In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Homomorphic Secret Sharing for Low Degree Polynomials

by

Mr. Giulio Malavolta

Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany

Date : 28th November, 2018 (Wed)

Time : 2:30pm – 3:00pm

Venue : Room 833, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

Homomorphic secret sharing (HSS) allows n clients to secret-share data to m servers, who can then homomorphically evaluate public functions over the shares. A natural application is outsourced computation over private data. In this work, we present the first plain-model homomorphic secret sharing scheme that supports the evaluation of polynomials with degree higher than 2. Our construction relies on any degree-k (multi-key) homomorphic encryption scheme and can evaluate degree-$((k+1)m - 1)$ polynomials, for any polynomial number of inputs n and any sub-logarithmic (in the security parameter) number of servers m. At the heart of our work is a series of combinatorial arguments on how a polynomial can be split into several low-degree polynomials over the shares of the inputs, which we believe is of independent interest.

Biography

Giulio Malavolta was born in Bologna and obtain his MSc at Saarland University in 2016. He is a PhD student at Friedrich-Alexander University Erlangen-Nuremberg. He is broadly interested in theoretical and applied aspects of public-key cryptography.

Remark: The visit is supported by Germany/Hong Kong Joint Research Scheme G-CUHK406/17.

**** ALL ARE WELCOME ****

Host: Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)

Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)