DIMINISH: Detection and Isolation of Malicious Inclusions in Secure Hardware

Mohammad Tehranipoor and Jim Plusquellic (www.engr.uconn.edu/~tehrani) (www.csee.umbc.edu/~plusquel)

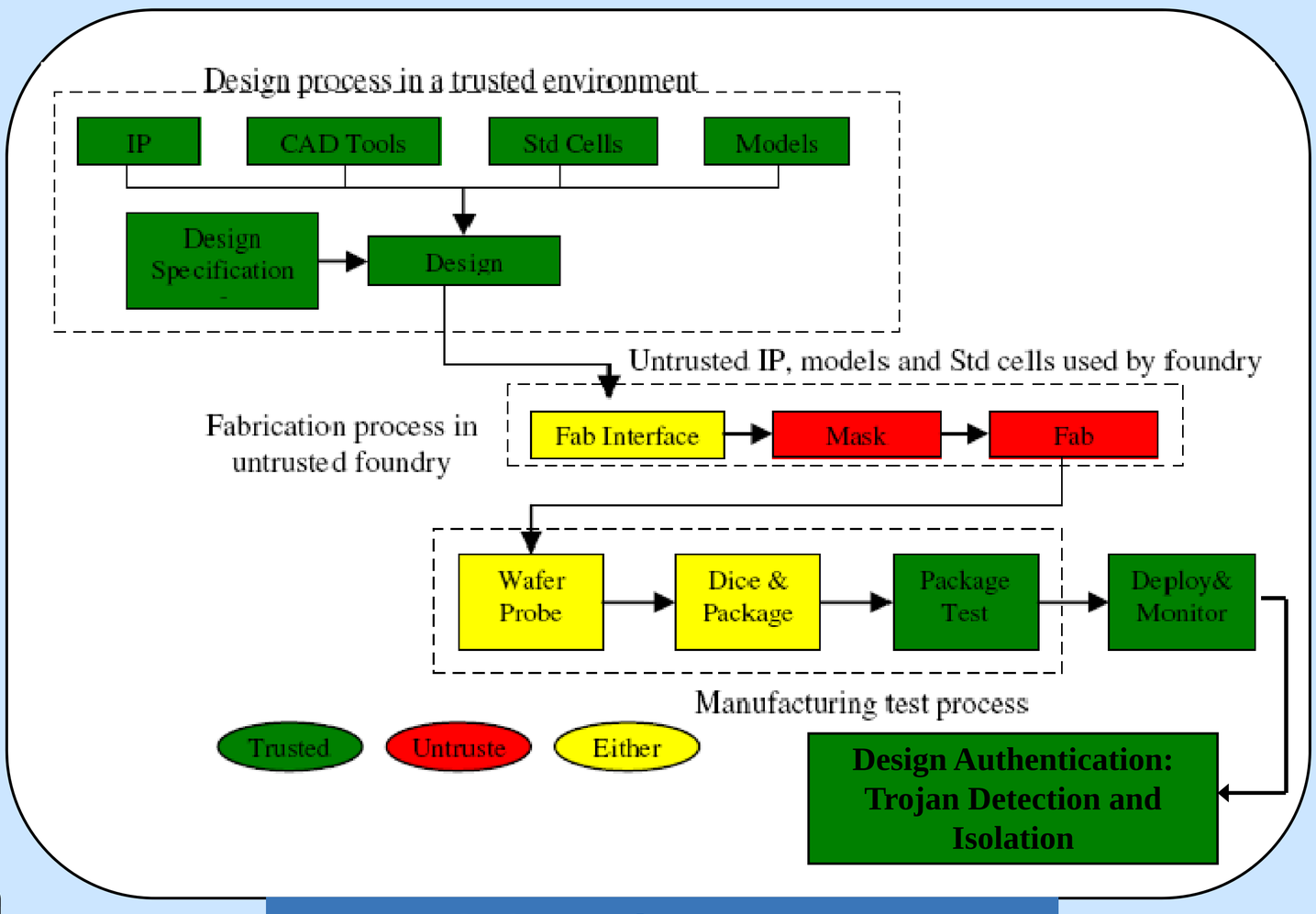
NSF Grant CNS-0716535 and 0716559

Problem:

Chip design and fabrication is becoming increasingly vulnerable to malicious activities and alterations with globalization. An adversary can introduce a Trojan designed to disable and/or destroy a system at some future time or the Trojan may serve to leak confidential information covertly to the adversary.

