

Rahul Satish

Researcher, Privacy and Scaling Explorations Group, Ethereum Foundation

rahulbs.me rahulbs1798@gmail.com [rahulbs98](https://github.com/rahulbs98) [+91-7019810875](https://www.linkedin.com/in/rahulbs1998) [in rahulbs1998](https://www.linkedin.com/in/rahulbs1998)

Education

Present Sep 2021	Alexander Kofkin Faculty of Engineering, Bar Ilan University M.Sc. with thesis in Engineering (Computer Engineering Track)	Ramat Gan, Israel
Aug 2021 Aug 2016	Birla Institute of Technology and Science (BITS) Pilani Dual Degree Programme, M.Sc.(Mathematics) & B.E.(Electronics & Instrumentation)	Goa, India

Experience

Present Oct 2021	BIU Center for Research in Applied Cryptography and Cyber Security [🌐] <i>Graduate Student Researcher</i> Working with Prof. Carmit Hazay in the area of Secure Computation, more specifically in Garbled Circuits.	Tel Aviv, Israel
Oct 2021 Jul 2021	Ethereum Foundation Privacy and Scaling Explorations Group [🌐] <i>Researcher</i> Working with a team developing a zk-rollup that directly supports the Ethereum Virtual Machine(EVM)	Singapore
Dec 2021 Jul 2021	Chain Reaction Cryptography Research Group [🌐] <i>Consultant Researcher</i> Advisor: Nir Elkayam, Guy Granot Working on modelling and understanding current leveled and fully Homomorphic Encryption Schemes	Tel Aviv, Israel
Jun 2021 Jan 2021	QED-it Systems Cryptography Group [🌐] <i>Research Intern</i> Advisors: Daniel Benarroch, Michael Adjedj Worked on constructing efficient circuits for the BFV scheme, for comparing & sorting encrypted integers.	Tel Aviv, Israel
May 2021 Aug 2020	Center for Research in Applied Cryptography and Cyber Security, BIU [🌐] <i>Research Intern</i> Advisors: Prof. Carmit Hazay, Prof. Muthu Venkitasubramaniam Worked on constructing efficient maliciously secure solutions for the PSI-Sum Problem	Tel Aviv, Israel
Aug 2020 May 2020	IBM Research Blockchain and Smart Contracts Group [🌐] <i>Research Intern</i> Advisors: Dr. Dhinakaran Vinayagamurthy, Nitin Singh Designed a modular framework to write interactive ZKP systems on arithmetic circuits	Bangalore, India
Aug 2019 May 2019	SETS India Applied Cryptography Research Group [🌐] <i>Summer Intern</i> Advisor: Dr. Jothi Ramalingam Worked on deploying cryptanalysis techniques on existing Beyond-Birthday Bound secure MACs	Chennai, India

Select Research Projects

Efficient protocol for the Private Set Intersection(PSI) Sum Problem <i>Advisors: Prof. Carmit Hazay, Prof. Muthu Venkitasubramaniam</i> > While understanding the approach used by the current solutions [IKN+17, IKN+19, MPR+20] to this problem, we recognise the efficiency trade-offs that are introduced by using Shuffled Distributed OPRFs in their approach and propose an alternate solution that does better asymptotically in the malicious setting. We also extend our work to be able to obtain the PSI-Sum on both sides, an improvement to the protocol described by [IKN+19].	Jan'21 - Jul'21
Efficient biprimality tests for Distributed RSA Modulus generation <i>Advisors: Prof. Carmit Hazay, Prof. Muthu Venkitasubramaniam</i> > With the goal of being able to efficiently generate RSA keys in a distributed setting, we analyse the protocol by [BF97]. More specifically, we try to improve the soundness of the distributed biprimality test proposed in the paper as the bounds are not tight. We also explore other testing methods to achieve better bounds.	Aug'19 - Dec' 20

Select Technical Projects

Efficient sorting and comparison in the homomorphic setting <i>Advisors: Daniel Benarroch, Michael Adjedj</i> [🌐 Blog] > Identifying and implementing the best possible ways to construct HE circuits for comparison and sorting integer data.	Jan'21 - Jun'21
---	-----------------

Generating custom polynomial constraints for efficient PLONK circuits

Jun'21 - Oct'21

Advisor: [Barry Whitehat](#) [🌐 Repository, 🌐 Specs]

- > Working on a zk-rollup that directly supports the Ethereum Virtual Machine(EVM). Prior to that, we are developing a ZKP layer over the EVM to be able to validate blocks through the PLONK proving system. Work is majorly on developing custom constraints for the EVM Opcodes as of now. This is a work in progress.

Workshops

Secure MPC : Theory and Practice Workshop, 2020 Amongst the 45 selected for the workshop at IISc, Bengaluru.

10th BIU Winterschool in Cryptography, 2020 Amongst the 3 students selected from India for the school at BIU, Israel.

RMIT Conference, 2018 Amongst the 50 selected for the workshop at IIIT, Bengaluru.

Theoretical CS Summer School, 2018 Amongst the 20 selected students for the summer school at IMSC, Chennai.

Teaching and Leadership Roles

Algebra-1 (MATHF215) *Teaching Assistant* Aug'19 - Dec'19

- > Responsibilities included evaluating tutorials, and helping students with the coursework and home assignments.

IEEE ANTS, 2019, BITS Goa *Web Development Lead* [Website] May'19 - Dec'19

- > Responsible for building and maintaining website of the IEEE International Conference on Advanced Networks and Telecommunications Systems 2019.

Introduction to Applied Cryptography, Quark Summer Technical Project *Instructor* May'19 - Aug'19

- > Voluntarily mentoring students from across the nation to get used to cryptographic objects and the math behind the subject.

BITSkrieg, Ethical Hacking and PenTesting Club, BITS Goa *Co-ordinator* Aug'18 - Jun'19

- > Responsibilities include ensuring that the club works towards achieving its annually laid out goals.
- > Handled a lecture series on Applied Cryptography for students of the college, being a member of the club.
- > Involved in solving Capture the Flag(CTF) events such as Google CTF, PICO CTF, DEFCON regularly.

Quark Controls, BITS Goa *Core Member* Mar'17 - Feb'18

- > Successfully established contacts with companies like Mozilla, JP Morgan, LIGO for hosting workshops on campus.
- > Responsible in helping the team arrange seminars and talks for the students on technical issues.

Academic Service

External Reviewer ACM CCS'21, TCC'21

References

- > Prof. Carmit Hazay Associate Professor, Bar Ilan University, Israel [🌐][📧]
- > Prof. Muthu Venkatasubramanian Associate Professor, Georgetown University, US [🌐][📧]
- > Dr. Dhinakaran Vinayagamurthy Researcher, IBM Research, India [🌐][📧]
- > Daniel Benarroch Director of Research, QED-it Systems, Israel [🌐][📧]
- > Michael Adjedj Senior Cryptography Engineer, QED-it Systems, Israel [🌐][📧]
- > Prof. Jothi Ramalingam Assistant Professor, NITK Suratkal, India [🌐][📧]