Rahul **Satish**

Ph.D. Researcher, ITU Copenhagen

rahulbs.me rahs@itu.dk rahulbs98 beacon.17 rahulbs1998

Education

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

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

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

Experience

Present – Jan 2024 | **Department of Computer Science, ITU Copenhagen** [🌐] — **Copenhagen, Denmark**
Ph.D. Fellow | Advisor: Prof. Bernardo David
Working on my PhD disseration in the area of secure computation

Nov 2023 – Oct 2021 | **BIU Center for Research in Applied Cryptography and Cyber Security** [🌐] — **Tel Aviv, Israel**
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 – Jul 2021 | **Ethereum Foundation | Privacy and Scaling Explorations Group** [🌐] — **Singapore**
Consultant Researcher
Worked with a team developing a zk-rollup that directly supports the Ethereum Virtual Machine(EVM)

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

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

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

Aug 2019 – May 2019 | **SETS India | Applied Cryptography Research Group** [🌐] — **Chennai, India**
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

[C.1] **Rumors MPC: GOD for Dynamic Committees, Low Communication via Constant-Round Chat** [🔗]
Bernardo David, Arup Mondal, Rahul Satish
[**ASIACRYPT'25**]

[S.1] **Oblivious Garbling and its Applications**
Tomer Ashur, Carmit Hazay, Rahul Satish
[**In Submission**]

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

Talks

"Garbling 3-input AND gates"

› CFAIL 2023 [🌐] [📹] August 2023 (Remote)

Select Technical Projects

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.

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.

Non-Interactive Proof Generation from Interactive Zero Knowledge Protocols May'20 - Aug'20
Advisors: Dr. Dhinakaran Vinayagamurthy, Nitin Singh

› Designed a modular framework for Interactive Zero Knowledge Protocols which was used to convert it to a non-interactive protocol. Implemented additional features for the design to support oracles, protocol composition, etc.. and tested existing protocols like Ligero on it.

Teaching and Leadership Roles

Foundations of Cryptography, Cryptographic Computation and Blockchains *Instructor* at ITU

› 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 ANTS 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 it.

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 AC'25, Crypto'25, PKC'25, ICDCS'25, TCC'24, EC'24, DCC'24, JoC'23, SAC'22 , EC'22, CCS'21, TCC'21

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* [][]