Approach:

1. Taxonomy of Trojans
2. Power/Current Analysis
3. IDDQ Pattern Generation
4. Delay Analysis
5. Novel Delay Pattern Generation
   - Hard-to-detect Inclusions
   - Small Delay Inclusions
6. Silicon Data Collection
   - Trojan Detection & Localization



ASIC Design Process

Approach and Impact

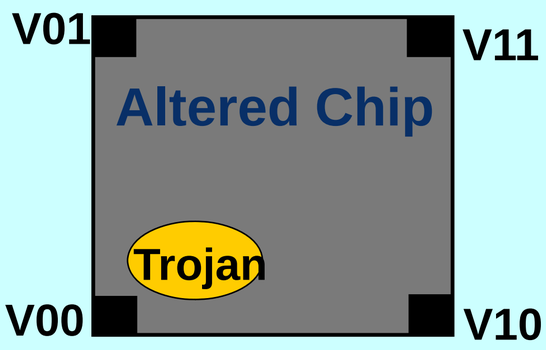
New approach:

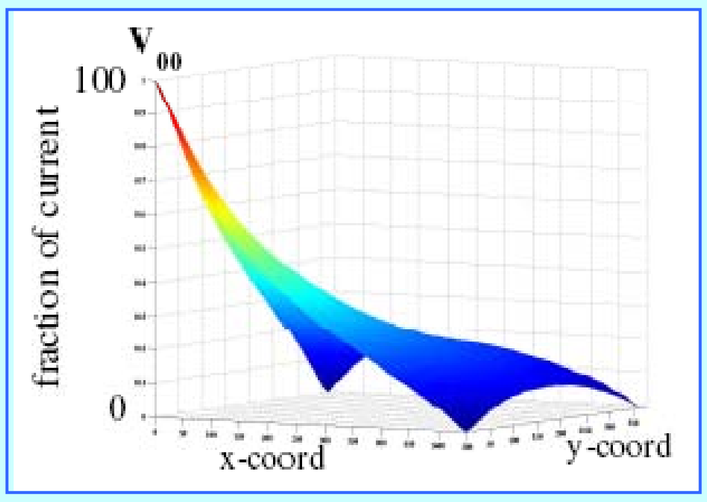
- Detecting and localizing Trojans
- Multiple power supply analysis
- Novel delay trace analysis

Research Impact:

