Rahul B S

Bengaluru, India

(+91) 7019810875 | rahulbs1798@gmail.com | rahulbs98.github.io | rahulbs98 | rahul-bs | @RahulBS1998 | bsrahul

“We are what we repeatedly do. Excellence, therefore, is not an act, but a habit.”

Education

Birla Institute of Technology and Science Pilani — *Goa, India*

B.E. in Electronics and Instrumentation, M.Sc. in Mathematics, CGPA : 6.95/10.0 — *Aug. 2016 - Aug. 2021*

Relevant Courses : Number Theory, Algebra, Optimisation, Graph Theory, Microprocessors, Complex Analysis, Discrete Mathematics

Experience

QED-IT Systems — *Dec. 2020 - Present*

Cryptography Research Intern - Freelance Consultant — *Tel Aviv, Israel*

Center for Research in Applied Cryptography and Cyber Security, Bar Ilan University — *Aug. 2020 - Present*

Research Intern - Remote — *Tel Aviv, Israel*

Blockchain Group, IBM India Research Labs — *May 2020 - July 2020*

Summer Research Intern — *Bengaluru, India*

Birla Institute of Technology and Science Pilani — *Aug. 2019 - Dec. 2019*

Undergraduate Teaching Assistant - Algebra — *Goa, India*

Society of Electronic Transactions and Security — *May 2019 - July 2019*

Summer Intern — *Chennai, India*

Institute of Mathematical Sciences — *Dec. 2018 - Jan 2019*

Visiting Student — *Chennai, India*

International Institute of Information Technology — *May 2018 - July 2018*

Summer Intern — *Bengaluru, India*

Relevant Projects

Efficient circuit construction and implementation for the distributed BFV-FHE scheme — *QED-it Systems*

Advised by : Daniel Benarroch, Michael Adjedj — *Dec. 2020 - Current*

- Understanding benchmarks set for the BFV-FHE Scheme with RNS Optimisations, through implementations in Lattigo library
- Working on generating efficient usable circuits for comparison that can be used in homomorphic sorting and searching.

Efficient protocols for Two-Sided Private Set Intersection(PSI) Sum with Cardinality — *BIU Cyber Center*

Advised by : Prof. Carmit Hazay (Bar-Ilan Univ.), Prof. Muthu Venkitasubramaniam (Univ. Of Rochester) — *Jan. 2021 - Current*

- Exploring possible methods to achieve 2-sided Malicious PSI protocols that can be extended to PSI-Sum with Cardinality problem
- Looking into efficient instantiations of primitives like Shuffled Distributed OPRF, Bloom Filters, etc..

Efficient methods for Distributed RSA Modulus generation and testing — *BIU Cyber Center*

Advised by : Prof. Carmit Hazay (Bar-Ilan Univ.), Prof. Muthu Venkitasubramaniam (Univ. Of Rochester) — *Aug. 2019 - Dec. 2020*

- Exploring possible efficient methods to improve theoretical bounds of soundness of the Boneh-Franklin test
- Investigating approaches from MPC and Number Theory for generating RSA modulus in a distributed setting as a product of two safe primes.

Non-Interactive Proof Generation from Interactive Zero Knowledge Protocols — *IBM Research*

Advised by : Dr. Dhinakaran Vinayagamurthy, Nitin Singh — *May 2020 - Aug. 2020*

- Designed a modular framework for Interactive Zero Knowledge Protocols which was used to convert it to a non-interactive protocol.
- Implemented additional features for the design to support oracles, protocol composition, etc.. and tested existing protocols like Ligero on it

Security Analysis of exisiting Beyond Birthday Bound Authentiation Schemes — *SETS India*

Advised by : Dr. Jothi Ramalingam — *May 2019 - Aug. 2019*

- Cryptanalysis techniques on Beyond Birthday-Bound Secure claimed MAC schemes such as EWCDM, etc..

Academic Projects

Secure Assisted Universally Blind Quantum Computation — *Aug 2019 - May 2020*

Advised by : Prof. Radhika Vatsan(BITS Pilani), Report — *Academic Project*

Random Graphs & Applications in Cryptography — *Aug. 2018 - May 2019*

Advised by : Prof. Tarkeshwar Singh (BITS Pilani), Report — *Academic Project*

Conferences and Workshops

Feb'20	10th BIU Winter School of Cryptography	*BIU, Israel*
Jan'20	Secure Multi Party computation: Theory and Practice	*IISc., India*
May'18	Summer School in Theoretical Computer Science	*IMSc., India*

Skills

Technical C++, GoLang, Rust, Python, Java, Matlab, SAGE, PARI-GP, LaTeX

Certifications

2020	Complete Modern C++(11/14/17) - Udemy
2020	Algorithmic Toolbox (University of California, San Diego) - Coursera
2020	Object-Oriented Data Structures in C++ (University of Illinois - Urbana Champaign) - Coursera
2020	The RUST Programming Language - Udemy
2019	Cryptography-1 (Stanford University) - Coursera

Positions of Responsibility

Student Volunteer - Web Development *India*
IEEE ANTS 2019 *May. 2019 - Dec. 2019*

Mentor - Cryptography *India*
Quark Summer Technical Program *May 2019 - Aug. 2019*

Coordinator *India*
BITSKrieg (Cybersecurity Club), BITS Goa *May 2018 - May. 2019*

Mentor - Ethical Hacking and Penetration Testing *India*
Quark Summer Technical Program *May 2018 - Aug. 2018*

Core Member *Goa, India*
Quark 2018 Controls *May 2017 - May 2018*

Part Time Associate *India*
National Agenda Forum *May 2017 - Dec. 2017*

Other Relevant Activities

- Part of a Reading Group discussions advised by Prof. Muthu and Prof. Carmit on research developments in cryptography
- Reading course in Algebraic Number Theory advised by Prof. Vijay Patankar
- Taken up various projects with Prof. Anupama to look into recent FPGA implementations of symmetric cryptographic primtives.

References

- Daniel Benarroch, QED-IT systems, Israel - Email ID
- Prof. Carmit Hazay, Bar Ilan University, Israel - Email ID
- Dr. Dhinakaran Vinayagamurthy, IBM Research, India - Email ID
- Prof. Muthu Venkitasubramaniam, Univ. Of Rochester, US - Email ID