Varun Maram

Research Scientist – Postdoc
Cybersecurity Group
SandboxAQ

Phone: +44 7464 127 694
Email: msvr81@gmail.com
Web: varun-maram.github.io

Research Interests

My interests lie in *quantum-resistant cryptography*, with an emphasis on provable post-quantum security of real-world cryptosystems. I also have a broader interest in *multi-party computation* and *distributed systems*. Recently, I've been interested in constructing advanced quantum-secure primitives—such as anonymous credentials and verifiable oblivious PRFs—from *zkSNARKs*.

Education

2019 - 2023 **Swiss Federal Institute of Technology, Zurich (ETH Zurich)**, *Zurich*
Dr.Sc. in Computer Science, member of the Applied Cryptography Group
Supervisor: Kenneth G. Paterson

2017 - 2019 **Swiss Federal Institute of Technology, Zurich (ETH Zurich)**, *Zurich*
M.Sc. in Computer Science "with distinction", *GPA* – ***5.75/6.0***

2013 - 2017 **Indian Institute of Technology, Roorkee (IIT Roorkee)**, *Roorkee*
B.Tech. in Computer Science and Engg., minors in Mathematics, *CGPA* – ***9.578/10***
(Departmental Rank 2, out of ≈ 75 students)

Work Experience

03/2024 - Present **SandboxAQ**, *London*
Research Scientist – Postdoc. Member of the Cybersecurity Group.
Manager(s): Nina Bindel, Andreas Hülsing

- Currently analysing post-quantum versions of real-world protocols, and constructing advanced quantum-secure primitives from zkSNARKs.
- Contributing new features to "*AQtive Guard*", SandboxAQ's cryptographic management product.
- Writing blogposts on "*The Cryptography Caffè*", SandboxAQ's engineering tech blog.

06/2022 - 09/2022 **Visa Research**, *Palo Alto*
Research Intern. Worked on constructing quantum secure public-key encryption schemes. Mentor: Navid Alamati

06/2021 - 09/2021 **Visa Research**, *Palo Alto (worked remotely from Zurich)*
Research Intern. Worked on analysing quantum (in)security of widely-used block cipher modes of operation. Mentors: Daniel Masny and Sikhar Patranabis

05/2016 - 07/2016 **Adobe BigData Experience Lab**, *Bangalore*
Research Intern. Conducted research on augmented reality technology in the context of digital marketing. Mentor: Gaurush Hiranandani

Standardization Efforts

2022 D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, *Varun Maram*, I. von Maurich R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, and W. Wang.
"Classic McEliece", Round 4 Submission in NIST's *Post-Quantum Cryptography (PQC) Standardization Project*, currently being considered for ISO standardization.

Publications

2025 B. Benčina, B. Dowling, *Varun Maram*, and K. Xagawa. **"Post-quantum Cryptographic Analysis of SSH"**, *46th IEEE Symposium on Security and Privacy 2025*.
[This work was also presented at the Real World Crypto (RWC) 2025 symposium.]

2024 N. Alamati, *Varun Maram*. **"Quantum CCA-Secure PKE, Revisited"** , 27th IACR Intl. Conference on Practice and Theory of Public-Key Cryptography – *PKC 2024*.
[Best Paper Award], [Invited to Journal of Cryptology]

2023 M. Jauch, *Varun Maram*. **"Quantum Cryptanalysis of OTR and OPP: Attacks on Confidentiality, and Key-Recovery"**, Selected Areas in Cryptography – *SAC 2023*.

2023 N. Alamati, *Varun Maram*, D. Masny. **"Non-Observable Quantum Random Oracle Model"**, 14th Intl. Conference on Post-Quantum Cryptography – *PQCrypto 2023.*

2023 *Varun Maram*, K. Xagawa. **"Post-Quantum Anonymity of Kyber"**, 26th IACR Intl. Conference on Practice and Theory of Public-Key Cryptography – *PKC 2023*.
[Best Paper Award]

2022 *Varun Maram*, D. Masny, S. Patranabis, and S. Raghuraman. **"On the Quantum Security of OCB"**, IACR Transactions on Symmetric Cryptology, *ToSC 2022* (2).

