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

Projects and Publications

1. **May the Force Not be With You: Brute-Force Resistant Biometric Authentication and Key Reconstruction** (*CCS 2025*): 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 Dr. Tianxin Tang. A Rust implementation of the scheme using the `voprf` and the `RustCrypto` crates is available here. This work was also presented at the BioAuthSec workshop at ASIACRYPT 2025. A poster for this work was presented at the RSA Conference 2024.
2. **Generic and Algebraic Computation Models** (*CRYPTO 2024*, Talk): 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.
3. **Proof of Replication Time** *(Ongoing)* We propose a new security definition and protocol for proof of replication time, which has applications in secure outsourced storage and decentralized storage networks like filecoin.
4. **Biometrics AKE** *(Ongoing)* We propose a new biometrics-based authenticated key exchange protocol that offers strong security properties such as brute-force resistance.
5. **Subsettable OPRF** *(Ongoing)* We propose a new OPRF protocol that allows for the generation of multiple OPRF outputs from subparts of a single input. This protocol has potential applications in biometric strengthening.
6. **Secure Identity Verification Using Cloud Services and FHE** (*Master's thesis*, *preprint*): 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.

7. **Modelling prejudice and its effect on societal prosperity**(*Journal of Simulation 2021*): 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.

TA Experience

OMSCS6260: Applied Cryptography *August, 2024 - May, 2025*
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

- **Selected in the Young Scholar Development Program** at CCS 2025 and awarded a travel grant.
- **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.