UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Behavioral and RT-level Synthesis of Secure Nano VLSI Digital ASIC Designs

by

Sheikh Ariful Islam

For the Ph.D. degree in Computer Science and Engineering

The tremendous computing capabilities of the modern nanometer-scale Integrated Circuit (IC) have fueled the "silicon" age revolution. However, the complexity of IC design changed the landscape of the globalized electronics supply-chain into horizontal business model. Unfortunately, due to the involvement of multiple parties, IC supply-chain has led to several exploits including IC subversion. Hence, it is important to integrate security mechanisms inexpensively and efficiently during the early stage of IC design. We will present two defense-via-synthesis techniques and an analytical framework to improve hardware security assuming the potential capabilities of an attacker. First, we will discuss Register Transfer Level (RTL) obfuscation mechanism during behavioral synthesis. We embed multiplexers on non-critical paths for obfuscated RTL design followed by design lockout and camouflaging. This technique hardens the RTL IP against Reverse Engineering to a great extent. Second, we present an analytical estimation framework to localize Hardware Trojan (HT) in RTL design. We characterize arithmetic module architectures and propagate them during technology mapping to identify suitable modules of least rare triggering and better design parameters. Third, we design monitor to capture original RTL controller behavior and prevent code-injection and code-reuse attacks via Control-Flow Integrity (CFI).

Examining Committee

Wilfrido A. Moreno, Ph.D., Chairperson
Srinivas Katkoori, Ph.D., Major Professor
Sriram Chellappan, Ph.D.
Xinming (Simon) Ou, Ph.D.
Hao Zheng, Ph.D.
Sanjukta Bhanja, Ph.D.
Kaiqi Xiong, Ph.D.

Thursday, April 23, 2020
9:00 AM
Online (Microsoft Teams)
Email sheikhariful@mail.usf.edu for more information

THE PUBLIC IS INVITED

Publications

1) **S. A. Islam**, L. K. Sah, and S. Katkoori, "High-Level Synthesis of Key Obfuscated RTL IP with Design Lockout and Camouflaging," in *ACM Trans. on Design Automation of Electronic Systems* (Second round, Major Revision).
2) **S. A. Islam**, L. K. Sah, and S. Katkoori, "A Framework for Hardware Trojan Vulnerability Estimation and Localization in RTL Designs," in *Journal of Hardware and Systems Security* (Accepted).
3) **S. A. Islam** and S. Katkoori, "High-level synthesis of key based obfuscated RTL datapaths," in *Proc. 19th International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, CA, 2018, pp. 407-412.
4) **S. A. Islam**, L. K. Sah, and S. Katkoori, "Empirical Word-Level Analysis of Arithmetic Module Architectures for Hardware Trojan Susceptibility," in *Proc. Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, Hong Kong, 2018, pp. 109-114.
5) **S. A. Islam**, L. K. Sah, and S. Katkoori, "DLockout: A Design Lockout Technique for Key Obfuscated RTL IP Designs," in *Proc. IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS),* Rourkela, 2019, pp. 17-20.
6) **S. A. Islam**, L. K. Sah, and S. Katkoori, "Analytical Estimation and Localization of Hardware Trojan Vulnerability in RTL Designs," in *Proc. International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, 2020, pp --.
7) **S. A. Islam** and S. Katkoori, "SafeController: Efficient and Transparent Control-Flow Integrity for RTL Design," in *Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI),* Cyprus, 2020 (Under Review).

Robert Bishop, Ph.D.
Dean, College of Engineering

Dwayne Smith, Ph.D.
Dean, Office of Graduate Studies

Disability Accommodations:
If you require a reasonable accommodation to participate, please contact the Office of Diversity & Equal Opportunity at 813-974-4373 at least five (5) working days prior to the event.