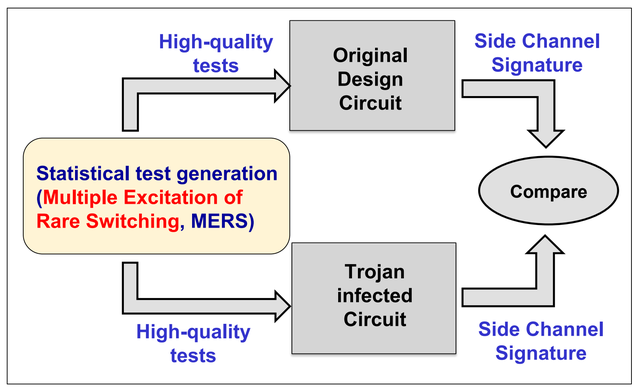
- **Each f_{spec} is reduced w.r.t Gröbner basis G**
- f_{spec} **can be reduced by** g_j**, if** $lm(g_j) | lm(f_{spec})$
- $r = f_{spec} - lt(f_{spec})/lt(g_j) \cdot g_j$ *or* $f_{spec} \rightarrow g_j + r$
- f_{spec} **can be reduced by set G**

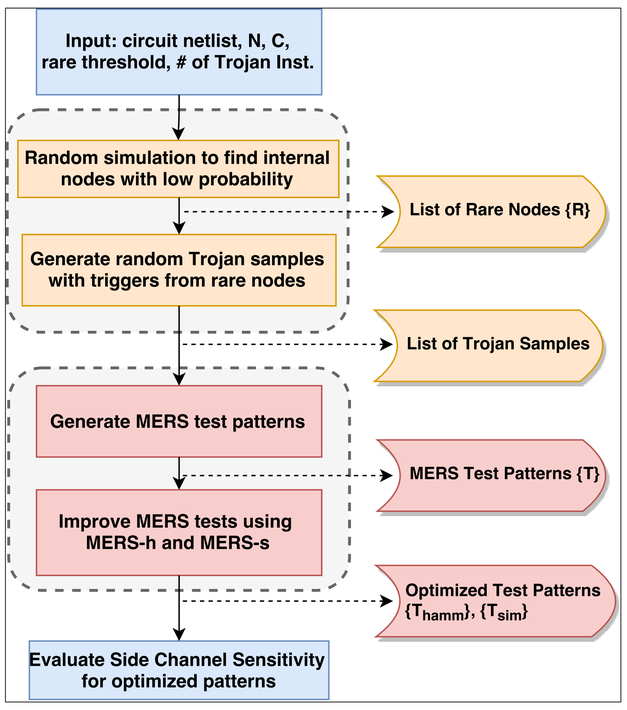
$f_{spec} \rightarrow G + r$

  - $r \neq 0 \rightarrow$ **security threat**
  - $r = 0 \rightarrow$ **the region is of safe functionality**

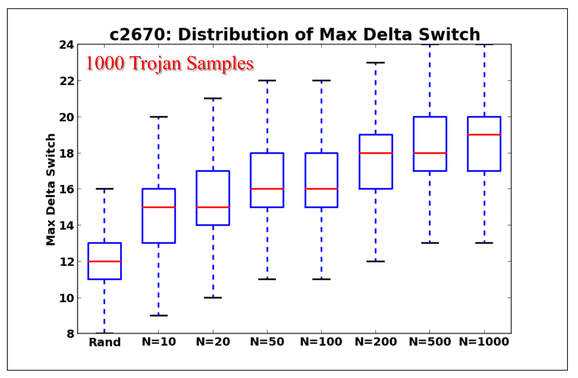
Side-Channel based Test Generation for Trojan Detection

- Existing approaches in two directions:
  - Test generation: Difficult to generate tests since Trojans are usually stealth.
  - Side-channel analysis: Sensitive to process noise for ultra-small Trojans.

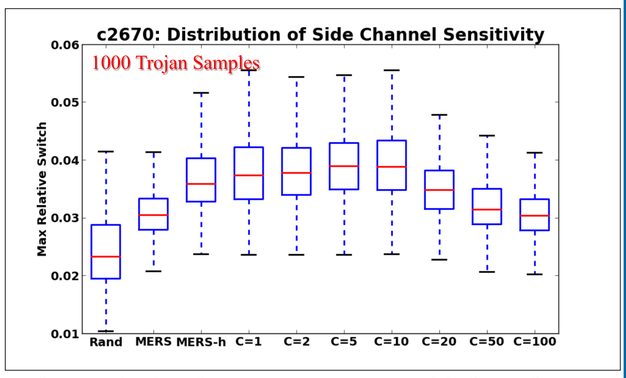




- Our statistical approach can improve the sensitivity of side-channel based Trojan detection, by generating high-quality tests.
- *MERS* (*Multiple Excitation of Rare Switching*) aims at generating high-quality tests for each rare node to switch for at least N times.
- MERS maximizes the activation probability for arbitrary Trojans with any trigger condition.
- MERS maximizes the detection sensitivity of unknown "stealthy" Trojans, by amplifying its effect in side-channel signature.
- Our simulation platform inserts large number of arbitrary Trojans in a design and shows that the proposed approach is highly effective in detecting them.



Trojan activity increases as N increases, which shows the effectiveness of MERS in creating switching in Trojans.



The optimized test patterns MERS-h and MERS-s (with weight C=1~10) can further increase the side channel sensitivity.

[1] Farimah Farahmandi and Prabhat Mishra, Automated Test Generation for Debugging Arithmetic Circuits, (DATE) 2016.
[2] Farimah Farahmandi, Yuanwen Huang and Prabhat Mishra, Trojan Localization using Symbolic Algebra, (ASPDAC) 2017.
[3] Yuanwen Huang, Swarup Bhunia and Prabhat Mishra, MERS: Statistical Test Generation for Side-Channel Analysis based Trojan Detection, CCS 2016.