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

Approach and Impact
New approach: Research Impact:
• Detecting and localizing Trojans
• Improve trustworthiness of chips
• Multiple power supply analysis
• Improve manufacturing testing
• Novel delay trace analysis
• Improve software-based diagnosis

Power/Current Analysis
Calibrated and normalized current from V00

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