Research Seminar

From Zero-knowledge Proofs to Ring Signatures

Dr Shang Gao
Research Assistant Professor
Department of Computing
The Hong Kong Polytechnic University
Hong Kong

Date : 17 November 2020 (Tuesday)
Time : 11:00 a.m. - 12:00 noon

► Abstract

Zero-knowledge proofs (ZKP) are fundamental building blocks used in many privacy-preserving applications such as anonymous cryptocurrencies and anonymous credentials. A particular example is one-out-of-many proofs which the prover's goal is to prove knowledge of an opening of a commitment within a set of commitments without revealing which one he has. Based on one-out-of-many proofs, we can further design ring signatures where a signatory signs a message on behalf of a group of users without revealing his identity. In this talk, we first introduce some logarithmic-size ring signature approaches. Then, we show that the one-out-of-many proof part in ring signatures can be safely replaced with a much looser relation, a linear sum proof, to improve efficiency without scarifying security. Furthermore, to implement efficient ring signatures, we introduce the idea of unbalanced relations and prove the unbalanced relation has the same security as the original relation in ZKPs. Our solutions work smoothly in both discrete log and lattice settings and can be applied in other ZKP techniques.

► About the Speaker

Dr Gao is the research assistant professor in the Department of Computing of The Hong Kong Polytechnic University. He obtained his Ph.D. degree from The Hong Kong Polytechnic University in 2019, supervised by Dr Bin Xiao. He received his M.Eng. degree from Southeast University, China and B.S. degree from Hangzhou Dianzi University, China, in 2014 and 2010 respectively. After graduation, he worked in Microsoft China for one year. Dr Gao is broadly interested in all security related areas, including information security, network security, data privacy, blockchain security, and applied cryptography.

ALL are welcome!

Enquiries : Professor George Baciu
Email : csgeorge@polyu.edu.hk
Tel : 2766 7272