Vassilis Zikas

vzikas@cs.rpi.edu
www.cs.rpi.edu/~zikasv

Cryptography on the Blockchain

Tuesday, May 31 2016, 14-15:30

In this lecture we discuss how blockchain protocols can be used to strengthen the security of general cryptographic protocols. We distill the core functionality of blockchains in a (global) transaction-ledger functionality within a universally composable (UC) setting. We then discuss how synchronous (G)UC protocols can use such a transaction-ledger functionality to leverage security-loss via a compensation mechanism. Concretely, we focus on the design of fair and robust multi-party computation (MPC) where fairness against dishonest majorities is achieved via a compensation mechanism and, additionally, a robustness property is guaranteed, which ensures that the protocol delivers output to the parties that get engaged. We discuss a formal model of secure MPC with compensation that can be used to prove the security of protocols within a standard cryptographic framework while ensuring universal composition.

Reading:

- Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas, Fair and Robust Multi-Party Computation using a Global Transaction Ledger, Cryptology ePrint Archive: Report 2015/574, https://eprint.iacr.org/2015/574