Pouyan Forghani

Curriculum Vitae

Georgia Institute of Technology School of Cybersecurity and Privacy
Cell Phone: (979) 595-8395 — **Email:** pforghani3@gatech.edu

Education

Texas A&M University—College Station, Texas
Department of Computer Science and Engineering
Doctor of Philosophy in Computer Science (December, 2025)

> **Dissertation Title:** Secure Composition of Asynchronous Cryptographic Protocols
>
> **Committee:** Juan Garay, PhD; Jianer Chen, PhD; Nitesh Saxena, PhD; Joseph Rojas, PhD

Sharif University of Technology—Tehran, Iran
Department of Electrical Engineering
Master of Science in Electrical Engineering—Secure Communication and Cryptography (January, 2019)

> **Thesis Title:** Design and analysis of a new code-based signature with provable security based on polar codes

Iran University of Science and Technology—Tehran, Iran
Department of Electrical Engineering
Bachelor of Science in Electrical Engineering (September, 2016)

> **Thesis Title:** Study and Analysis of One-Bit Compressed Sensing Using Gradient Descent Method

Academic Experience

Zikas Research Group, Georgia Institute of Technology—Atlanta, Georgia
Postdoctoral Fellow (June, 2026 — Current)

- Developing randomized and early-stopping cryptographic protocols
- Universally composable treatment of blockchain protocols
- Industry-sponsored research (Sunday Group, Inc. and DAG Technologies, Inc.) on round-efficient Byzantine agreement and composable security analysis for the Möbby blockchain protocol

Garay Research Group, Texas A&M University—College Station, Texas
Graduate Research Assistant (September, 2019 — December 2025)

- Conduct fundamental research on fast and secure parallel composition of asynchronous cryptographic protocols
- Investigate composable security of secure multiparty computation (MPC) in sparse communication graphs
- Revisiting round definition on asynchronous setting
- Contributor to NSF-supported projects (Awards CNS-2001082 and CNS-2055694, PI Juan Garay; collaborative Award CNS-2055599, PI Vassilis Zikas) and to MEGA-ACE, the Algorand Foundation-funded multi-institution research alliance led by Purdue

Information System and Security Lab (ISSL), Sharif University of Technology—Tehran, Iran
Graduate Research Assistant (January, 2017 — January, 2019)

- Investigated possibility of using Polar codes for reducing key size for post-quantum digital signatures
- Developed privacy preserving protocols for data aggregation with application to smart grids

Mobile Broadband Networks Research Group (MBNRG), Iran University of Science and Technology—Tehran, Iran
Research Assistant (May, 2014 — October, 2014)

- Studied fourth generation of mobile broadband networks

Industrial Experience

Input Output Global (IOHK USA LLC)—Remote
Research Intern (June 16 — August 24, 2025)

- Universally composable framework for decentralized applications (DApps) and smart contracts
- Formalized a UC global ledger with smart-contract capabilities and developed the representative decentralized application and its security proof

Publications

Peer-Review Conferences and Journals

- Cohen, R., Collins, D., Forghani, P., Garay, J. and Zikas, V., (2026). On the Round Complexity of Dishonest-Majority MPC. *Theory of Cryptography Conference — TCC 2026* (accepted August 2026; to appear). Cryptology ePrint Archive, Report 2026/1277
- Chandran, N., Forghani, P., Garay, J., Ostrovsky, R., Patel, R., & Zikas, V. (2026). Universally Composable Almost-Everywhere Secure Computation. In *Journal of Cryptology*
- Cohen, R., Forghani, P., Garay, J., Patel, R. and Zikas, V., (2025). Is It Even Possible? On the Parallel Composition of Asynchronous Cryptographic Protocols. *Theory of Cryptography Conference — TCC 2025*
- Cohen, R., Forghani, P., Garay, J., Patel, R. and Zikas, V., (2023). Concurrent Asynchronous Byzantine Agreement in Expected-Constant Rounds, Revisited. *Theory of Cryptography Conference — TCC 2023*
- Chandran, N., Forghani, P., Garay, J., Ostrovsky, R., Patel, R., & Zikas, V. (2022). Universally Composable Almost-Everywhere Secure Computation. In *3rd Conference on Information-Theoretic Cryptography (ITC 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik
- Forghani, P., Koochak Shooshtari, M., & Aref, M. R. (2020). PolarSig: An efficient digital signature based on polar codes. *IET Communications*, *14*(17), 2889-2897
- Sarenche, R., Forghani, P., Ameri, M. H., Aref, M. R., & Salmasizadeh, M. (2018, December). An Efficient Secure Scheme for Lossy and Lossless Data Aggregation in Smart Grid. In *2018 9th International Symposium on Telecommunications (IST)* (pp. 528-534). IEEE

Manuscripts Under Submission

- Ciampi, M., Forghani, P., Lu, Y. and Zikas, V. Randomized Early-Stopping Byzantine Agreement with Applications to Round-Efficient MPC. Submitted to EUROCRYPT 2027, September 2026 (under review)

