Deep Inder Mohan

E-mail: dmohan@gatech.edu
Contact Number: (+1) 470-929-4920
Github: https://github.com/deep-inder

Education

Georgia Institute of Technology Atlanta, USA
Ph.D. in Computer Science @ School of Cybersecurity and Privacy (SCP) *2022-present*

- GPA - 4.0/4.0
- Co-advised by Sasha Boldyreva and Joseph Jaeger

International Institute of Information Technology (IIITB) Bangalore, India
Integrated M.Tech. Computer Science and Engineering *2017-2022*

- CGPA - 3.71/4.0
- Dean's Merit List awardee for 2017-18, 2018-19, 2019-20, 2020-21, and 2021-22

Interests and Skills

Research Interests

- Provable Security, Idealized Models of Computation, Secure Biometric Authentication, Privacy-Enhancing Technologies, Multi-Party Computation, Threshold Signatures.

Programming Languages

- Python, C, C++, Rust

Projects and Publications

1. **Generic and Algebraic Computation Models** *(CRYPTO 2024)*: We define a new framework for the Algebraic Group Model to allow security proofs to directly transfer from the AGM to the GGM (under certain conditions). Our framework supports multiple formalisms and thus allows for easier proof-writing in the AGM. It further resolves all of the logical discrepancies that remained in Fuchsbauer et. al.'s AGM framework. Joint work with Prof. Joseph Jaeger.
2. **Memory-less Brute Force Resistant Biometric Key Storage/Retrieval** (*Submitted*): We create a biometrics-based key storage/retrieval system that does not require the user to remember any secret information beyond their own biometric template. We use a combination of Fuzzy Vaults and Oblivious Pseudorandom Functions. Our scheme is provably secure against both online and offline brute force in a variety of corruption scenarios. Joint work with Prof. Sasha Boldyreva and Tianxin Tang. A Rust implementation of the scheme using the `voprf` and the `RustCrypto` crates is available here. A poster for this work was presented at the RSA Conference 2024.
3. **Secure Identity Verification Using Cloud Services and FHE** (*Master's thesis*): Created a prototype for a practically deployable identification platform that delegates all computation and storage to third-party nodes. In collaboration with Prof. Srinivas Vivek as a part of the Modular Open Source Identity Platform (MOSIP). Accepted as a talk at the Trustworthy Digital Identity Conference by the Alan Turing Institute, London. We implement the protocol in C++ using the Microsoft SEAL FHE library. A copy of the successfully defended thesis can be found here.

4. **Modelling prejudice and its effect on societal prosperity**: Created an agent-based model to simulate inter-group prejudice in society, and used it to study the changes/disparities that may arise among groups over time. Research conducted in collaboration with Prof. Shrisha Rao. Paper published in the Journal of Simulation.
5. **TVLA Methodology:** Created a Python implementation of the Test Vector Leakage Assessment methodology to analyse power traces from AES-128 implementations for potential DPA side-channel attacks. Work done under Prof. Srinivas Vivek. See technical report here.

Other Research Experience

- Completed a semester of research under Prof. Ashish Choudhury studying Verifiable Secret Sharing in Secure Multi Party Computation and exploring the feasibility of Perfectly Secure VSS protocols in hybrid (synchronous and asynchronous) network settings *(Spring 2021)*.
- Completed a literature survey on AT-free graphs. Covered various results and theorems on AT-Free graphs and also coloring algorithms for these graphs. Final project for CS825 Graph Theory. See final report here *(Spring 2021)*.
- Completed a qualitative research project under Prof. Preeti Mudliar which studies the critical factors for the employability of Indian engineering graduates in IT. See final report here. *(Fall 2020)*
- Completed a research internship under Prof. Dinesh Babu Jayagopi at IIIT Bangalore in the field of Natural Language Processing. Developed a model to generate follow-up questions for HR interviews using OpenNMT, BERT, and ConceptNET. *(Summer 2019)*

TA Experience

OMSCS6260: Applied Cryptography *January, 2025 - present*
Prof. Sasha Boldyreva

OMSCS6260: Applied Cryptography *August, 2024 - December, 2024*
Prof. Sasha Boldyreva

CS6260: Applied Cryptography *August, 2023 - December, 2023*
Prof. Sasha Boldyreva *Head TA*

CS 512: Discrete Mathematics and Computability *September 2021 - January 2022*
Prof. Srinivas Vivek

CS 302: Introduction to Automata Theory *August 2021 - December 2021*
Prof. Shrisha Rao

NPTEL course on Secure Computation *July, 2021 - October, 2021*
Prof. Ashish Choudhury

Academic Service

- **Subreviewer** for the Annual International Conference on the Theory and Applications of Cryptographic Techniques (**EUROCRYPT 2025**).

- **Subreviewer** for the International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT 2024**).
- **Organizing volunteer** for the International Conference on Theory and Practice in Public Key Cryptography (**PKC 2023**).
- **Head student volunteer** for the **IEEE InDIITA Workshop**, Bangalore, 2019.

Awards and Scholarships

- **Nominated as an RSAC Security Scholar** by Georgia Tech. for the year 2024.
- **Enlisted in Dean's Merit List**, IIIT Bangalore, for 5 consecutive years (2017-18, 2018-19, 2019-20, 2020-21, and 2021-22).
- Received a **Scholarship for Academic Excellence** from IIITB in the academic year 2018-19, worth INR 50,000.
- Received a **Post Graduate Scholarship** from the All India Council for Technical Education, worth INR 150,000.
- Received an NSF student stipend award to attend RWC 2025 in Sofia, Bulgaria.
- Received an NSF student stipend award to attend RWC 2024 in Toronto, Canada.
- Awarded a student grant to attend USENIX Security '21 virtually.

Positions of Responsibility

- **Communications Chair of the SCS/SCP GSA** (2023-2024): Serving as the communications chair for the joint Graduate Student Association of the School of Computer Science (SCS) and the School of Cybersecurity and Privacy (SCP) at Georgia Tech.
- **Head of Logistics, Zense@IIITB** (2019-2020): Served as a core member of Zense, IIIT Bangalore's student developers club.
- **Co-founder/Head of DebSoc: Debate Society**, IIIT Bangalore.
- **Master of Ceremonies for *TEDx IIIT Bangalore*** held in March, 2018.

References

Dr. Joseph Jaeger josephjaeger@gatech.edu
Assistant Professor

Dr. Alexandra Boldyreva sasha@gatech.edu
Professor