NJIT

Department of Computer Science

Cryptography For Fast and Scalable Distributed Applications

Sri AravindaKrishnan Thyagarajan
NTT Research

Hosted by Shantanu Sharma

Date: Friday, January 27, 2023
Coffee: 10:45 AM – 11:00 AM
Time: 11:00 AM – 12:00 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit.webex.com/njit/j.php?MTID=mf3a157f1ac39297cd3112da83e1a112c

http://cs.njit.edu/seminars

Abstract: Distributed applications are settings where a set of mutually distrustful users interact and compute functions over their private inputs without any centralized trust. Such scenarios are abundant in the digital world, like cloud computing, privacy-preserving computation, and emerging technologies like Decentralized Finance (DeFi) applications, including blockchains, cryptocurrencies, etc. These new systems offer payment services where we do not require any trusted entity, such as a Bank or a Government, to make payments. Users seek security and privacy that ensures an attacker cannot learn unintended information from an honest user. They also desire (a) cryptographic fairness, which assures users of receiving their output if the attacker receives his, and (b) game-theoretic fairness, where a rational adversary has no incentive to harm honest users.

Given their potential and their growing importance in mainstream society, numerous foundational and practical questions arise concerning security and fairness in these applications. My research amalgamates techniques from applied cryptography and game theory as part of a concerted effort by the community to address these questions. In this talk, I will highlight some key challenges for security and fairness in the specific case of DeFi applications and present a brief overview of my research that overcomes these challenges.

The talk will then focus on the specific scenario of conditional asset transfers in DeFi systems, that is, user Alice transfers her assets to user Bob provided some condition external to the transfer itself is satisfied. Such conditional transfer of assets or payments is highly common in the real world and has several applications in the context of DeFi systems that are currently used in practice. However, current solutions seriously fall short in at least one or more of the following metrics: (1) privacy of users' information, (2) computation and economic costs borne by the users and the system, (3) scalability with the size of the system, and (4) compatibility across many DeFi systems. I will present novel cryptographic solutions with provable security guarantees that solve all of the above pitfalls in specific conditional payment scenarios like payments based on real-life event outcomes. The solution is carefully set up with new cryptographic tools and techniques and offers high efficiency that is enough to be deployed in all major DeFi systems of today. Beyond DeFi systems, the cryptographic solution also unlocks new use cases in other distributed applications like sending messages to the future, and financial adjudication, among many others.

Bio: Sri AravindaKrishnan Thyagarajan (or shortly Aravind) is currently a Postdoc at NTT Research with Dr. Hoeteck Wee and was formerly a Postdoc at Carnegie Mellon University with Prof. Elaine Shi. He completed his Ph.D. in Computer Science at the University of Erlangen Nuremberg, Germany, with Prof. Dominique Schröder as his advisor in 2021. Before that, he finished his Masters in Science at Saarland University, Germany, in 2016. His primary research interest is in applied cryptography, where he develops new tools and techniques with sound theoretical foundations to solve security, privacy, fairness, and efficiency problems in distributed applications like distributed computing, blockchains, cryptocurrencies, and other multi-party computation scenarios. Several of his works have been featured at top cryptography and security conferences like CRYPTO, Oakland IEEE S&P, ACM CCS, and NDSS.