Rahul **Satish**

Ph.D. Researcher, ITU Copenhagen

rahulbs.me rahs@itu.dk rahulbs98 +45-91958601 rahulbs1998

Education

Present | **Department of Computer Science, IT University of Copenhagen** | **Copenhagen, Denmark**
Jan 2024 | Ph.D. in Computer Science

Nov 2023 | **Alexander Kofkin Faculty of Engineering, Bar Ilan University** | **Ramat Gan, Israel**
Sep 2021 | M.Sc. with thesis in Enginnering (Computer Engineering Track)

Aug 2021 | **Birla Institute of Technology and Science (BITS) Pilani** | **Goa, India**
Aug 2016 | Dual Degree Programme, M.Sc.(Mathematics) & B.E.(Electronics & Instrumentation)

Experience

Present | **Department of Computer Science, ITU Copenhagen** [🌐] | **Copenhagen, Denmark**
Oct 2021 | *Ph.D. Fellow | Advisor: Prof. Bernardo David*
Working on my PhD disseration in the area of secure computation

Nov 2023 | **BIU Center for Research in Applied Cryptography and Cyber Security** [🌐] | **Tel Aviv, Israel**
Oct 2021 | *Graduate Student Researcher | Advisor: Prof. Carmit Hazay*
Working with Prof. Carmit Hazay in the area of Secure Computation, more specifically in Garbled Circuits.

Oct 2021 | **Ethereum Foundation | Privacy and Scaling Explorations Group** [🌐] | **Singapore**
Jul 2021 | *Researcher*
Worked with a team developing a zk-rollup that directly supports the Ethereum Virtual Machine(EVM)

Dec 2021 | **Chain Reaction | Cryptography Research Group** [🌐] | **Tel Aviv, Israel**
Jul 2021 | *Consultant Researcher* | Advisor: Nir Elkayam, Guy Granot
Worked on modelling and understanding current leveled and fully Homomorphic Encryption Schemes

Jun 2021 | **QED-it Systems | Cryptography Group** [🌐] | **Tel Aviv, Israel**
Jan 2021 | *Research Intern* | Advisors: Daniel Benarroch, Michael Adjedj
Worked on constructing efficient circuits for the BFV scheme, for comparing & sorting encrypted integers.

Aug 2020 | **IBM Research | Blockchain and Smart Contracts Group** [🌐] | **Bangalore, India**
May 2020 | *Research Intern* | Advisors: Dr. Dhinakaran Vinayagamurthy, Nitin Singh
Designed a modular framework to write interactive ZKP systems on arithmetic circuits

Aug 2019 | **SETS India | Applied Cryptography Research Group** [🌐] | **Chennai, India**
May 2019 | *Summer Intern* | Advisor: Dr. Jothi Ramalingam
Worked on deploying cryptanalysis techniques on existing Beyond-Birthday Bound secure MACs

Publications

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

[W.1] **Garbling 3-input AND gates** [🔗]
Tomer Ashur, Carmit Hazay, Rahul Satish
Conference for Failed Approaches and Insightful Losses in Cryptology **[CFAIL'23]**

[S.1] **On the Feasibility of Sliced Garbling** [🔗]
Tomer Ashur, Carmit Hazay, Rahul Satish
[In Submission]

Select Research Projects

Constructing communication efficient Garbled Circuits Feb'22 - till date
Advisors: Prof. Carmit Hazay, Dr. Tomer Ashur

› 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 2κ bits of communication. We try to understand generalizations of these models, and see what are the possible ways to practically bypass these lower bounds.

Efficient biprimality tests for Distributed RSA Modulus generation Aug'19 - Dec' 20

Advisors: Prof. Carmit Hazay, Prof. Muthu Venkitasubramaniam

› 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. Bernardo David ..... *Associate Professor, IT University of Copenhagen, Denmark* [][]
› Prof. Carmit Hazay ..... *Associate Professor, Bar Ilan Univeristy, Israel* [][]
› Dr. Tomer Ashur ..... *Co-Founder, Cryptomeria, Belgium* [][]
› Daniel Benarroch ..... *Director of Research, QED-it Systems, Israel* [][]