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 Summary

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

Experience

- **Computer Security and Industrial Cryptography group - KU Leuven** Leuven, Belgium
  Research Intern (Master's thesis) *Feb 2023 - Aug 2023*
  - **Literature Review**: Review of current state-of-the-art protocols used in industrial IoT settings or in distributed systems
  - **Design of a new protocol**: Designed a new practically feasible protocol that is privacy-preserving, has offline key management and is tailored specifically for the IoT environment
  - **Protocol**: The protocol is a broadcast encryption protocol which uses zero knowledge proofs for proving membership and is compatible with the publish-subscribe model and can be implemented over MQTT Protocol

- **TCG Crest** Kolkata, India
  Intern *May 2022 - Aug 2022*
  - **Randomness Testing for QRNG**: Used Entroy test and *BoolTest* on the data generated by a Quantum random number generator device to test the randomness of a sequence. Compared the results obtained on the QRNG device with the Humboldt and ANU datasets.

- **Société Générale** Bangalore, India
  Software Engineer *Aug 2020 - Sep 2021*
  - **Calypso Data Warehouse Team**: 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.
  - **Green Coding**: Apart from reducing the technical debt, application of green coding practices was ensured. Enhancements were made in the Calypso codebase to improve the green code rating and it was later merged with the production code.
  - **Technology**: Java, Spring, JUnit, Jenkins, Bash

- **Mercedes Benz Research and Development India** Bangalore, India
  Research Intern *May 2019 - Aug 2019*
  - **Problem Statement**: Prediction of battery state of charge for an electric bus.
  - **Modeling**: Automated the process of data processing and the change in state of charge was modeled using machine learning.

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
- **Double Ratchet Algorithm**: Implemented Double Ratchet algorithm used by WhatsApp and Signal. Cryptography package available in Python was used to implement this.
- **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++.

Publications

- **Paper**: 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.

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 **scholarship** for pursuing Master's thesis in KU Leuven as an **international scholar**

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