UNIVERSITY OF SOUTH FLORIDA

Defense of a Doctoral Dissertation

Secure VLSI Hardware Design Against Intellectual Property (IP) Theft and Cryptographic Vulnerabilities

by

Matthew Dean Lewandowski

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

Over the last two decades or so, VLSI hardware is increasingly subject to sophisticated attacks on both the supply chain and design fronts. There is no explicit trust that the manufacturers/providers are not producing counterfeit designs or that cryptographic algorithms we know to be secure in software are also secure in hardware. The novelty and key contributions of this work are as follows: 1) a continually refined method for Intellectual Property (IP) Protection that provides an approach for verification of IP ownership, 2) demonstrate how to break the PRESENT-80 cryptographic algorithm with significantly limited resources, and 3) provide a multitude of hardware based countermeasures to counter such attacks. First, in order to thwart intellectual property theft, the proposed state encoding based watermarking method and the mapping algorithm outperforms the prior techniques. We propose a hybrid genetic algorithm, dubbed the Darwinian Genetic Algorithm, for efficiently solving the difficult sub-graph matching problem. As a result, we outperformed prior work maximally 20-30% and on average 1-12% when considering the post-synthesis watermarked designs in terms of literals, area, and delay. Second, we demonstrate for the first time ever how the lightweight cryptographic algorithm PRESENT-80 can be broken via a Differential Plaintext Attack with significantly limited resources. Lastly, to prevent such attacks, we present a series of countermeasures to not only PRESENT-80, but for all substitution-permutation network ciphers, by inducing non-static behavior. We novel interconnection network primitives, dynamic routing networks, and ultimately modify round invariant items to round based variants that necessitate decision making for an attacker.

Examining Committee
Ismail Uysal, Ph.D., Chairperson
Srinivas Katkoori, Ph.D., Major Professor
Jay Ligatti, Ph.D.
Swaroop Ghosh, Ph.D.
Andrew Hoff, Ph.D.
Brendan Nagle, Ph.D.

Monday, June 21, 2021
12:00-2:00PM
Online (Microsoft Teams)
Please email for more information
mlewando@usf.edu
THE PUBLIC IS INVITED

Publications

1) **M. Lewandowski** and S. Katkoori, "A Darwinian Genetic Algorithm for State Encoding Based Finite State Machine Watermarking," 20th International Symposium on Quality Electronic Design (ISQED), 2019, pp. 210-215, doi: 10.1109/ISQED.2019.8697760.
2) **M. Lewandowski** and S. Katkoori "Lightweight Countermeasure to Differential-Plaintext Attacks on Permutation Ciphers," In: Casaca A., Katkoori S., Ray S., Strous L. (eds) Internet of Things. A Confluence of Many Disciplines. IFIPIoT 2019. IFIP Advances in Information and Communication Technology, vol 574. Springer, Cham. https://doi-org.ezproxy.lib.usf.edu/10.1007/978-3-030-43605-6_10
3) **M. Lewandowski** and S. Katkoori, "State Encoding Based Watermarking of Sequential Circuits using Genetic Algorithm, Behavioral Synthesis for Hardware Security," Book Chapter, In: S. Katkoori and S. A. Islam, *Behavioral Synthesis for Hardware Security,* Springer Nature Switzerland, To Appear
4) **M. Lewandowski** and S. Katkoori, "Enhancing PRESENT-80 and Substitution-Permutation Network Cipher Security with Dynamic "Keyed" Permutation Networks," IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2021, To Appear
5) **M. Lewandowski**, R. Meana, M. Morrison and S. Katkoori, "A novel method for watermarking sequential circuits," 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, 2012, pp. 21-24, doi: 10.1109/HST.2012.6224313.
6) **M. Lewandowski** and S. Katkoori, "Watermarking of Sequential Circuits using Genetic Algorithm based Search for Isomorphic Signature Subgraphs," Florida Institute for Cybersecurity (FICS) Research Conference, Mar. 2017
7) **M. Lewandowski** and S. Katkoori, "A Genetic Algorithm for Watermarking Sequential Circuits," University of South Florida 10th Annual Graduate Research Symposium, Mar. 2018

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.