Rachit Garg | CS14B050

rachit0596@gmail.com • github.com/RachitG54

Academic Qualifications

Program	Institution	%/GPA	Year of Completion
B.Tech and M.Tech in Computer Science And Engineering	Indian Institute Of Technology Madras	9.32/10	2019
XII	Delhi Public School, Faridabad, Haryana	97/100	2014
X	Delhi Public School, Faridabad, Haryana	10/10	2012

Patents and Publications

- Prioritization in a permissioned blockchain - Rachit Garg, Seep Goel, Abhishek Singh, Praveen Jayachandran, Mudit Verma. Patent filed in **US Patent Office** on January 2018 by IBM Research. Docket - P201704237US01.
  Research paper was submitted and **accepted** at ACM/IFIP International Middleware Conference 2018 - Rennes, France.

Internship

- **IBM Research** — **New Delhi, India**
  Industry Research — *(May 2017 - April 2018)*
  - Researched the problem of fair scheduling of transactions that are submitted to a permissioned blockchain system.
  - Proposed a weighted fair queueing strategy for ordering transactions that can support differentiated quality of service on the blockchain.
  - Implemented on a blockchain network using Hyperledger Fabric version 1.0. **Patent filed**.
- **Purdue University** — **Indiana, USA**
  Purdue Undergraduate Research Experience — *(May - July 2016)*
  - Researched in the field of applied cryptography. Main goal of the project was to prevent leakage of access patterns when accessing information from a cloud network (Oblivious RAMs). Studied this problem in a distributive computing setting.
  - Essentially a data structures problem, which required intelligent shuffling of data to prevent leakage of information.
  - Guides: Prof. Aniket Kate (Purdue University), Dr. Srivatsan Ravi (Purdue University).
- **Paytm** — **Chennai, India**
  Industry Research — *(June 2018)*
  - Studied the multiple aspects and nuances of data protection and privacy.
  - Provided a memoranda on recommendations for formulating the personal data privacy framework for India. Submitted a report to the Ministry of Electronics & IT, India.

Research Projects

- **Searchable and Computable Encryption** — **IIT Madras & IIT Bombay, India**
  Undergraduate Research Course — *(February 2017 - October 2018)*
  - Constructed, implemented cryptographic multi-party protocols for efficient statistical analysis on large encrypted databases.
  - Cryptographic primitives of Searchable Symmetric Encryption(SSE), Additive Homomorphic Encryption(AHE), Yao's garbled circuits were used.
  - Submitted a **research paper** to IEEE S&P Conference 2019. Acceptance awaited.
  - Guides: Prof. Shweta Agrawal (IIT Madras), Prof. Manoj Prabhakaran (IIT Bombay).
- **Lattice Cryptography** — **IIT Madras, India**
  Dual Degree Thesis Project — *(June 2018 - Ongoing)*
  - Surveyed the construction of cryptosystems based on assumptions related to lattices. Summarized and gave a talk on constructions based on cyclic lattices.
  - Researching on possible ideas that can improve constructions to the primitive of Identity Based Encryption(IBE).
  - Guide: Prof. Shweta Agrawal (IIT Madras).

Scholastic Achievements

- Secured **All India Rank 326 in JEE(Advanced)** and **All India Rank 176 in JEE(Mains)**. *(2014)*
- Acquired a **perfect GPA** of 10 in eighth semester and a **second highest GPA** of 9.9 in first semester. *(2018, 2014)*
- Cleared **Indian National Mathematics Olympiad(INMO)** 2013. Trained by the National Board of Higher Mathematics (NBHM). Selected for **senior batch** by clearing postal coaching in 2014. *(2013, 2014)*
- Received **Kishore Vaigyanik Protsahan Yojna Fellowship Award**. *(2013)*
- Qualified for **scholarship** by clearing **National Talent Search Examination(NTSE)** and continues to receive the scholarship. *(2010 - Ongoing)*
- Cleared **National Standard Examination in Junior Science(NSEJS)**. *(2012)*

