Mathematics and CS Seminar

Rossario Gennaro; Zero-Knowledge Contingent Payments Revisited

Rossario Gennaro
The City College of New York

Host: Krzysztof Pietrzak

Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for ServicesRosario Gennaro The City College of New YorkAbstract: Zero Knowledge Contingent Payment (ZKCP) protocols allowfair exchange of sold goods and payments over the Bitcoin network. Inthis paper we point out two main shortcomings of current proposals forZKCP.First we show an attack that allows a buyer to learn partialinformation about the digital good being sold, without paying for it.This break in the zero-knowledge condition of ZKCP is due to the factthat in the protocols we attack, the buyer is allowed to choose commonparameters that normally should be selected by a trusted third party.We present ways to fix this attack that do not require a trusted third party.Second, we show that ZKCP are not suited for the purchase of digitalservices rather than goods. Current constructions of ZKCP do not allowa seller to receive payments after proving that a certain service hasbeen rendered, but only for the sale of a specific digital good. Wedefine the notion of Zero-Knowledge Contingent Service Payment (ZKCSP)protocols and construct two new protocols, for either public orprivate verification.We implemented and tested the attack on ZKCP, and our two new ZKCSPprotocols, showing their feasibility for very realistic examples. Wepresent code that learns, without paying, the value of a Sudoku cellin the original "Pay-to-Sudoku" ZKCP implementation. We also implementZKCSP protocols for the case of Proof of Retrievability, where aclient pays the server for providing a proof that the client's data iscorrectly stored by the server. A side product of our implementationeffort is a new optimized circuit for SHA256 with less than a quarterthan the number of AND gates of the best previously publicly availableone. Our new SHA256 circuit may be of independent use forcircuit-based MPC and FHE protocols that require SHA256 circuits.Joint work with Matteo Campanelli, Steven Goldfeder and Luca Nizzardo.To appear at ACM CCS 2017

Wednesday, October 25, 2017 02:00pm - 03:30pm
Mondi Seminar Room 1, Central Building

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station. Please find a schedule of the ISTA Shuttle on our webpage: https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.