In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Multi-Key Homomorphic Signatures Unforgeable under Insider Corruption
by
Mr. Russell W. F. Lai
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany

Date	**:**	**28th November, 2018 (Wed)**
Time	**:**	**3:05pm – 3:35pm**
Venue	**:**	**Room 833, Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

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 *et al.* (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 (*e.g.*, 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 open the pressing question of what level of authenticity and utility can be achieved in the presence of corrupt signers under standard assumptions.

Biography

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 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)