Provenance Attestation: From Silicon Chips to Biological Cells and Beyond

Yiorgos Makris
Professor
The University of Texas at Dallas

Monday, April 8, 2024
10:30 AM • MSEE 112

Abstract Complex processes, whether natural or artificial, often exhibit inherent variability and result in slightly different products even when identical steps, equipment, materials and conditions are employed. Such variability typically consists of a random component, which is attributed to the endogenous stochasticity of the process itself, and a systematic component, which is attributed to the exogenous aspects of the production. In this presentation, we will discuss how this variability can be harnessed for the purpose of attesting both the process and each copy of the product, thereby facilitating trust, traceability and intellectual property protection. First, in the context of semiconductor manufacturing, using both physical and electrical measurements (a.k.a., metrology and wafer acceptance tests, respectively) from wafers manufactured using multiple copies of a mask-set in a 12nm GlobalFoundries technology, we will demonstrate the use of contemporary statistical and machine learning-based methods for determining whether a wafer was produced by a ratified mask-set. Leveraging the insight gained through this analysis, we will also discuss the design of custom sensors for obtaining the relevant information from each die on a wafer to collectively attest the mask-set used to produce this wafer, without relying on potentially untrusted foundry-provided data. Then, in the context of synthetic biology, using amplicon sequencing data from multiple cell lines (i.e., HEK293, HCT116 and HeLa), we will demonstrate that the stochasticity of the non-homologous end-joining (NHEJ) DNA repair process can be leveraged as a mechanism for introducing a unique identifier (i.e., a Genetic Physical Unclonable Function (PUF)) in every legitimately produced copy of a cell line. Akin to their counterparts in the semiconductor industry, Genetic PUFs can be used for attesting the provenance and protecting the intellectual property of valuable, genetically-engineered cell lines.

Bio Yiorgos Makris received the Diploma of Computer Engineering from the University of Patras, Greece, in 1995 and the M.S. and Ph.D. degrees in Computer Engineering from the University of California, San Diego, in 1998 and 2001, respectively. After spending a decade on the faculty of Yale University, he joined UT Dallas where he is now a Professor of Electrical and Computer Engineering, the Co-Founder and Site-PI of the NSF Industry University Cooperative Research Center on Hardware and Embedded System Security and Trust (NSF CHEST I/UCRC), as well as the Leader of the Safety, Security and Healthcare Thrust of the Texas Analog Center of Excellence (TxACE) and the Director of the Trusted and RELiable Architectures (TRELA) Research Laboratory. His research focuses on applications of machine learning and statistical analysis in the development of trusted and reliable integrated circuits and systems. He has served as an Associate Editor of the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, the IEEE Transactions on Information Forensics and Security and the IEEE Design & Test of Computers Periodical, and as a guest editor for the IEEE Transactions on Computers and the IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. He has also served as the 2016-2017 General Chair and the 2013-2014 Program Chair of the IEEE VLSI Test Symposium. He is a recipient of the 2006 Sheffield Distinguished Teaching Award, Best Paper Awards from the 2013 IEEE/ACM Design Automation and Test in Europe (DATE'13) conference and the 2015 IEEE VLSI Test Symposium (VTS'15), as well as Best Hardware Demonstration Awards from the 2016 and the 2018 IEEE Hardware-Oriented Security and Trust Symposia (HOST'16 and HOST'18) and a recipient of the 2020 Faculty Research Award from the Erik Jonsson School of Engineering and Computer Science at UT Dallas.

Host Professor Shreyas Sen, Shreyas@purdue.edu, 765-496-6520

PURDUE UNIVERSITY | Elmore Family School of Electrical and Computer Engineering