UCF DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

Fall 2016 Seminar Series

Cryptoleq: A Heterogeneous Abstract Machine for Encrypted and Unencrypted Computation

MONDAY November 7, 2016

2:00 PM – HEC 450

The rapid expansion and increased popularity of cloud computing comes with no shortage of privacy concerns about outsourcing computation to semi-trusted parties. Leveraging the power of encryption, this presentation introduces Cryptoleq: an abstract machine based on the concept of One Instruction Set Computer, capable of performing general-purpose computation on encrypted programs. The program operands are protected using the Paillier partially homomorphic cryptosystem, which supports addition on the encrypted domain. Full homomorphism over addition and multiplication, which is necessary for enabling general-purpose computation, is achieved by inventing a software re-encryption module written using Cryptoleq instructions and blended into the executing program. Cryptoleq is heterogeneous, allowing mixing encrypted and unencrypted instruction operands in the same program memory space. Programming with Cryptoleq is facilitated using an enhanced assembly language that allows development of any advanced algorithm on encrypted datasets. As a case study, the performance of a typical Private Information Retrieval problem

Michail Maniatakos

New York University

Michail (Mihalis) Maniatakos is an Assistant Professor of Electrical and Computer Engineering at New York University (NYU) Abu Dhabi, UAE, and a Research Assistant Professor at the NYU Tandon School of Engineering, New York, USA. He is the Director of the MoMA Laboratory (nyuad.nyu.edu/momalab), NYU Abu Dhabi. He received his Ph.D. in Electrical Engineering, as well as M.Sc., M.Phil. degrees from Yale University. He also received the B.Sc. and M.Sc. degrees in Computer Science and Embedded Systems, respectively, from the University of Piraeus, Greece. His research interests, funded by industrial partners and the US government, include robust microprocessor architectures, privacy-preserving computation, as well as industrial control systems security. He has authored several publications in IEEE transactions and conferences, holds patents on privacy-preserving data processing, and he is currently the faculty lead for the Embedded Security challenge held yearly at CSAW, Brooklyn, NY.

Host: Dr. Yier Jin