STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Samaneh Berenjian
Degree:	Doctor of Philosophy
School/Department:	Charles V. Schaefer, Jr. School of Engineering and Science / Computer Science
Date:	Wednesday, March 29th, 2023
Time/Location:	10AM-12PM / https://stevens.zoom.us/j/95544275064
Title:	Encryption-Based Secure Protocol Design for Networks
Chairperson:	Dr. Nikolaos Triandopoulos, Department of Computer Science, Schaefer School of Engineering & Science
Committee Members:	Dr. Robert Gilman, Department of Mathematical Sciences, Schaefer School of Engineering & Science Dr. Michael Greenberg, Department of Computer Science, Schaefer School of Engineering & Science Dr. Georgios Portokalidis, Department of Computer Science, Schaefer School of Engineering & Science Dr. Jun Xu, School of Computing, University of Utah

ABSTRACT

Security is vital for any distributed computing application running over a set of networked machines, some of which may possibly misbehave, due to misconfigurations, cost-cutting incentives, or after being compromised by an external attacker. In addition to protection against data breaches, eavesdropping, or data manipulation, caused by Attacker-In-The-Middle threats, data management and computations that are jointly performed by individual machines, should satisfy application-specific properties that relate to fairness, privacy, and correctness, in various threat models, rendering efficient secure protocol design an important and challenging task.

In this thesis, we explore the use of cryptographic tools, in particular, special forms of encryption, to provide efficient solutions for security problems that relate to two general distributed computing models. First, in the setting of decentralized participatory, or Peer-to-Peer (P2P), networks, where individual network nodes share common resources, we study the problem of fairness, which seeks for mechanisms that ensure the longevity of provided services in the network via proportional use of offered resources amongst participating peers. In particular, we propose, analyze and experimentally study, a novel encryption-based protocol for data management that achieves high levels of fairness by reducing the workloads of peers in the network which make resources available, so that they are encouraged to stay longer in the network, and by forcing the peers in the network which consume resources to additionally contribute resources to the P2P system.

Second, in the setting of secure Multi-Party Computation (MPC), where individual network nodes communicate to compute a function over their private inputs, we study the problem of Private Set Membership (PSM), which seeks for protocols that allow two parties to jointly compute whether an element owned by one party is contained in a set owned by the other, but nothing else is learned beyond the membership result. We propose, analyze and experimentally study two low-communication PSM protocols, one permitting only the client and one permitting only the server to learn the set-membership result. At its core, our design lies in the judicious and optimized modification of the state-of-the-art and practical solution for the problem of Private Information Retrieval (PIR), namely SealPIR, wherein we reduce the underlying communication overheads by utilizing homomorphic encryption (such as BFV and ElGamal) in specific advantageous configurations. We prove the security of our protocol that reveals the output to the client, in the semi-honest and malicious settings, and we demonstrate the properties of client and server privacy for our protocol that reveals the output to the server. Finally, we conclude by discussing research directions and future work plans related to the above problems and results.