2022 P. Grubbs, *Varun Maram*, and K. G. Paterson. **"Anonymous, Robust Post-Quantum Public Key Encryption"**, 41st Annual Intl. Conference on the Theory and Applications of Cryptographic Techniques – *EUROCRYPT 2022*.
[This work was also presented at NIST's 3rd PQC Standardization Conference.]

2021 K. Cong, D. Cozzo, *Varun Maram*, and N. P. Smart. **"Gladius: LWR Based Efficient Hybrid Public Key Encryption with Distributed Decryption"**, 27th Annual Intl. Conference on the Theory and Application of Cryptology and Information Security – *ASIACRYPT 2021*.

2020 *Varun Maram*. **"On the Security of NTS-KEM in the Quantum Random Oracle Model"**, 8th Intl. Workshop on Code-Based Cryptography – *CBCrypto 2020*.

2020 C. Liu-Zhang, *Varun Maram*, and U. Maurer. **"On Broadcast in Generalized Network and Adversarial Models"**, 24th Conference on Principles of Distributed Systems – *OPODIS 2020*.

2019 C. Liu-Zhang, *Varun Maram*, and U. Maurer. **"Brief Announcement: Towards Byzantine Broadcast in Generalized Communication and Adversarial Models"**, 33rd International Symposium on Distributed Computing – *DISC 2019*.

2017 G. Hiranandani, K. Ayush, A. R. Sinha, *Sai Varun Reddy Maram*, C. Varsha, and P. Maneriker. **"[Poster] Enhanced Personalized Targeting Using Augmented Reality"** 16th IEEE Intl. Symposium on Mixed and Augmented Reality – *ISMAR 2017*.

Patents

2016 G. Hiranandani, *Sai Varun Reddy Maram*, K. Ayush, C. Varsha, and S. Jain. **"Method, Medium, and System for Product Recommendations Based on Augmented Reality Viewpoints"**, *US 10475103 B2.*

2016 G. Hiranandani, C. Varsha, *Sai Varun Reddy Maram*, K. Ayush, and A. R. Sinha. **"Identifying Augmented Reality Visuals Influencing User Behavior in Virtual-Commerce Environments"**, *US 10950060 B2.*

2016 G. Hiranandani, K. Ayush, C. Varsha, and *Sai Varun Reddy Maram*. **"Creating Targeted Content Based on Detected Characteristics of an Augmented Reality Scene"**, *US 10922716 B2.*

Selected Honors and Awards

2024 **Best Paper Award** given by the program committee of PKC 2024 conference for our paper *"Quantum CCA-Secure PKE, Revisited"*; given to 2 papers out of 178 submissions.

2023 **Best Paper Award** given by the program committee of PKC 2023 conference for our paper *"Post-Quantum Anonymity of Kyber"*; given to 2 papers out of 183 submissions.

2017 **Master Scholarship** awarded by the Department of Computer Science, ETH Zurich to admitted students based on their excellent academic achievements so far; was offered to ≈ 10 students that year.

2014 **Aditya Birla Group Scholarship** awarded to engineering, management and law students all over India, based on their excellence on the academic and leadership front; given to ≈ 40 graduates in the country.

2012 **Kishore Vaigyanik Protsahan Yojana (KVPY) Fellowship** awarded by Dept. of Science and Technology, Govt. of India, to highly motivated students interested in pursuing a research career; given to ≈ 250 high school students in the country.

2011 **Bronze Medal**, 16th International Astronomy Olympiad, Kazakhstan.
One of the 3 high school students selected to represent India in the competition.

2011 **Infosys Award** for International Olympiad Medallists, by HBCSE in association with Tata Institute of Fundamental Research (TIFR) Endowment Fund

2011 **Gold Medal**, 13th National Science Olympiad, Science Olympiad Foundation, Delhi. National Rank 1st out of ≈ 20,000 participants.

Technical Skills

Programming	C++, C, Python, Java, bash, C#
OS	Linux (Ubuntu), macOS, Windows
Software	Git, PostgreSQL, Docker, SageMath, liboqs, OpenSSH, EasyCrypt, LaTeX

Service

I was on the program committee for the following conference:

- *PKC 2025*

I was also a sub-reviewer for the following conferences:

- *CRYPTO 2025*
- *CRYPTO 2024, ASIACRYPT 2024*
- *EUROCRYPT 2023*
- *CRYPTO 2021, ASIACRYPT 2021*
- *CRYPTO 2020, CT-RSA 2020*