NJIT

Department of Computer Science

Using Zero-Knowledge to Reconcile Law Enforcement Secrecy and Fair Trial Rights in Criminal Cases

Dor Bitan
Simons Institute for the Theory of Computing at UC Berkeley

Hosted by Shantanu Sharma

Date: Thursday, October 31, 2022
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=m35de3d75a3eabf13324f5b6567d50034

Join by meeting number

Meeting number (access code): 2620 839 3883

Meeting password: CDnpniyS466

http://cs.njit.edu/seminars

Abstract: The use of hidden investigative software to collect evidence of crimes presents courts with a recurring dilemma: On the one hand, there is often clear public interest in keeping the software hidden to preserve its effectiveness in fighting crimes. On the other hand, criminal defendants have rights to inspect and challenge the full evidence against them, including law enforcement's investigative methods. Presently, courts balance these conflicting interests on a case-by-case basis, often voicing their frustration with the challenging dilemma they face.

In this talk, I'll describe recent joint work with professors Ran Canetti, Shafi Goldwasser, and Rebeca Wexler, where we demonstrate how Zero Knowledge Proofs (ZKP) could help to mitigate this dilemma: Based on actual court cases where evidence was collected using a modified version of P2P software, we demonstrate how law enforcement could, in these cases, augment their investigative software with a ZKP-based mechanism that would allow them to later provide full responses to challenges made by a defense expert -- and allow a defense expert to independently verify law enforcement claims -- while keeping the software hidden.

I'll describe our proof-of-concept implementation of a system that demonstrates the technical feasibility of our solution. If time allows, I'll discuss how the tools and methods developed within our work could be used to address further problems -- both in the legal landscape, and to enhance privacy in the public interest.

Bio: Dor Bitan is a postdoctoral researcher at the Simons Institute for the Theory of Computing at UC Berkeley. He is PI'ed by professor Shafi Goldwasser and works in DARPA's SIEVE project. He received his Ph.D. in mathematics from Ben-Gurion University of the Negev, Israel, in 2021. In between, Dor worked at Rafael Advanced Defense Systems, where he led and worked on projects in the scope of machine learning, data science, and cryptography. His published peer-reviewed papers present algorithms for computation over encrypted data. Before turning to academia, Dor served nine years as a fighter, commander, and officer in the Israeli army. Among his roles, he was an infantry company commander in an elite combat unit.