Mayank
Research Fellow
1145, 1st Floor
Microsoft Research India,
Lavelle Road, Bangalore - 560001

Email-id : **mayank.cse14@iitbhu.ac.in**
Webpage : **mayank0403.github.io**
GitHub : **https://github.com/mayank0403**
Mobile No.: **+91-8901510055**

ACADEMIC DETAILS

- Indian Institute of Technology (BHU), Varanasi, India
  B.Tech in Computer Science and Engineering 2014-18 (GPA: 8.98/10)

PROFESSIONAL EXPERIENCE

- **Secure Multiparty Computation (MPC) with applications to Machine Learning** (Research Fellow)
  Microsoft Research, Bangalore, India `Paper Link`, `Code` and `Webpage`
  Guide: Dr. Nishanth Chandran, Dr. Divya Gupta, Dr. Aseem Rastogi and Dr. Rahul Sharma
  *June 2018 - **Present***
  - Worked on the CRYPTFLOW project which compiles unmodified TensorFlow code to MPC code secure against semi-honest as well as malicious adversaries.
  - In CRYPTFLOW, I worked on the design and implementation of *Aramis* and *Porthos* components. *Aramis* is a generic method that converts any semi-honest secure MPC protocol to a maliciously secure protocol by placing minimal assumptions on trusted hardware. *Porthos* is an efficient semi-honest secure 3PC protocol built over SecureNN [WGC18].
  - Currently working on extending our core-crypto techniques in CRYPTFLOW.

PUBLICATIONS AND MANUSCRIPTS

- *CrypTFlow: Secure TensorFlow Inference*
  *Nishant Kumar[a], **Mayank Rathee**[a], Nishanth Chandran, Divya Gupta, Aseem Rastogi, Rahul Sharma*
  In **submission** to IEEE Symposium on Security and Privacy (**S&P/Oakland**) 2020.
  Available on eprint. Report No. 2019/1049.

  [a] EQUAL FIRST AUTHOR CONTRIBUTORS

- *Efficient Private Database Queries using Ring-LWE Somewhat Homomorphic Encryption*
  *Tushar Saha, **Mayank Rathee**, Takeshi Koshiba*
  Published in the Journal of Information Security and Applications (**JISA** - Elsevier),
  Volume 49, Article 102406, December 2019. Available here.

- *Checking Laws of the Blockchain With Property-Based Testing*
  *Alexander Chepurnoy, **Mayank Rathee***
  In the proceedings of the International Workshop on
  Blockchain Oriented Software Engineering (**IWBOSE**), IEEE 25th International Conference on
  Software Analysis, Evolution and Reengineering (**SANER** 2018), Campobasso, Italy. Available here.

- *Efficient Protocols for Private Database Queries*
  *Tushar Saha, **Mayank**, Takeshi Koshiba*
  In the proceedings of the 31st Annual IFIP WG 11.3 Conference on
  Data and Applications Security and Privacy (**DBSec** 2017), Philadelphia, PA, USA. Available here.

- *Private Comparison Protocol and Its Application to Range Queries*
  *Tushar Saha, **Mayank**, Deevashwer, Takeshi Koshiba*
  In the proceedings of the 10th International Conference on
  Internet and Distributed Computing System (**IDCS** 2017), Fiji. Available here.

- *Part-of-Speech Tagging of Bhojpuri Data*
  ***Mayank**, Deevashwer, Janvijay Singh, Anil Kumar Singh*
  Manuscript available here.

INTERNSHIPS AND MAJOR PROJECTS

- **Blockchain protocols and Scorex** (Internship)
  Tanaka Lab, Tokyo Institute of Technology, Japan — `Paper Link` and `Talk PPT`
  Guide: Prof. Keisuke Tanaka and Alexander Chepurnoy, May-July 2017 (3 months)
  - Contributed to the Scorex project (my contributions are available here)—a modular blockchain design framework by IOHK—and extensively investigated the existing proof-of-stake based blockchain proposals.
  - Defined property tests to check for soundness of blockchain implementations.

