Aarav Varshney

+65-88984784 | aarav.varshney22@gmail.com | linkedin.com/in/aarav22 | github.com/aarav22 | www.aaravvarshney.in

Education

Ashoka University — Sonepat, India

Postgraduate Diploma in Advanced Studies and Research — Sept. 2022 – May 2023

- Graduated Cum Laude with a thesis focused on Anonymous Credentials under Prof. Mahabir P. Jhanwar.
- Advanced Major in CS; relevant coursework includes Information and Coding Theory, Reading, Reviewing, and Presenting Scientific Papers, and Machine Learning for Finance.

Ashoka University — Sonepat, India

Bachelor of Science in Computer Science, Minor in Mathematics — Aug. 2019 – May 2022

- Graduated Cum Laude; relevant coursework includes Computer Security and Privacy, Blockchain and Cryptocurrencies, Theory of Computation, Advanced Programming, and Abstract Algebra.

Research Experience

Project Officer — Nov. 2024 – Present

Nanyang Technological University (NTU) — Singapore

- Analyzing NIST and IETF standards to establish concrete policies for mandating secure cryptography adoption within organizations.
- Secured 750K SGD grant from CyberSG Research & Development Programme Office (CRPO) to develop and commercialize quantum-safe cybersecurity solutions.
- Contributed to securing OCBC Bank post-quantum migration project by drafting project specifications.

Co-founder & CTO | *Previously* Research Fellow — June 2024 – Present

PQStation (NTU Spinoff) — Remote/Singapore

- Developing migration roadmaps for organizational transition to post-quantum cryptography.
- Identifying critical gaps in cryptographic asset discovery and designing a network scanner to automatically inventory organizational cryptographic infrastructure.

Research Assistant — Nov. 2022 – June 2024

Ashoka University & Defense Research and Development Organization (DRDO) — Sonepat, India

- Led development of a PQC key management software and managed its integration into DRDO's existing systems.
- Implemented a custom Dilithium signature scheme in C based on the original source code.
- Designed and developed custom post-quantum X.509 certificates without relying on third-party libraries. Strictly followed the X.509 standard and offered verifiability through OQS's OpenSSL.

Publications

[PUB01] YouChoose: A Lightweight Anonymous Proof of Account Ownership — IACR ePrint

Aarav Varshney, Prashant Agrawal, and Mahabir Prasad Jhanwar — under submission

- We proposed and implemented a concrete YouChoose protocol for anonymously proving account ownership for SMTP and HTTP based protocols over the TLS secure channel.
- We also look into using a zk-SNARK based approach to extend the anonymous PAO paradigm to develop anonymous SSO without requiring any changes at the server.

[PUB02] HY-QSN: HYbrid Quantum Safe Networks — IACR ePrint

Sayan Das, Aarav Varshney, Prasanna Ravi, and Anupam Chattopadhyay — under submission

- We propose a post-quantum proxy protocol to secure QKD interfaces against quantum adversaries.
- Our proxy transparently applies PQC-based signatures and key encapsulation to ETSI-compliant QKD APIs, without requiring changes to existing infrastructure.

[REPORT01] Transitioning to a Post-Quantum Key Management Framework

Mahabir Prasad Jhanwar, Aarav Varshney and Adit Dhawan — available on request

- We propose and implement a post-quantum key management solution to safeguard the existing communication infrastructure against quantum adversaries. Our report details the implementation of X.509 PQC certificates without relying on third-party libraries.

Work Experience

Teaching Fellow & Teaching Assistant Aug. 2021 – Dec. 2023
Ashoka University Sonepat, India

- Instructed and assisted in courses including Blockchain and Cryptocurrencies, Computer Networks, Computer Security and Privacy, and Database Management Systems.
- Facilitated student learning through weekly office hours, tutorials on Hyperledger Fabric, TLS, SQL, and assessed assignments and course projects.

Software Engineer Intern June 2022 – Aug. 2022
Amuse Labs Bengaluru, India

- Developed an Alexa app for playing Amuse Labs puzzles like quizzes and crosswords via voice commands, enhancing user accessibility and creating new revenue opportunities with clients such as The Washington Post.
- Overcame technical challenges in voice command design and REST API integration with the existing backend. Created a general TypeScript library for websites to offer Alexa-integrated quizzes.

Backend Developer Intern Mar. 2022 – June 2022
SALT (Funded by YC'W22) Bengaluru, India

- Developed a document templating service to generate customized PDFs through form inputs for legal agreement templates. Achieved a 30-40% reduction in document generation time by switching to AWS Lambda functions.

Co-Founder & Head of Development Sept. 2020 – Aug. 2022
Beyond Design Studio Chennai, India

- Led team of 20-30 members, successfully delivering industry projects and generating net profits exceeding $3,600 USD. Employed a diverse range of tools and frameworks, including Next.js, TailwindCSS, Node.js, Express.js, and GCP, across various projects.
- Cultivated partnerships with esteemed organizations, such as Niti Aayog, InIFarms, Quintessentially, and DaurCom, for collaborative development projects and ongoing tech maintenance initiatives.

Projects

Trading App | Typescript, Socket.js, Node.js, Next.js, PostgreSQL, GCP April 2022 – Aug. 2022

- Designed backend handling 200+ concurrent users with minute-by-minute updates via cron scheduler.

Jaan Pehchan | Javascript, Node.js, React Native, Neo4j, Heroku Jan. 2022 – May 2022

- Full-stack social networking app for small businesses with 500+ Play Store downloads, managing 60K+ graph nodes.

MindBlock | React Native, BlockCypher API April 2021 – May 2021

- Educational app on Bitcoin with 7 structured modules using analogies and interactive tools for effective learning.

Other Activities

Head of Technology Dec. 2019 – May 2022
Ashoka Business Review Ashoka University, India

- Supervised tech development, website redesign, and blockchain podcast series with expert interviews.

Teacher Dec. 2021 – Jan. 2022
South Asian Winter Camp Remote

- Designed and taught comprehensive CS curriculum to 30+ high school students covering programming and ethics.

Achievements

- **Nomination for Microsoft Research Fellowship** - CS Dept., Ashoka University
- **Dean's List** - Dean of Academic Affairs, Ashoka University
- **Top 20% in DevCTF: Capture the Flag** - IIT Delhi

References

Anupam Chattopadhyay
Associate Professor, College of Computing and Data Science, NTU anupam@ntu.edu.sg
Mahabir P. Jhanwar
Associate Professor, CS Department, Ashoka University mahavir.jhawar@ashoka.edu.in
Debayan Gupta
Assistant Professor, CS Department, Ashoka University debayan.gupta@ashoka.edu.in