Workshops

- Attended **IMOTC at Homi Bhabha Centre for Science and Education(HBCSE).** *(May - June 2013)*
  - Among 30 students all over India to receive training in advanced mathematics.
  - Attended lectures in Geometry, Number Theory, Combinatorics, Algebra by distinguished professors.
- Participated in **Lattice Algorithms and Cryptography** workshop held at IIT Kanpur. *(December 2017)*
  - The event included talks based on recent developments in theoretical computer science with respect to lattice cryptography and algorithms.
- Attended the **Theory of Cryptography Conference(TCC)** 2018 held in Goa, India. *(November 2018)*

Development Projects

- Designed a **Code Obfuscator** for C language. Guide: Prof. Rajsekar Manokaran (IIT Madras). *(July - November 2016)*
  - Obfuscated programs to pass plagiarism detection under the MOSS(Measure Of Software Similarity) system.
  - Implemented ideas based on a research paper and wrote a context free grammar for a mini version of C and used gotos and random hashes to obfuscate a C code.
- Theorized and implemented a new **block cipher** scheme. Guide: Prof. Chester Rebeiro (IIT Madras). *(January - May 2017)*
  - Suggested new substitution boxes and permutation layers.
  - Implemented block cipher using C and performed security, efficiency analysis.
- Designed modules for **kernel clustering** in python. Guide: Prof. C. Chandra Sekhar (IIT Madras). *(Jannuary - May 2017)*
  - Transformed clustering algorithms such as k-means clustering to work in different kernel spaces.
  - Visualized the clustering on 2-dimensional data of non linearly separable classes and contrasted different kernels.
- Showcased a project in **Envisage, part of the technical fest of IIT Madras**. *(August - November 2015)*
  - Built a mechanical wire structure called **Lumarca (9 feet by 6 feet by 6 feet)** that could **model 3-D patterns** effectively. Implemented vector equations to model 3-D objects.
  - Used Processing (Java based open source programming software) and created a 3-D music visualizer.
  - Project witnessed a footfall of 8000 students over two days.

Co-Curricular Activities

- Selected for **ACM-ICPC Regionals** in 2015 and attended two regionals in 2016. *(2015, 2016)*
- Represented the hostel and secured third place in the **techsoc, Online Programming Contest** at IIT Madras. *(2018)*
- Developed successful applications in 2015 in **Microsoft Code.Fun.Do Hackathon** and implemented facial detection, recognition algorithms for verifying idenities in **LynkHacks hackathon**. *(2015, 2017)*

Key Course Work (*Ongoing)

- **Theoretical Computer Science:** Foundations of Cryptography, Lattice Algorithms, Approximation Algorithms, Matching and Network flow Algorithms, Pseudorandomness, Automata theory, Complexity theory*, Algorithmic Approaches to Computational Biology*.
- **Mathematics:** Tools in Combinatorics, Game Theory, Graph Theory, Linear Algebra, Calculus.
- **Systems:** Applied Cryptography, Computer Networks, Concurrent Computing, Compiler Design.
- **Intelligent Systems:** Machine Learning, Kernel Methods for Pattern Recognition.
- **Lab courses:** Basic and Advanced Programming Lab, Compiler Design Lab, Operating System Lab, Assembly Language Lab.

Technical Skills

- **Programming Languages:** Proficient in: C, C++, Java, Python, Matlab, Arduino, LaTeX. Basic ability with: Assembly, Verilog, HTML5. If needed: can readily adapt to a new language.
- **Text Editors:** Comfortable with sublime, gedit, vim, eclipse.

Positions of Responsibility

- **Teaching Assistant:** Foundations of Cryptography, an introductory course in cryptography, designed to focus on building a theoretical base for cryptographically secure constructions.
- Coordinator at Shaastra 2016. Part of Envisage, responsible for organizing **India's largest student organized techno-cultural show.**
- **Chess team captain** for Ganga Hostel, IIT Madras.

Extra Curricular Activities

- Enthusiastic chess player.
  - As captain, guided team to Bronze medal in **Deans Trophy Chess, IIT Madras**.
  - In 2008, **Represented State at National Level**, Secured 3rd position in Haryana state games for Chess.
  - Secured 1st position in 2009 and 2008 while competing in **CBSE north zone II Chess tournament** in senior and junior category respectively.