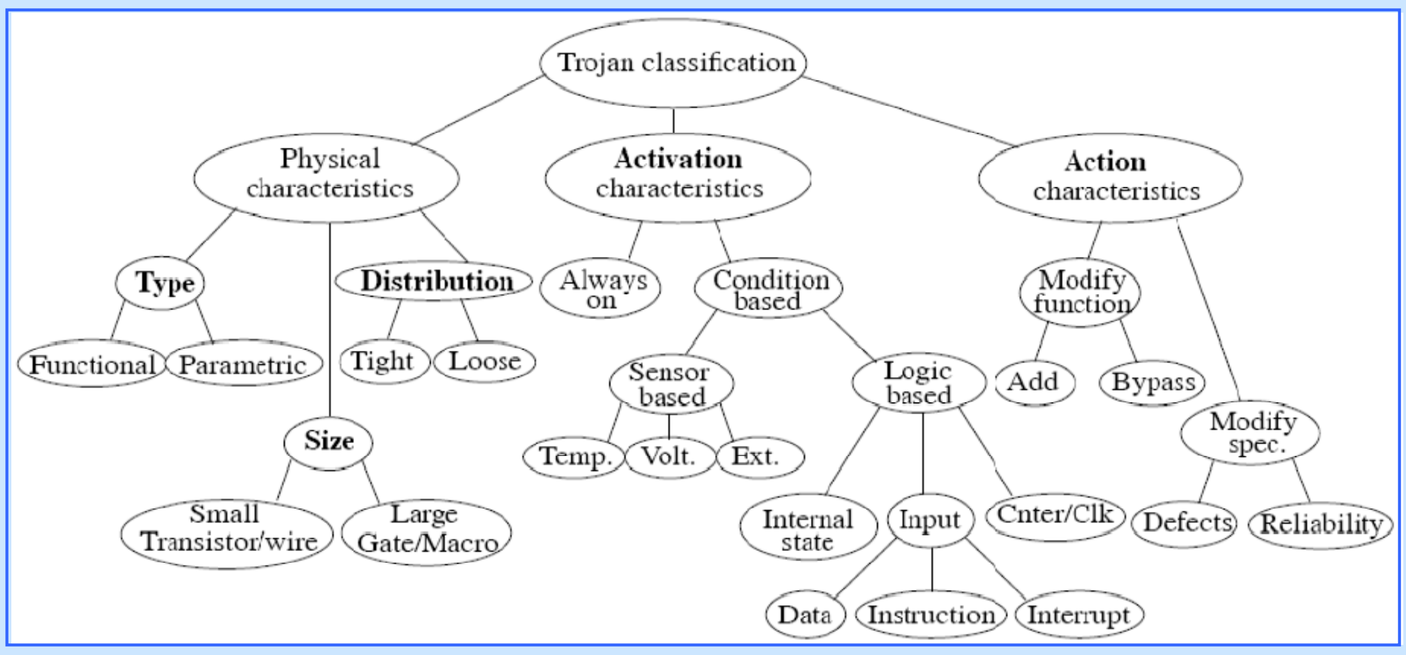
- Improve trustworthiness of chips
- Improve manufacturing testing
- Improve software-based diagnosis

Power/Current Analysis



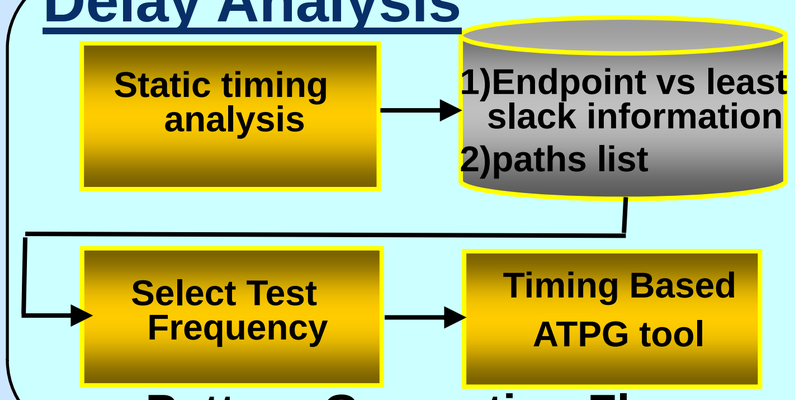


Calibrated and normalized current from V00

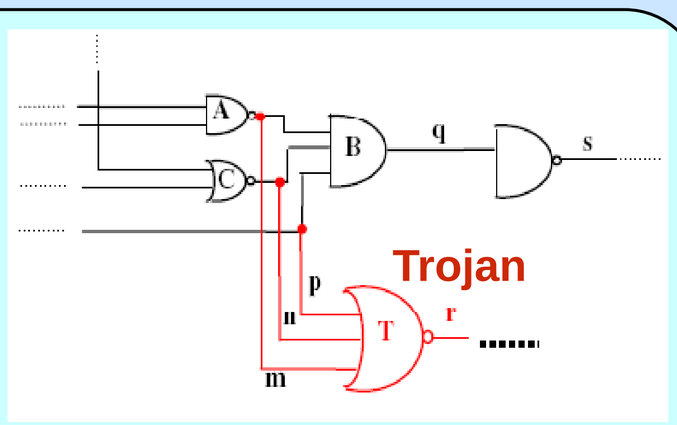


Taxonomy of Trojans

Delay Analysis



Pattern Generation Flow



Circuit with Trojan

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

UNIVERSITY OF CONNECTICUT 1881