In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Recent advances in privacy-preserving cryptocurrencies and augments for (bilinear) group relations

by

Mr. Russell W. F. Lai

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

Date : 7th January, 2020 (Tueday)

Time : 2:30pm – 3:30pm

Venue : Room 801, Ho Sin Hang Engineering Building
The Chinese University of Hong Kong

Abstract

In this talk, we will look at recent advances in 1) Ring Confidential Transactions (RingCT), one of the main approaches to construct privacy-preserving cryptocurrencies, and 2) zero-knowledge argument systems for (bilinear) group relations with short proofs.

RingCT is the core cryptographic component of Monero, one of the largest privacy-preserving cryptocurrencies. In RingCT, transactions are described in such a way that the spenders, the receivers, and the amount being transferred are hidden from third parties. Despite its importance in practice, the security guarantees of RingCT are poorly understood, and the efficiency of deployed schemes leaves much room for improvement.

In view of this, we devise a rigorous formulation of RingCT, which involves designing complex security experiments. We also describe a generic construction of RingCT, which mainly involves proving large statements using a zero-knowledge argument system for group relations. The latter motivates constructing such argument systems with short proofs -- those of length sublinear in the statement size.

Besides its application in RingCT, zero-knowledge argument systems for (bilinear) group relations is an important object in its own right. In their celebrated work, Groth and Sahai [EUROCRYPT'08, SICOMP' 12] constructed non-interactive zero-knowledge (NIZK) proofs for general (bilinear) group arithmetic relations, which spawned the entire subfield of structure-preserving cryptography. This branch of the theory of cryptography focuses on modular design of advanced cryptographic primitives. Although Groth-Sahai proofs is a powerful toolkit, its efficiency hits a barrier when the statement size is large, as the proof size is linear in that of the statement.

In a recent work, we revisit the problem of proving knowledge of general (bilinear) group arithmetic relations in zero-knowledge. Specifically, we construct a zero-knowledge argument for such relations, where the communication complexity is logarithmic in the integer and source group components of the witness. In many applications, our argument system can serve as a drop-in replacement of Groth-Sahai proofs, turning existing advanced primitives in the vast literature of structure-preserving cryptography into practically efficient systems.

Biography

Mr. Lai is a PhD candidate in the Friedrich-Alexander University Erlangen-Nuremberg advised by Prof. Dominique Schröder. He received his MPhil degree in Information Engineering in 2016, his BSc degree in Mathematics and BEng degree in Information Engineering in 2014, all from the Chinese University of Hong Kong. His recent research interests include succinct zero-knowledge arguments, privacy-preserving cryptocurrencies, searchable encryption, and password-based cryptography.

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

**** ALL ARE WELCOME ****

Host: Prof Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)