In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Unlinkable Policy-Compliant Signatures for Compliant and Decentralized Anonymous Payments

By

Mr. Mahdi Sedaghat
KU Leuven, ESAT/COSIC, Belgium

Date : 12 December 2023 (Tuesday)
Time : 11:00am – 12:00pm
Venue : Rm 801, Ho Sin Hang Engineering Building, CUHK

Abstract
Privacy-preserving payment systems face the difficult task of balancing privacy and accountability: on one hand, users should be able to transact privately and anonymously, on the other hand, no illegal activities should be tolerated. The challenging question of finding the right balance lies at the core of the research on accountable privacy that stipulates the use of cryptographic techniques for policy enforcement, but still allows an authority to revoke the anonymity of transactions whenever such an automatic enforcement is technically not supported. Current state-of-the-art systems are only able to enforce rather limited policies, such as spending or transaction limits, or assertions about participants, but are unable to enforce more complex policies that for example jointly evaluate both, the private credentials of sender and recipient, let alone to do this without an auditor in the loop during payment.

In this talk, I discuss how to enforce complex and joint policies while offering strong privacy and anonymity guarantees by enhancing the notion of policy-compliant signatures (PCS) introduced by Badertscher, Matt and Waldner (TCC'21). In more detail, we first define the notion of unlinkable PCS (ul-PCS) and show how this cryptographic primitive can be generically integrated with a wide range of systems including UTxO-based ledgers, privacy-preserving protocols like Monero or Zcash, and central-bank digital currencies. We give a generic construction for ul-PCS for any policy, and optimized constructions tailored for special policy classes, such as role-based policies and separable policies. To bridge the gap between theory and practice, we provide prototype implementations for all our schemes.

Biography
I'm Mahdi Sedaghat, a fourth-year PhD student at COSIC, KU Leuven. My primary research area goes around privacy-enhancing mechanisms within distributed systems. During my PhD journey, I've delved into various subjects, ranging from updateable and universal zkSNARKs to the development of digital signatures such as threshold signatures and policy-compliant signatures, as well as access control encryptions. In the early part of this year, I had the opportunity to visit the Blockchain Technology Lab at the University of Edinburgh. Additionally, I enriched my experience as a research scientist during the past summer through an internship at Mysten Labs. At present, my primary focus lies in the realm of privacy-balancing cryptocurrencies and trying to enrich threshold structure-preserving signatures. I'm looking forward to meeting you all in person and discussing any intriguing topic.

**** ALL ARE WELCOME ****

Host: Prof. Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8474)