Aggressive Design Reuse for Ubiquitous and Hardware-Patchable Silicon Chip Security – From Physical Sensing and Design to On-Chip Machine Learning

SPEAKER:

Prof. Massimo Alioto, Ph.D.

ECE - National University of Singapore

E-mail: *massimo.alioto@nus.edu.sg*, *malioto@ieee.org*

Homepage: *http://www.green-ic.org/*

ABSTRACT: Divide-and-conquer design methodologies facilitate building block design, but conflict with basic security requirements, while also precluding opportunities for efficient system integration and inexpensive embedment of security features. At the same time, the insertion of security primitives as standalone blocks is inherently additive in terms of area, power, design effort and integration effort, limiting their embeddability in low-cost devices (i.e., the vast majority of the upcoming trillion chips for the Internet of Things). As further limitation of conventional approaches to security enforcement in silicon chips (e.g., against side-chanel attacks), the discovery of hardware vulnerabilities cannot be followed by later hardware fixes as we are used to do with software systems, given the inherently rigid nature of systems on chip after manufacturing.

In this keynote, the road towards ubiquitous hardware security is pursued from a primitive design perspective, designing roots of trust (e.g., PUFs, TRNGs) that are inherently immersed in existing memory arrays and logic fabrics, and breaking the boundaries of traditional system partitioning. Ultra-low cost primitives for on-chip distributed physical sensors are also discussed to counteract physical attacks from side-channel to laser voltage probing attacks. In this talk, the new concept of hardware patching is also discussed, where circuit flexibility is introduced to make silicon chips able to evolve over time and counteract newly discovered vulnerabilities through learning based physical protection mechanisms.

To exemplify the above concepts and the resulting technological advances, several silicon demonstrations are illustrated to quantify the benefits and the limits of conventional techniques, and identify opportunities and challenges for the decade ahead. At the end of the keynote, fundamental directions on how to make hardware security more pervasive, unceasing and intelligent are discussed.

BIO: Massimo Alioto is a Professor at the ECE Department of the National University of Singapore, where he leads the Green IC group, the Integrated Circuits and Embedded Systems area, and the FD-fAbrICS center on intelligent&connected systems. Previously, he held positions at the University of Siena, Intel Labs – CRL (2013), University of Michigan - Ann Arbor (2011-2012), University of California – Berkeley (2009-2011), EPFL - Lausanne.

He is (co)author of 350+ publications on journals and conference proceedings, and six books with Springer. His primary research interests include ultra-low power and self-powered systems, green computing, circuits for machine intelligence, hardware security, and emerging technologies.

He is the Editor in Chief of the IEEE Transactions on VLSI Systems, and he is/was Distinguished Lecturer for the IEEE Circuits and Systems and the Solid-State Circuits Society. He is also the Chair Elect of the Distinguished Lecturer Program for the IEEE CAS Society, and was the Deputy Editor in Chief of the IEEE

Journal on Emerging and Selected Topics in Circuits and Systems. Previously, Prof. Alioto was the Chair of the “VLSI Systems and Applications” Technical Committee of the IEEE Circuits and Systems Society (2010-2012), and member of the Board of Governors (2015-2020). He served as Guest Editor of numerous journal special issues (e.g., JSSC, TCAS-I, TCAS-II, JETCAS, Technical Program Chair of several IEEE conferences (e.g., ISCAS, SOCC, PRIME, ICECS), and TPC member (ISSCC, ASSCC). Prof. Alioto is an IEEE Fellow.