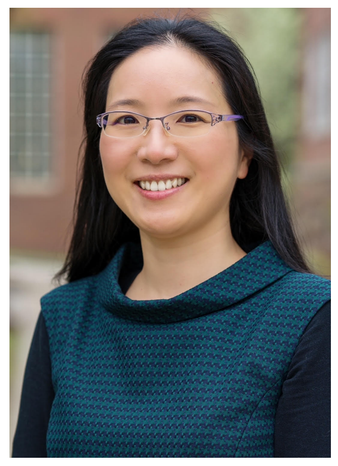
CAREER: Proactive Defense Methods for Chip Integrity and Security



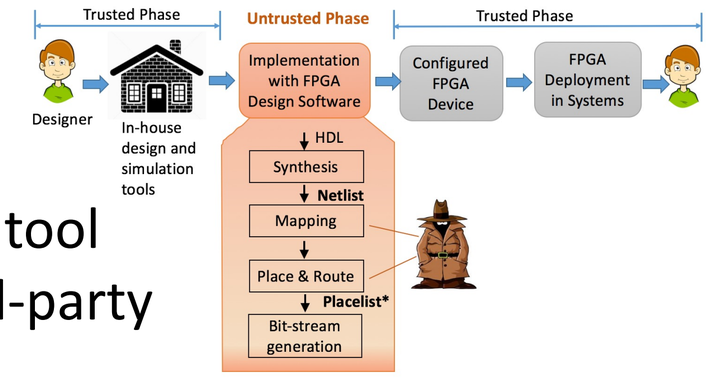
Qiaoyan Yu, University of New Hampshire

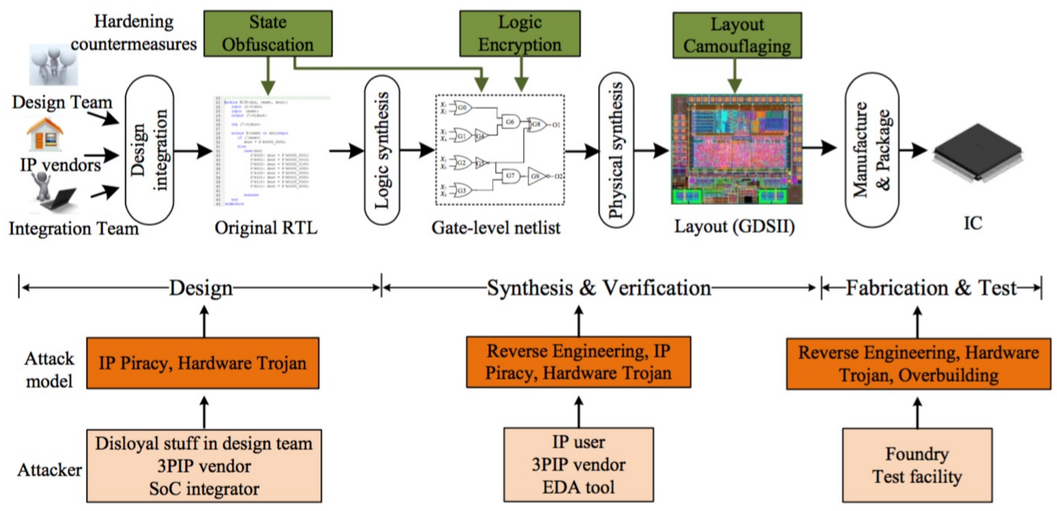
https://mypages.unh.edu/qyu/research

Motivation and Background

Security concerns

- Untrusted manufacturing
- Untrusted EDA tool
- Untrusted third-party hard/soft IPs