- **Efficient protocols for threshold queries over encrypted databases** (Internship)
  Foundations of Cryptography Lab, Saitama University, Japan — `Paper Link`
  Guide: Prof. Takeshi Koshiba, May-July 2017 (3 months)
  - Developed an integer packing method for Ring-LWE (RLWE) based homomorphic encryption that enables batched comparisons and used it for building an encrypted database system supporting both equality and threshold queries.
  - Implemented complex cryptographic methods like relinearization and modulus switching in the context of RLWE based homomorphic encryption schemes.

- **Querying over encrypted databases using Homomorphic Encryption** (Internship)
  Foundations of Cryptography Lab, Saitama University, Japan — `Paper Link`
  Guide: Prof. Takeshi Koshiba, Dec 2016 - Jan 2017 (1.5 months)
  - Implemented a scalable encrypted database system, using RLWE based somewhat homomorphic encryption, that supports large equality queries. The code was written in C++ using PARI library.
  - Also implemented secure comparison protocols (including this) in C++ (with PARI).

- **Encrypted computation using Homomorphic Encryption** (Project)
  OpenMined (Remote) and Indian Institute of Technology (BHU), Varanasi — Links: `PyAono` and `PyYashe`
  Guide: Andrew Trask (UOxford) and Prof. KK Shukla, Jan-Dec 2017 (12 months)
  - Wrote C++ implementations and developed Python API of homomorphic encryption schemes supporting operations like key rotation. Worked on BV [LNV11], YASHE [BLLN13] and Aono et al.'s [AHPW15] homomorphic schemes.

- **Development and analysis of Public-Key Cryptography** (Training)
  Defense Research and Development Organization, New Delhi (SAG) — `Report Link`
  Guide: Dr. Saibal Pal, May-Aug 2016 (3.5 months)
  - Implemented public-key encryption schemes, integer factorization algorithms and studied Number Field Sieve with a focus on CADO-NFS software.

- **Part-of-Speech Tagging of Bhojpuri language data** (Project)
  Indian Institute of Technology (BHU), Varanasi — `Manuscript Link`
  Guide: Dr. Anil Kumar Singh, Jan-Oct 2016 (9 months)
  - Implemented and analyzed the results of Part-of-Speech Tagging of Bhojpuri language data using tools like MaxEnt, CRF++, SVMStruct, and Trigrams & Tags.
  - A performance comparison was also made with the Hindi language for each of the taggers.

TEACHING EXPERIENCE AND UNDERGRADUATE PROJECT MENTORSHIP

- **CSE-202: Artificial Intelligence**
  Teaching Assistant | Semester VIII — `GitHub Link`

- **CSE-291: Exploratory Project**
  Project Mentor | Semester VIII

REVIEWING EXPERIENCE AND SERVICE

- **Cryptography**
  ASIACRYPT'19: Sub-reviewer
  INDOCRYPT'19: Sub-reviewer

- **Software Engineering**
  ISEC'19: Sub-reviewer

NOTABLE COURSE PROJECTS AND OTHER INFORMAL PROJECTS

- [Mentoring CSE-202: AI] Developed an encrypted and automated assignment evaluation system for undergrad AI course using GnuPG and GitHub. Link
- Implemented Rabin OT, 1-out-of-2 OT and Feige Fiat Shamir ZKP in Sage Math. GitHub Link
- Developed a project management system for my institute using Django. GitHub Link
- Implemented a relational algebra DBMS engine in C++. GitHub Link
- Implemented a shell program in C++ with functionalities like redirection and pipelining. GitHub Link

RELEVANT COURSES TAKEN

- **Indian Institute of Technology (BHU), Varanasi**
  Information Security
  Network Security
  Theory of Computation
  Data Structures
  Algorithms
  Probability and Statistics
  Computer Architecture
  Compiler Design
  Stochastic Process
  Operating Systems
- **Indian Institute of Science, Bangalore**
  Theoretical Foundations of Cryptography (*Audited*) Webpage