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)

Semester	I	II	III	IV	V	VI	VII	VIII
SPI[a]	8.59	7.26	9.20	9.00	9.22	9.36	**10.00**	9.51
YGPA[b]	7.92		9.12		9.29		9.77	

[a] Semester Performance Index $\approx$ Semester GPA
[b] Yearly GPA, Fall and Spring Semester combined

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.

  [a] **`Equal First Author Contributors`**

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

- *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.

- *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.

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

PROFESSIONAL EXPERIENCE

- **Secure Multiparty Computation 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-Present 2018-19 (1.6 years)
  - Worked on design and implementation of `Aramis` component – a generic method that converts any semi-honest secure MPC protocol to a maliciously secure protocol – of `crypTFlow` project which a system that compiles unmodified TensorFlow code to MPC code secure against both semi-honest and malicious adversaries.
  - Also worked on `Porthos` which is an efficient semi-honest secure 3PC protocol.

MAJOR INTERNSHIPS AND PROJECTS

- **Cryptocurrency 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 cryptocurrency framework by IOHK – and extensively investigated the existing proof-of-stake cryptocurrencies.
  - Formalized essential requirements for blockchain implementations to be sound.

- **Secure and 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 Homomorphic Encryption that supports SIMD integer 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 Ring-LWE based Homomorphic Encryption schemes.

- **Querying over encrypted databases using Somewhat Homomorphic Encryption** (Internship)
  Foundations of Cryptography Lab, Saitama University, Japan — `Paper Link`
  Guide: Prof. Takeshi Koshiba , Dec-Jan 2016-17 (1.5 months)
  - Implemented an encrypted database system supporting equality queries and implemented secure comparison protocols in C++ using PARI library, based on somewhat homomorphic encryption.

- **Encrypted computation using Homomorphic Encryption** (Project)
  Open Mined (Remote) — GitHub Links: `PyAono` and `PyBV`
  Project Mentor: Andrew Trask (University of Oxford), Aug-Dec 2017 (5 months)
  - Wrote C++ implementations and developed Python API (with PARI library) of common Homomorphic Encryption schemes supporting operations like Key Rotation. Worked on BV, YASHE and Aono et al.'s 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 Cryptography Schemes, Integer Factorization algorithms and studied Number Field Sieve with 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 POS Tagging of Bhojpuri language data using MaxEnt, CRF++, SVMStruct and Trigrams & Tags. A performance comparison was also done with 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

- **CSE-392: UG 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 submission and 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`

CRYPTOGRAPHY/SECURITY: RELEVANT COURSES TAKEN

- **IIT (BHU), Varanasi** (*Computer Science Courses*)
  INFORMATION SECURITY[a] | Instructor: Prof. Kaushal Kumar Shukla
  NETWORK SECURITY[a] | Instructor: Prof. Kaushal Kumar Shukla
  THEORY OF COMPUTATION[b] | Instructor: Prof. Lavanya Selvaganesh

  [a] Highest Grade Awarded
  [b] Second Highest Grade Awarded

- **IISc, Bangalore**
  THEORETICAL FOUNDATIONS OF CRYPTOGRAPHY (*Audited*) | Instructors: Prof. Bhavana Kanukurthi and Dr. Nishanth Chandran
  Received **full** marks on problem set.