Rahul B S

https://www.linkedin.com/in/rahul-bs/
rahulbs1798@gmail.com | f20160470@goa.bits-pilani.ac.in | +91-7019810875 | +91-9606703265

PERSONAL INFORMATION

Date of Birth : 17 Feb, 1998

Nationality : Indian

EDUCATION

MASTER OF SCIENCE (HONS)
Mathematics | 2016-21(Expected)
BITS Pilani, KK Birla Goa Campus

BACHELOR OF ENGINEERING(HONS)
Electronics and Instrumentation | 2016-21(Expected)
BITS Pilani, KK Birla Goa Campus

WORK EXPERIENCE

IBM India Research Labs, Bangalore Summer Research Intern

Society of Electronic Transaction and Security, Chennai Summer Research Intern

Institute of Mathematical Sciences, Chennai Winter Research Intern

International Institute of Information Technology, Bangalore Summer Research Intern

Institute of Mathematical Sciences, Chennai Summer Research Student

RESEARCH EXPERIENCE

Efficient RSA shared key generation in a multi-party setting | Guided by Prof. Carmit Hazay

- Working on coming up with efficient methods of biprimality testing for generation of shared RSA modulus.
- Also trying to improve efficiency of existing shared RSA-modulus generation methods such as Boneh Franklin's test using tools in such as the average case error estimate method as in Damgard et al. for Miller Rabin test.

Analysis of existing Beyond Birthday Bound MAC schemes | Work outline | Guided by Dr. Jothi Ramalingam

- 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.

Secure Assisted Universally Blind Quantum Computation | Guided by Dr. Radhika Vatsan

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

TECHNICAL EXPERIENCE

Zero Knowledge Proofs | Ongoing Work | Guided by Dr. Dhinakaran Vinayagamurthy

- Efficient implementations of interactive and non-interactive versions of Ligero-like protocols.

Homomorphic Encryption Schemes | Beta-version | Guided by Dr. Srinivas Vivek

- Programming Platform: C++, Tools Involved: NTL (ZZ class mainly), HELib (BGV-SHE scheme)
- Worked on integrating the HElib-MP Library to the HEAT API by analysing differences between HElib and HElib-MP.

Efficient Hardware-based Symmetric Cryptographic Implementations | Guided by Prof. K R Anupama

- Implementation and analysis of ciphers GIMLI and PRESENT on FPGA and ARM Microcontroller.

Random Graphs & applications in Cryptography | Report | Guided by Dr.Tarkeshwar Singh

CONFERENCES AND WORKSHOPS

Secure Multiparty computation: Theory and Practice | IISc. Bangalore

The 10th BIU Winter School on Cryptography | Bar-Ilan University, Israel

Summer school in Theoretical Computer Science | IMSc. Chennai

Ramanujan Math and IT Conference 2018 | IIIT, Bangalore

IEEE International Conference on Advanced Networks & Telecommunications Systems 2019

RELEVANT COURSEWORK AND TEACHING EXPERIENCE

A Reading Course in Algebraic Number Theory | Guided by Dr. Vijay Patankar

Teaching Assistant: Algebra 1

Mentor, Quark Technical Project | Cryptography

Mentor, Quark Technical Project | Ethical Hacking and Penetration Testing

Coursework |Academic

- Completed : Number Theory, Algebra, Graph Theory, Microprocessors, Complex Analysis, VLSI Design.
- Ongoing : Analog Electronics, Digital Image Processing, Power Electronics

Coursework | MOOC

- Cryptography-1 (Stanford University), Foundations of Cryptography(IIIT-B), The RUST Language(Udemy)
- Object Oriented Data Structures in C++(University of Illinois)
- Classical Cryptosystems and Core Concepts(University of Colorado)
- Ongoing : Data Structures and Algorithms

TECHNICAL SKILLS

Computational: Java, C, C++, Python, MATLAB, SAGE, PARI/GP, Rust

Others: GIT, LaTeX, HTML, XML, Shell Scripting(Linux).

CERTIFICATIONS AND OTHER TECHNICAL EXPERIENCES

Certification in Network Management | Nettech Pvt. Ltd | Oct'17

Technical Project in ReactJS: | Quark'19

Quick-Heal Certification in Cybersecurity and Forensics | Quark'18

SEBI Certification in Introduction to technical Analysis | Quark'18

POSITIONS OF RESPONSIBILITY

Co-ordinator | BITSkrieg, Cybersecurity Club
Core Member | QUARK'18 Controls, BITS Goa
Part-Time Associate | National Agenda Forum

ACADEMIC ACHIEVEMENTS

- Qualified JEE Mains and Advanced(top 1%)
- Ranked in the top 0.2% of the Karnataka CET.
- Ranked in the top 1% of the CBSE Board in class 12.
- Ranked in the top 0.01% ICSE Board in Class 10.

REFERENCES

- Prof. Carmit Hazay, Bar Ilan University, Israel - Carmit.Hazay@biu.ac.il
- Prof. Anupama K R, BITS Pilani Goa campus - anupkr@goa.bits-pilani.ac.in
- Dr. Shilpa Gondhali, BITS Pilani Goa Campus - shilpag@goa.bits-pilani.ac.in
- Dr. Jothi Ramalingam, NITK, Surathkal - jothiram@nitk.edu.in