Talks/Presentations

- Texas Crypto Day (April 2024) (https://texascryptoday.github.io/events/4-TAMU.html)

- **Title:** Is It Even Possible? On the Parallel Composition of Asynchronous Cryptographic Protocols
- Texas Crypto Day (April 2023) (https://texascryptoday.github.io/events/2-UTAustin.html)
  - **Title:** Optimal Asynchronous and Multi-valued Oblivious Common Coin — A Detective Story
- Conference on Information-Theoretic Cryptography (2022) (https://itcrypto.github.io/2022/2022prog.html)
  - **Title:** Universally Composable Almost-Everywhere Secure Computation

Teaching and Instruction

Lecturing

Texas A&M University, Department of Computer Science and Engineering—College Station, TX
Guest Lecturer

- Distributed Algorithms and Systems, Fall 2024
- Foundation of Modern Cryptography, Spring 2024
- Blockchain Foundations and Applications, Spring 2023
- Data Structures and Algorithms, Fall 2019

University of Buenos Aires, Department of Computer Science— Buenos Aires, Argentina
Guest Lecturer

- Blockchain Foundations and Applications, Fall 2023

Teaching Assistantship

Texas A&M University, Department of Computer Science and Engineering—College Station, TX
Graduate Teaching Assistant (September 2019 – December 2025)

- Analysis of Algorithms (CSCE 629, Fall 2025)
- Analysis of Algorithms (CSCE 629, Spring 2025)
- Distributed Algorithms and Systems (CSCE 668, Fall 2024, Fall 2023)
- Discrete Structures for Computing (CSCE 222, Summer 2024, Fall 2022, Summer 2022)
- Intro to Modern Crypto (CSCE 711, Spring 2024)
- Foundations and Applications of Blockchains (CSCE 689, Spring 2023)
- Computer and Network Security (CSCE 465, Fall 2021)
- Cryptography (CSCE 689, Fall 2019)

Sharif University of Technology, Department of Electrical Engineering—Tehran, Iran
Graduate Teaching Assistant (September 2017 – December 2017)

- Cryptography Mathematics (Fall 2017)
- Cryptography (Fall 2017)

Iran University of Science and Technology, Department of Electrical Engineering—Tehran, Iran
Teaching Assistant (September 2013 – December 2013)

- Signals and Systems (Fall 2013)

Academic Leadership and Service

Peer Review

- Reviewer of **International Symposium on Distributed Computing 2026**
- Reviewer of **IEEE Transactions on Dependable and Secure Computing 2026**
- Reviewer of **Journal of Cryptology 2026**
- Reviewer of **ITC 2026**
- Reviewer of **Journal of Parallel and Distributed Computing 2025**
- Reviewer of **Journal of Cryptology 2025**
- External Reviewer of **Crypto 2025, 2026**
- Reviewer of **ACM PODC 2025**
- External Reviewer of **Eurocrypt 2024, 2025, 2026**
- Reviewer of **Journal of ACM 2024**
- External Reviewer of **Theoretical Cryptography Conference (TCC) 2024, 2025**
- External Reviewer of **Security and Cryptography for Networks (SCN) 2022, 2024**
- External Reviewer of **Asiacrypt 2022**
- Reviewer of **IET Information Security 2020, 2021**

Community

- Panelist, CSCE 682 (Introduction to PhD Studies) senior-student panel, Texas A&M University, October 2024
- On-site volunteer with some of the local organization of CRYPTO 2024.

Professional Development

- Co-organized the interdepartmental "Advanced Cryptography Reading Group" and co-designed its semester-long schedule, at Texas A&M University, College Station, Texas, Fall 2023
- Co-organized "Universal Composability and Lattice-Based Cryptography Reading Group", at Texas A&M University, College Station, Texas, Spring 2025

Certificates

- GRAD Aggies Foundations Certificate, Texas A&M University — 2026 (professional development program)

Grants, Awards, and Honors

- Awarded $1000 Texas A&M University Graduate and Professional School Travel Award (2025)
- Awarded $1000 Texas A&M University College of Engineering, Department of Computer Science and Engineering Travel Grant (2025)
- Awarded $500 IACR travel grant for Crypto'24 conference.
- Ranked 1st among Secure Communication and Cryptography students, at Sharif University of Technology (SUT) (May 2018)
- Ranked among the top 10 in all 149 master's students at the Electrical Engineering Department, Sharif University of Technology (SUT) (May 2018)

- Awarded certificate for attending the “Workshop on Data Security in Cloud Computing” held on November 9-10, 2016 at Sharif University of Technology (SUT), Tehran, Iran.
- Recognized as an excellent student in the Electrical Engineering – Communication B.Sc. program, at Iran University of Science and Technology (IUST). (December 2015)
- Semi-finalist in the Iranian National Olympiad (Both Mathematics and Computer). (January 2007)
- Semi-finalist in the Iranian National Olympiad, Mathematics. (January 2008)