

# Rahul Satish

Graduate Student Researcher, BIU Cyber Center

[rahulbs.me](mailto:rahulbs.me) [rahulbs1798@gmail.com](mailto: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	<b>Alexander Kofkin Faculty of Engineering, Bar Ilan University</b> M.Sc. with thesis in Engineering (Computer Engineering Track)	Ramat Gan, Israel
Aug 2021 Aug 2016	<b>Birla Institute of Technology and Science (BITS) Pilani</b> Dual Degree Programme, M.Sc.(Mathematics) & B.E.(Electronics & Instrumentation)	Goa, India

## Experience

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

## Publications

S=In Submission, C=Conference, W=Workshop, P=Poster/Demo, J=Journal

[W.1]	<b>Garbling 3-input AND gates</b> [🌐] Tomer Ashur, Carmit Hazay, <a href="#">Rahul Satish</a> <i>Conference for Failed Approaches and Insightful Losses in Cryptology</i>	[CFAIL'23]
-------	---	------------

## Select Research Projects

<b>Constructing communication efficient Garbled Circuits</b> <i>Advisors: Prof. Carmit Hazay, Dr. Tomer Ashur</i>	Feb'22 - till date
> Construction of garbling schemes, where we aim to reduce concrete communication costs in existing state of art schemes. Current practical schemes, also called linear garbling schemes, have a lower bound of sending $2\kappa$ bits of communication. We try to understand generalizations of these models, and see what are the possible ways to practically bypass these lower bounds.	
<b>Efficient biprimality tests for Distributed RSA Modulus generation</b> <i>Advisors: Prof. Carmit Hazay, Prof. Muthu Venkitasubramaniam</i>	Aug'19 - Dec' 20
> 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.	

## Select Technical Projects

---

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

## Workshops

---

- Foundations and Frontiers of Probabilistic Proofs, 2023** Amongst the few selected for the summer school in Zurich
- Theory and Practice of MPC workshop, 2022** Amongst the few selected for the workshop at Aarhus University,Denmark
- 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.
- Theoretical CS Summer School, 2018** Amongst the 20 selected students for the summer school at IMSC, Chennai.

## Talks

---

- “Garbling 3-input AND gates”**  
> CFAIL 2023 August 2023 (Remote)

## 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,SAC'22

## References

---

- > Prof. Carmit Hazay ..... Associate Professor, Bar Ilan Univeristy, Israel [🌐][📧]
- > Dr. Tomer Ashur ..... Co-Founder, Cryptomeria, Belgium [🌐][📧]
- > Prof. Muthu Venkitasubramaniam ..... Associate Professor, Georgetown University, US [🌐][📧]
- > Dr. Dhinakaran Vinayagamurthy ..... Researcher, IBM Research, India [🌐][📧]
- > Daniel Benarroch ..... Director of Research, QED-it Systems, Israel [🌐][📧]