Department of Computer Science, The University of Hong Kong

CS Seminar

Talk 1: ***Homomorphic Secret Sharing for Low Degree Polynomials***
Giulio Malavolta

Talk 2: ***Multi-Key Homomorphic Signatures Unforgeable under Insider Corruption***
Russell W. F. Lai

Date:
November 26, 2018
Monday
3:00 pm

Venue:
Room 328
Chow Yei Ching Building
The University of Hong Kong

Talk 1: Homomorphic Secret Sharing for Low Degree Polynomials

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-$\left((k+1)m -1 \right)$ 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.

About the Speaker: 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.

Talk 2: Multi-Key Homomorphic Signatures Unforgeable under Insider Corruption

Abstract: Homomorphic signatures (HS) allows the derivation of the signature of the message-function pair (m, g), where $m = g(m_1, \ldots, m_K)$, given the signatures of each of the input messages m_k signed under the same key. Multi-key HS (M-HS) introduced by Fiore~\etal~(ASIACRYPT'16) further enhances the utility by allowing evaluation of signatures under different keys. The unforgeability of existing M-HS notions assumes that all signers are honest. We consider a setting where an arbitrary number of signers can be corrupted, called unforgeability under corruption, which is typical for natural applications (\eg, verifiable multi-party computation) of M-HS. Surprisingly, there is a huge gap between M-HS (for arbitrary circuits) with and without unforgeability under corruption: While the latter can be constructed from standard lattice assumptions~(ASIACRYPT'16), we show that the former likely relies on non-falsifiable assumptions.
Specifically, we propose a generic construction of M-HS with unforgeability under corruption from zero-knowledge succinct non-interactive argument of knowledge (ZK-SNARK) (and other standard assumptions), and then show that such M-HS implies zero-knowledge succinct non-interactive arguments (ZK-SNARG). Our results leave openthe pressing question of what level of authenticity and utility can be achieved in the presence of corrupt signers under standard assumptions.

About the Speaker::Russell W. F. Lai is a PhD student in the Chair of Applied Cryptography, Friedrich-Alexander University Erlangen-Nuremberg, Germany. He received his MPhil degree in the Department of Information Engineering, Chinese University of Hong Kong. His research interests range from applied to theoretical cryptography.

All are welcome!
For enquiries, please call 2859 2180 or email enquiry@cs.hku.hk
Department of Computer Science
The University of Hong Kong