Bhavish Raj Gopal

PhD Candidate, Department of Computer Science and Automation, Indian Institute of Science, Bangalore
bhavishraj@iisc.ac.in | +91-9962970900 | Personal Webpage

Research Interests

My research focuses on applied cryptography and secure multiparty computation (MPC), with an emphasis on designing, implementing, and evaluating practical privacy-preserving systems. My work spans scalable secure computation frameworks, maliciously secure protocols, privacy-preserving machine learning, and implementation-level security analysis. I have extensive experience developing networked MPC systems, optimizing cryptographic protocols, and evaluating their performance across different computational and network settings. My broader research interests include building efficient and deployable cryptographic systems that bridge the gap between theoretical security guarantees and practical applications.

Education

- **PhD, Indian Institute of Science, Bangalore, India** *2022 – present* ((Thesis submission expected October 2026))
  Computer Science and Automation CGPA: 9/10
- **BS-MS Dual Degree, Indian Institute of Science Education and Research Mohali** *2016 – 2021*
  Mathematics CGPA: 7.3/10

Research Contributions Relevant to Secure Systems

- **Scalable secure distributed computation.** Designed and implemented Graphiti and GraSP, MPC frameworks for large-scale privacy-preserving graph computation. Developed communication-efficient protocols and implemented multithreaded, networked MPC systems, with extensive benchmarking across different graph sizes, party configurations, and network settings. Implementation available at https://github.com/Bhavishrg/CrIS-MPC
- **Implementation-level security analysis across MPC and FHE.** As a visiting researcher at Aarhus University, I investigated discrepancies between theoretical security guarantees and practical MPC implementations, including selective-abort leakage in MPC and garbled-circuit protocols, noise-based leakage in FHE, and security auditing of existing MPC frameworks such as MP-SPDZ, FRESCO, FANNG, etc.
- **Maliciously secure protocol design.** Designed efficient maliciously secure MPC protocols with applications to secure graph computation, parsing, anonymous broadcast and heavy hitters. Worked across different adversarial settings, including two-party, three-party, four-party and general multiparty computation.

Research and Professional Experience

Visiting PhD Researcher, Aarhus University, Aarhus, Denmark May 2026 – Aug 2026

- Investigated gaps between theoretical security proofs and real-world implementations of cryptographic protocols: selective-abort leakage in MPC and garbled-circuit protocols, and noise-based leakage in FHE schemes; hands-on work with TFHE-rs and the TFHE C++ wrapper library.

Research Intern, Silence Laboratories, Remote Mar 2026 – May 2026

- Co-developed efficient maliciously secure MPC protocols, including Truffle, and privacy-preserving protocols for anti-money-laundering analytics over distributed financial transaction networks.

Researcher, Bell Labs – Nokia, Antwerp Sep 2025 – Dec 2025

- Designed an MPC-based system for secure audio conferencing, including MPC-friendly techniques for audio compression, decompression, and mixing under real-time performance constraints.

Research Associate, Indian Urban Data Exchange Project, IISc Jan 2022 – Jul 2022

Publications and Preprints

Authors listed in alphabetical order.

Peer-Reviewed Publications

- Nidhish Bhimrajka, Yashvanth Kondi, Daniel Noble, **Bhavish Raj Gopal**. Truffle: Maliciously Secure Three-Party Shuffles with Applications to Parsing. *ACM CCS 2026*.
- Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. Entrada to Secure Graph Convolutional Networks. *IEEE TDSC 2025*. eprint.iacr.org/2023/1807
- Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. Match Quest: Fast and Secure Pattern Matching. *PoPETS 2025*.
- **Bhavish Raj Gopal**. Privacy-Preserving Graph Analysis. *ACM CCS 2024 Doctoral Symposium*. dl.acm.org/doi/pdf/10.1145/3658644.3690867
- Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. Graphiti: Secure Graph Computation Made More Scalable. *ACM CCS 2024*. eprint.iacr.org/2024/1756
- Pranav Jangir, Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**, Somya Sangal. Vogue: Faster Computation of Private Heavy Hitters. *IEEE TDSC 2023*. eprint.iacr.org/2022/1561
- Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. Shield: Secure Allegation Escrow System with Stronger Guarantees. *The Web Conference 2023*. eprint.iacr.org/2023/338
- Pranav Shriram A, Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**, Somya Sangal. Ruffle: Rapid 3-Party Shuffle Protocols. *PoPETS 2023*. eprint.iacr.org/2023/431
- Pranav Shriram A, Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. Privacy-Preserving Local Clustering Based on Heat Kernel PageRank. *PoPETS 2023*. eprint.iacr.org/2022/1727
- Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. PentaGOD: Stepping beyond traditional GOD with five parties. *ACM CCS 2022*. eprint.iacr.org/2022/1118

