Brief Introduction to Zero-Knowledge Proofs with Applications to Privacy Preserving Distributed Ledgers

Dr Kamil Krzysztof Kluczniak
Postdoctoral Fellow
Department of Computing
The Hong Kong Polytechnic University
Hong Kong

Date : 29 June 2018 (Friday)
Time : 11:00 a.m. – 12:00 noon
Venue : Room PQ703, 7/Floor, PQ Core, Mong Man Wai Building,
The Hong Kong Polytechnic University

Abstract

Cryptographic zero-knowledge proof and argument systems are fundamental tools in cryptography which allow to argument the truth of statements while simultaneously keeping the witness secret. The properties which such proof systems offer are vastly exploited in the design of secure cryptographic protocols and are fundamental techniques for guaranteeing privacy. Although zero-knowledge proofs are already around for decades, very recently a special type of argument protocols called Zero-Knowledge Succinct Non-interactive Arguments of Knowledge (or simply zk-SNARKs), have found numerous applications in distributed ledger technology. In this talk I will discuss the fundamental concepts underlying zero-knowledge proofs and zk-SNARKs. I will start the talk by explaining the fundamental intuitions behind the definitions and constructions of such protocols classic zero-knowledge proofs. Finally I will conclude the talk by explaining the fast terminology in the field and give brief introduction to zk-SNARKs and their connection to distributed ledger technology.

About the Speaker

Kamil Kluczniak received his B. Eng. in 2011 and M.Sc. in 2012 from Wroclaw University of Technology. He received his PhD from the Institute of Computer Science of the Polish Academy of Sciences in 2016. His PhD dissertation entitled “Anonymous Authentication using Electronic Identity Documents” obtained a distinction from the Polish Academy of Sciences. He participated and supervised a number of research projects focusing mainly on privacy preserving authentication and anonymous credentials with applications to electronic identity documents. In 2016 he served as a consultant in the Polish Ministry of Digital Affairs on “the concept of implementing personal identity documents with electronic layer”. He is currently a post-doctoral fellow at The Department of Computing of The Hong Kong Polytechnic University. His current research interests include applied cryptography and privacy.

All are welcome!

Enquiries:
Professor George Baciu
Email: csgorge@comp.polyu.edu.hk
Tel : 2766 7295 / 2766 7272