

Mayank

Room number 180,

Morvi Hostel,

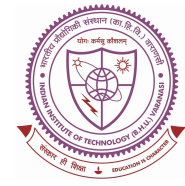
IIT BHU, Varanasi - 221005

Email-id : mayank.cse14@iitbhu.ac.in

Webpage : [mayank0403.github.io](https://github.com/mayank0403)

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 (Current GPA: 8.92/10)

Semester	I	II	III	IV	V	VI	VII	VIII
SPI	8.59	7.26	9.20	9.00	9.22	9.36	10.00	-
YGPA	7.92		9.12		9.29		-	

- Bharat Mata Saraswati Bal Mandir School, New Delhi
All India Senior School Certificate Examination | Score: 92.6%
- Model School, Rohtak
Central Board of Secondary Education (CBSE) Examination (CGPA: 10)

PUBLICATIONS

- 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.
- 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.
- Checking Laws of the Blockchain: Property-Based Testing of Blockchain Systems*
Alexander Chepurnoy, **Mayank**
To be submitted

FIELDS OF INTEREST

- Algorithms, Functional Programming, Number Theory, Cryptography, Cryptocurrency technologies and Homomorphic Encryption

TECHNICAL SKILLS

- Languages** (C, C++ (with specialisation in GNU GMP and PARI/GP), Java, Scala, Python), **Database** (MySQL), **Tools** (Eclipse, L^AT_EX, XCode, IntelliJ Idea), **Technologies** (Bitcoin, Scorex)

MAJOR INTERNSHIPS AND PROJECTS

- Cryptocurrency protocols and Scorex** (Internship)
Tanaka Lab, Tokyo Institute of Technology, Japan
Guide: Prof. Keisuke Tanaka, May-July 2017
 - Actively contributed to the Scorex project (my contributions are available on the Github page of the project) - A modular cryptocurrency framework by Input-Output Hong Kong, China, and extensively investigated the existing proof-of-work and proof-of-stake cryptocurrencies.
- Secure and efficient protocols for threshold queries over encrypted databases** (Internship)
Foundations of Cryptography Lab, Saitama University, Japan
Guide: Prof. Takeshi Koshiba, May-July 2017

- Developed an efficient secure integer comparison protocol to facilitate secure and practical threshold queries over encrypted databases using Somewhat Homomorphic Encryption and a multiparty secure sorting method. Implemented complex cryptographic protocols and a Fully Homomorphic Encryption scheme based on Ring-LWE.
- **Querying over encrypted databases using Somewhat Homomorphic Encryption (Internship)**
 Foundations of Cryptography Lab, Saitama University, Japan
Guide: Prof. Takeshi Koshiba, Dec-Jan 2016-17
 - Developed an encrypted database system supporting equality queries and implemented secure comparison protocols in C++ using PARI library, based on somewhat homomorphic encryption.
- **Decentralized Encrypted Neural Networks (Project)**
 Open Mined, United Kingdom (Remote)
Project Mentor: Andrew Trask (University of Oxford), Aug-Present 2017
 - Working on C++ implementations and Python API development (with PARI library) of core Cryptographic functions to support prediction tasks on encrypted Neural Networks. Already developed major cryptographic functions for BV, YASHE and Aono et al.'s homomorphic schemes (can be found on GitHub).
- **Development and analysis of Public Key Cryptography (Internship)**
 Defense Research and Development Organization, New Delhi (SAG)
Guide: Dr. Saibal Pal, May-Aug 2016
 - Implemented Public Key Cryptography Schemes, Integer Factorization algorithms and studied Number Field Sieve with focus on CADO-NFS software.
- **Encrypted Machine Learning (B.Tech Thesis Project)**
 Indian Institute of Technology (BHU), Varanasi
Guide: Prof. K. K. Shukla (HoD), Jan-Present 2017
 - Working on encrypted neural networks based on somewhat homomorphic encryption and already implemented secure logistic regression using somewhat homomorphic encryption (using SEAL library).
- **Part-of-Speech Tagging of Bhojpuri language data (Project)**
 Indian Institute of Technology (BHU), Varanasi
Guide: Dr. Anil Kumar Singh, Jan-Oct 2016
 - 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 MENTOR

- **CSE-202: Artificial Intelligence**
 Teaching Assistant | Semester VIII (Fall Semester 2018)
- **CSE-291: Exploratory Project**
 Project Mentor | Semester VIII (Fall Semester 2018)
- **CSE-392: UG Project**
 Project Mentor | Semester VIII (Fall Semester 2018)

COURSE PROJECTS AND OTHER INFORMAL PROJECTS

- Developed a Project Management System for the Institute using Django.
- Implemented a Relational Algebra DBMS Engine in C++.
- Implemented a shell program in C++ with functionalities like redirection and pipelining.
- Implemented multiple numerical algorithms including linear system solvers like Gauss- Jordan eliminations and Gauss-Siedel method; polynomial solvers like Secant Regula- Falsi and Newton-Raphson; Lagrange's method of interpolation; and Trapezoidal rule of integration in Python using Numpy and illustrated the results in Matplotlib.
- Developed a Unity-based game for Windows OS and used socket connections between an Android phone and a PC to manoeuvre objects in the game.

- Wrote and implemented a flight search algorithm in Java to search for the cheapest flights in a database.
- Made and implemented Othello (Reversi) game (like checkers and chess) with GUI in JAVA

ACADEMIC ACHIEVEMENTS, CO-CURRICULAR AND EXTRACURRICULAR ACTIVITIES

- Stood amongst top 2% candidates in JEE Advanced 2014.
- Secured an All India Rank of 40 in National Cyber Olympiad 2005.
- Google AdWords certified.
- Position of Responsibility: Worked as a member in the Organizing Committee of the IIT BHU MUN-2014.
- Active on competitive coding platforms and contests.
- Got 222/9053 rank in CodeChef SnackDown Online Qualifier 2016.