

**Computer Science Department**

Public Blockchains as General Computing Platforms

**Shai Halevi, Ph.D.**

  Algorand Foundation

Hosted by Guiling Wang, Ph.D.

**Date:**    Wednesday, November 4, 2020

**Time:**    2:30 PM - 3:30 PM

**WebEx:** https://njit.webex.com/njit/j.php?MTID=m71a4c799d039c054d9a84a359fa7e48f

**Abstract:**

Public blockchains have emerged over the last decade as a promising architecture for distributed computing, touted by some as "the world's computer". Using "smart contracts" with public execution and agreement protocol, public blockchains provide a compute environment with highly dependable results. However, the public nature of the computation also makes is challenging to use secret data in the computation.

In an ongoing sequence of works, we are developing an architecture and protocols that let smart contracts on a public blockchain maintain and manipulate secret data. The starting point of the solution is secret-sharing the data instead of replicating it, and using secure multiparty computation (SMPC) tools to compute on it. But a public blockchain may have many thousands of nodes, and running SMPC protocols among all of them is prohibitively expensive. We thus need to use small committees to carry out the work on behalf of the entire system.

The technical challenge that we face is that being small, these committees may be subject to targeted attacks (such as DDoS). We address this challenge with new techniques for setting up these committees and allowing them to compute without anyone knowing who they are, until after they completed their work. Even the committee members themselves cannot know each other's identities. Importantly, we are not relying on anonymous communication: all we need is a completely public broadcast channel (which is provided by the blockchain).

Our SMPC protocols use ephemeral stateless parties that operate locally for a while, then conclude their participation by broadcasting a single message. We term this style "You Only Speak Once" (YOSO). Besides the application to blockchains, YOSO protocols are also useful in the context of serverless computing.

Based on joint works with: Fabrice Benhamouda, Craig Gentry, Sergey Gorbunov, Hugo Krawczyk, Chengyu Lin, Bernardo Magri, Jesper Buus Nielsen, Tal Rabin, Leonid Reyzin, Sophia Yakoubov

**Bio:**
Dr. Shai Halevi is a research fellow at the Algorand Foundation. He obtained his PhD from MIT in 1997, and his work since then is focused on advanced cryptographic techniques such as homomorphic encryption, cryptographic code obfuscation, and secure computation. Shai is a fellow and a vice president of the IACR, and the recipient of the 2017 ACM-SIGSAC Outstanding Innovation Award and several best-paper awards. Shai also wrote the HElib library for homomorphic encryption.