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 — *Aug. 2016 - Aug. 2021*

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

Skills

Technical C++, Rust, Python, Java, C, Matlab, SAGE, LaTeX, Cadence, Verilog

Experiences

UCL Crypto Group, Université Catholique De Louvain — *Louvain-la-Neuve, Belgium*

Research Intern - Advisor : Prof. Francois-Xavier Standaert — *Aug. 2020 - Present*

- Analysing possible hardware implementations of leakage-resilient TBC-based authenticated encryption schemes

Blockchain Group, IBM India Research Labs — *Bengaluru, India*

Summer Research Intern - Advisors : Dr. Dhinakaran Vinayagamurthy, Nitin Singh — *May 2020 - July 2020*

- Designed a modular framework for Interactive Zero Knowledge Protocols which was used to convert it to a non-interactive protocol.
- The design seamlessly supports nesting protocols as sub protocols, oracle-type messages.

Society of Electronic Transactions and Security — *Chennai, India*

Summer Intern — *May 2019 - July 2019*

- Cryptanalysis techniques on Beyond Birthday-Bound Secure claimed MAC schemes such as EWCDM, etc..
- Theoretically and practically analyzed the Encrypted Wegmen-Carter MAC scheme and H-coefficients technique.

International Institute of Information Technology — *Bengaluru, India*

Summer Intern — *May 2018 - July 2018*

- Worked on integrating the HElib-MP Library to the HEAT API by analysing differences between HElib and HElib-MP.

Projects

Efficient methods for Distributed RSA Modulus generation and testing — *Remote Work*

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

- Investigating existing methods for generating RSA Modulus in a distributed setting for certain applications like construction of VDFs.
- Exploring different ways to increase the theoretical soundness of existing methods such as Boneh-Franklin's Biprimality Test

Efficient Hardware-based Symmetric Cryptographic Implementations — *Academic Project*

Advised by : Prof. K R Anupama (BITS Pilani) — *Aug 2019 - May 2020*

- Implementation and analysis of ciphers GIMLI and PRESENT on FPGA and ARM Microcontroller, to compare their efficiency

Secure Assisted Universally Blind Quantum Computation — *Academic Project*

Advised by : Prof. Radhika Vatsan(BITS Pilani) — *Aug 2019 - May 2020*

- A study based project inspecting quantum protocols which provide fully private assisted quantum computation.

Random Graphs & applications in Cryptography — *Academic Project*

Advised by : Prof. Tarkeshwar Singh (BITS Pilani) — *Aug. 2018 - May 2019*

- Surveyed exisiting applications of Random Graphs in Cryptography, in particular, constructions of hash functions which use Random Graphs

Conferences and Workshops

Aug'20	Crypto	*Virtual*
Jun'20	Theory and Practice of Multiparty Computation	*Virtual*
May'20	Eurocrypt	*Virtual*
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*

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
2018 Classical Cryptosystems and Core Concepts (University of Colorado) - Coursera
2017 Certification in Network Management, Nettech Pvt. Ltd.

Positions of Responsibility

Undergraduate Teaching Assistant - Algebra *India*
BITS Pilani *Aug. 2019 - Dec. 2019*

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*

References

- Prof. Carmit Hazay, Bar Ilan University, Israel - Email ID
- Dr. Dhinakaran Vinayagamurthy, IBM Research, India - Email ID
- Nitin Singh, IBM Research, India - Email ID
- Dr. Shilpa Gondhali, BITS Pilani Goa Campus - Email ID
- Dr. Jothi Ramalingam, NITK, Surathkal - Email ID