Challenges

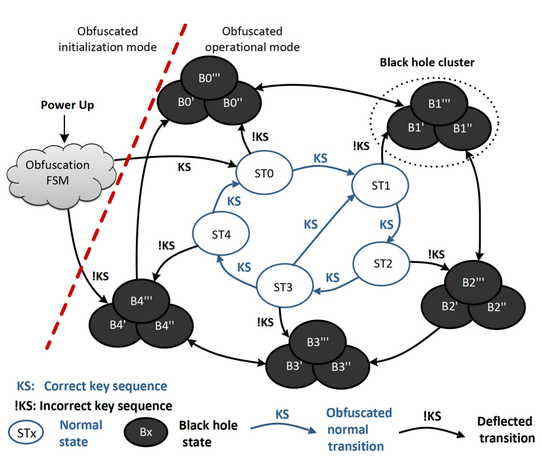
- Hardware cannot be patched like software if a security vulnerability is identified
- A countermeasure should have self-defensive capabilities
- Multiple existing attack methods can be combined into an advanced attack

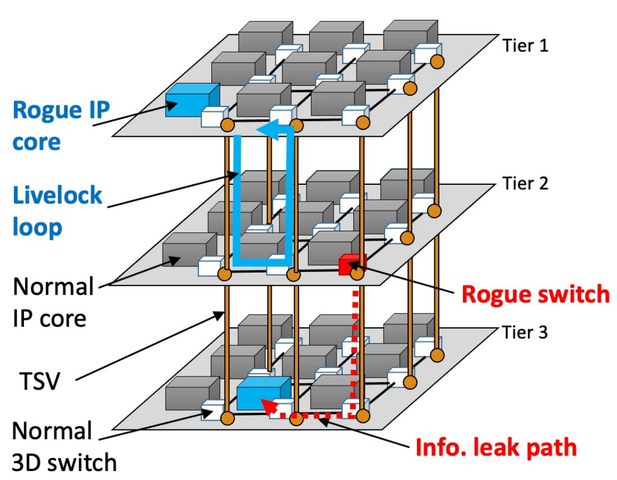
Scientific Impact

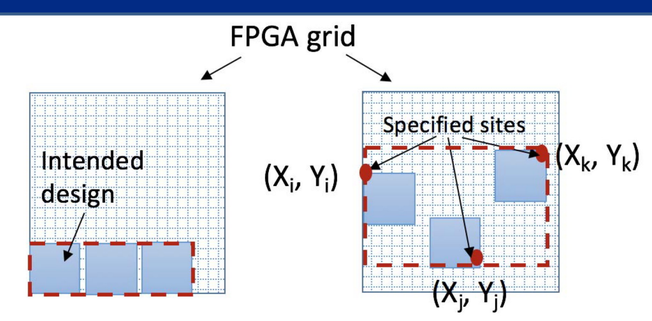
- The obfuscated system resists an attack that exploits the advanced tools to analyze the IP netlist and primary outputs
- The proposed method particularly considers the cross influence among countermeasures for different attacks
- Hardware reconfiguration is leveraged to address emerging attacks on FPGAs

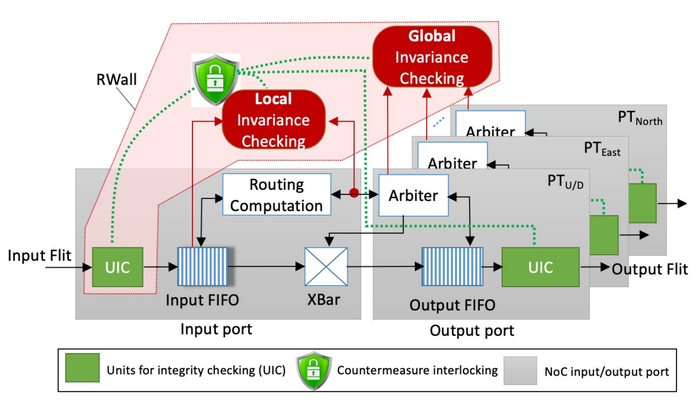
Key Contributions

- Dynamically deflective hardware obfuscation
- On-chip interconnect network dynamic hardening
- Moving-target-defense (MTD) based obfuscation for FPGAs









Broader Impact

- Project outcomes will facilitate the implementation of trustworthy chips for both mission-critical and commercial applications
- The PI used Snap Circuits to develop teaching modules for grades 2-5 students in the UNH KEEPERS program to attract young students to the field of ECE
- The PI organized Workshop for Women in hardware and Systems Security (WISE)