COLLEGE OF ENGINEERING
AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Mohammad Ghaseminejad Raeini

for the degree of Doctor of Philosophy (Ph.D.)

"Selected Applications of MPC"

June 30, 2022, 11:00 A.M.
Virtual Dissertation

Zoom Meeting
Meeting ID: 822 5876 7512
Passcode: 2dquDj

DEPARTMENT:
Electrical Engineering and Computer Science

ADVISOR:
Feng-Hao Liu, Ph.D.

CO-ADVISOR:
Mehrdad Nojoumian, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Feng-Hao Liu, Ph.D., Chair
Mehrdad Nojoumian, Ph.D., Co-Chair
Hanqi Zhuang, Ph.D.
Reza Azarderakhsh, Ph.D.
Edoardo Persichetti, Ph.D.

ABSTRACT OF DISSERTATION
Selected Applications of MPC

Secure multiparty computation (secure MPC) is a computational paradigm that enables a group of parties to evaluate a public function on their private data without revealing the data (i.e., by preserving the privacy of their data). This computational approach, sometimes also referred to as secure function evaluation (SFE) and privacy-preserving computation, has attracted significant attention in the last couple of decades. It has been studied in different application domains, including in privacy-preserving data mining and machine learning, secure signal processing, secure genome analysis, sealed-bid auctions, etc. There are different approaches for realizing secure MPC. Some commonly used approaches include secret sharing schemes, Yao's garbled circuits, and homomorphic encryption techniques.

The main focus of this dissertation is to further investigate secure multiparty computation as an appealing area of research and to study its applications in different domains. We specifically focus on secure multiparty computation based on secret sharing and fully homomorphic encryption (FHE) schemes. We review the important theoretical foundations of these approaches and provide some novel applications for each of them. For the fully homomorphic encryption (FHE) part, we mainly focus on FHE schemes based on the LWE or RLWE problem. Particularly, we provide a C++ implementation for the ring variant of a third generation FHE scheme called the approximate eigenvector method (a.k.a., the GSW scheme). We then propose some novel approaches for homomorphic evaluation of common functionalities based on the implemented (R)LWE and RGSW schemes. We specifically present some constructions for homomorphic computation of pseudorandom functions (PRFs). For secure computation based on secret sharing, we provide some novel protocols for secure trust evaluation (STE). Our proposed STE techniques enable the parties in trust and reputation

systems (TRS) to securely assess their trust values in each other while they keep their input trust values private. We would like to remark that trust and reputation are social mechanisms which can be considered as soft security measures that complement hard security measures (e.g., cryptographic and secure multiparty computation techniques).

BIOGRAPHICAL SKETCH
Born in Sirjan, Kerman, Iran
B.S., Bahonar University of Kerman, Kerman, Kerman, Iran, 2004-2008
M.S., University of Tehran, Tehran, Tehran, Iran, 2099-2012
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2017-2022

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2019 - 2022

Qualifying Examination Passed: Spring 2018

Published Papers:

D. Gordon, Feng-Hao Liu, M. Liang, D. Mcvicker, Mohammad Raeini, “MPC with Guaranteed Output Delivery”, manuscript under preparation, to be submitted to a cryptography-related venue, 2022. Important note: this is a collaborative work under preparation. The title, the order of the authors, and other relevant things might change with the authors’ consent. This student’s contribution is based on chapter 4 and 5 of the draft of the dissertation.

Raeini, Mohammad, and Mehrdad Nojoumian. "Privacy-preserving big data analytics: from theory to practice." International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2019.

Raeini, Mohammad G., and Mehrdad Nojoumian. "Secure trust evaluation using multipath and referral chain methods." International Workshop on Security and Trust Management. Springer, Cham, 2019.

Raeini, Mohammad G., and Mehrdad Nojoumian. "Secure error correction using multiparty computation." 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2018.