Rachit Parikh

Email: rachit.parikh4@gmail.com
Personal Website

Education

ISI Kolkata West Bengal, India
Master of Technology - Cryptology and Security *Sep 2021 - June 2023*

Courses: *Operating Systems, Data Structures, Algorithms, Cryptology, Privacy, Security, Networking, Databases*

IIT Roorkee Uttarakhand, India
Bachelor of Technology - Mechanical Engineering *July 2016 - June 2020*

Courses: *Optimization, Numerical Methods, Programming with C++, Linear Algebra, Calculus*

Skills

Languages:	C, C++, Java, Python, SQL
Tools & Frameworks:	Spring, NLTK, Jekyll, Docker, GIT, MySQL

Experience

COSIC, KU Leuven Leuven, Belgium
Research Intern (Master's thesis) *Feb 2023 - Present*

- Designed a novel **privacy-preserving protocol** with **offline key management**, and compatibility with the publish-subscribe model, incorporating **broadcast encryption** and **zero-knowledge proofs** for secure data sharing

Société Générale Bangalore, India
Software Engineer *Aug 2020 - Sep 2021*

- Made enhancements in Calypso for the back office operations in private banking segment of Luxembourg and Monaco. Daily tasks included writing **unit tests**, handling process pipeline for **continuous integration** and delivery, completing **user stories**. Got acquainted with **agile** process for software development and **Test driven development**.
- Used **Java** for Calypso codebase, **Jenkins** for facilitating continuous integration, ensured green coding practices which later got merged into production.

Mercedes Benz Research and Development India Bangalore, India
Research Intern *May 2019 - Aug 2019*

- Predicted the state of charge of an electric bus during recalibration using machine learning in **Python**
- Created a script that would automate the process of data conversion and cleaning and training

Achievements

- Secured an **All India Rank of 2016** in **JEE Advanced 2016** out of **150,000+** candidates
- Recepient of **M.Tech fellowship** from the Government of India
- Awarded a monthly **scholarship** of **€2550** for pursuing Master's thesis in KU Leuven as an **international scholar** for 6 months

Projects

Randomness Testing using Boolean functions: Designed an algorithm that can efficiently find the Boolean function with the best z-score for a given sequence of data. The algorithm developed provides significant improvement over the existing *BoolTest* algorithm which is a heuristic based algorithm to find randomness. The paper has been published in Indocrypt 2022

Elliptic Curve Diffie Hellman: Implemented ECDH in C++. For the field arithmetic, Karastuba for multiplication and Barret's reduction for modular operations for 256 bit integers were used.

Phrase extraction from paragraph: Created a tool that would extract parse trees based on the phrase types and traversal will give list of noun, propositional and verb phrases in the paragraph. NLTK and stanza were used.

Huffman Coding for Compression: Developed an end-to-end compression-decompression tool that employs Huffman coding to optimally compress data in C++.

Is my scrolling random?: Tracked my trackpad movements using Python and then applied statistical tests on the coordinate frequency data and concluded non-randomness in the movements.

Publications

1. Chatterjee, Bikshan, Rachit Parikh, Arpita Maitra, Subhamoy Maitra, and Animesh Roy. "Revisiting BoolTest–On Randomness Testing Using Boolean Functions." In Progress in Cryptology–INDOCRYPT 2022: 23rd International Conference on Cryptology in India, Kolkata, India, December 11–14, 2022, Proceedings, pp. 471-491. Cham: Springer International Publishing, 2023.
2. R. Parikh, N. Sharma and A. Bansal, "Lossy compression of climate data using principal component analysis," 2019 International Conference on Nascent Technologies in Engineering (ICNTE), Navi Mumbai, India, 2019, pp. 1-3, doi: 10.1109/ICNTE44896.2019.8945947.

Extra-Curricular

- Placement Representative at ISI Kolkata
- Taught underprivileged children as a part of NSS IIT Roorkee
- Participated in the Inter-IIT Tech meet at IIT Bombay '18