Manuscripts Under Submission

- Riddhiman Dutta Roy, Kaustubh Limaye, Arpita Patra, **Bhavish Raj Gopal**. TreePSI: Structure-Aware Private Set Intersection via Hierarchical Search Trees.
- Siddharth Kapoor, Shravani Patil, Arpita Patra, **Bhavish Raj Gopal**. Making Maliciously Secure Graph Computation Practical.
- Ethan Y. Chen, Kartik Nayak, Arpita Patra, **Bhavish Raj Gopal**. Grapharo: Secure and Updatable Graph Computation.
- Siddharth Kapoor, Nishat Koti, Varsha Bhat Kukkala, Arpita Patra, **Bhavish Raj Gopal**. GraSP: Secure Collaborative Graph Processing Made Scalable. eprint.iacr.org/2025/590
- Siddharth Kapoor, Shyam Murthy, Sriram Murthy, Arpita Patra, **Bhavish Raj Gopal**, Raghavan Ramesh. SMILIES: Secure eMaIL InfrastructurE and Services.

Technical Skills

- **Programming:** C++ (primary), Python; extensive experience implementing multithreaded and networked MPC systems, cryptographic protocol optimization, performance benchmarking, and experimental evaluation.
- **Cryptographic frameworks and libraries:** EMP-toolkit, CrypTen, MOTION, TFHE-rs, TFHE C++ wrapper, FANNG-MPC.
- **Research areas:** Applied cryptography, secure multiparty computation, homomorphic encryption, privacy-enhancing technologies, secure systems, graph analytics.

Mentoring and Leadership

- Mentored junior researchers on active projects: Siddharth Kapoor (GraSP), and Riddhiman Dutta Roy and Kaustubh Limaye (TreePSI).
- Organizer, MPC Retreat 2026 and TPMPC 2025, IISc Bangalore — helped organize an invite-only research retreat and workshop bringing together researchers and students in secure computation and applied cryptography.

Invited Talks and Presentations

- Secure Graph Computation. MPC Retreat, IISc, March 2026.
- GraSP: Secure Collaborative Graph Processing Made Scalable. RWMPC 2026, Taipei, Taiwan, March 2026.
- Privacy-Preserving Graph Analysis: The Journey So Far and The Road Ahead. KU Leuven, September 2025; George Mason University, Washington, DC, July 2025.
- Match Quest: Fast and Secure Pattern Matching. PETS 2025, Washington, DC, July 2025.
- Privacy-Preserving Graph Analysis. EECS Symposium 2025, IISc, April 2025; ACM CCS Doctoral Symposium, Salt Lake City, Utah, October 2024.
- Graphiti: Secure Graph Computation Made More Scalable. NIST Workshop on Privacy-Enhancing Cryptography, Online, September 2024.
- Shield: Secure Allegation Escrow System with Stronger Guarantees. ACM ARCS, NISER Bhubaneswar, February 2024.

- Entrada to Secure Graph Convolutional Networks. CyPhySS 2023, IIT Kharagpur, July 2023.
- Find thy Neighbourhood: Privacy-Preserving Local Clustering. TPMPC 2023, Aarhus University, Denmark, June 2023.
- Digital Signatures. ISEA Workshop 2023, SERC, Indian Institute of Science, April 2023.

Professional Service

- **Conference Reviewing:** The Web Conference 2024, EUROCRYPT 2023, IEEE FOCS 2024.
- **Journal Reviewing:** IEEE Transactions on Dependable and Secure Computing.
- **Teaching Assistant:** Data Structures and Algorithms; Foundations of Cryptography; Foundations of Secure Computation.

Awards and Honors

- Prime Minister Research Fellowship, Government of India, 2023.
- Kotak IISc AI Center Scholarship, 2023.
- ACM Travel Grant to attend ACM CCS Doctoral Symposium, 2024.
- Google Travel Grant to attend ACM CCS, 2024.
- PETS stipend and ACM Travel Grant to attend Privacy Enhancing Technologies Symposium, 2023.
- Rashtrapati Scout Award, Bharat Scouts and Guides.