Aryan Nath

natharyan | natharyan.github.io | aryan-nath | aryannath2004@gmail.com | +91 8800690755

Education

Ashoka University — *India*

Bachelor of Science (Honours), Major in Computer Science; Minor in Mathematics — *Expected May 2025*

3.93/4.0 CGPA; 3.96/4.0 Major CGPA

Undergraduate Thesis: Post-Quantum Anonymous Credentials

Step by Step School — *India*

CLASS XII, CBSE — *2022; 95.6%*

CLASS X, CBSE — *2020; 96.6%*

Relevant Coursework

Linear Algebra, Multivariable Calculus, Algebra I, Cryptography I & II, Computer Networks, Operating Systems, Lattice-based Cryptography, Elliptic Curves, Theory of Computation, Information and Coding Theory.

Publications & Pre-prints

Soumyajit Basu, Fiona Arora, **Aryan Nath**, Karan Kumar, Lipika Dey (Dec 2025). "An Explainable Deep-Clustering Approach to Assess Climate Vulnerability in India". In: *International Conference on Pattern Recognition and Machine Intelligence*. URL: accepted papers (to be presented in December 2025).

Research Experience

Undergraduate Thesis — *India; August 2025 - present*

Capstone Project Report — Advisors: Prof. Mahavir Jhawar; Prof. Saravanan Vijayakumaran

- The Capstone Project involved developing an incremental version of Falcon and deploying it with Latticefold to create an Aadhaar credential QR code-based age proof for low-resource systems.
- The Capstone Thesis focuses on designing efficient zero-knowledge arguments for post-quantum anonymous credentials.

Trust Lab, IIT Bombay — *Mumbai, India; May 2025 - July 2025*

Research Intern - Post Quantum Signature Verification (Report) — Advisor: Prof. Saravanan Vijayakumaran

- Implemented R1CS circuits for the **SHA3-256**, **SHAKE128**, and **SHAKE256** in **Rust** using **Arkworks**.
- Designed a step function for SHA3-256, SHAKE128, and SHAKE256 to develop an Incrementally Verifiable Computation (IVC) using the Latticefold folding scheme framework, which helped me reduce the number of constraints from **153,536** to **37,000**.
- Currently designing a step function to represent ML-DSA post-quantum signature scheme as incremental computation and using it to create an incrementally verifiable computation proof using the Latticefold folding scheme.

Ashoka University — *Sonipat, India; January 2025 - September 2025*

Research Intern - Private Set Intersection — Advisor: Prof. Debayan Gupta

- Enabled authentication of inputs using a transparent setup in a private set intersection protocol based on key agreements and extended it to the setting of authorized private set intersection and achieved improved runtime and communication overhead. Also implemented the protocol using **C++**. (working manuscript, to be submitted at ASIACCS)
- Designing a private set intersection protocol with input authentication based on KZG commitments. Developed a new variant of private set intersection on authenticated inputs called All-or-Nothing APSI.

Automotive Security Lab, Ashoka University — *March 2024 - August 2025*

Research Intern - RF Fingerprinting Based IDS (Working Manuscript) — Advisor: Prof. Debayan Gupta

- Engineered features for radio frequency fingerprinting. Adapted it with an autoencoder-based anomaly detection model for detecting replay attacks against remote keyless entry systems in automobiles and achieved improved recall and accuracy.

Automotive Security Lab, Ashoka University — *June 2023 - January 2024*

Research Assistant - Synthetic Data Generation (Working Manuscript) — Advisor: Prof. Debayan Gupta

- Studied the Controller Area Network (CAN) bus in automotive vehicles and all known attacks against it.
- Investigated synthetic data generation using LSTMs and GANs to counter the unavailability of reliable data for training CAN bus intrusion detection systems.

Projects

NTT Fast Polynomial Multiplication: Implemented Cooley-Tukey (NTT) and Gentleman-Sande (INTT) in **Python** for fast polynomial multiplication.

Arithmetic-Coding: Implemented with E1 and E2 rescaling and floating-point precision tags in **Python** for arbitrary length sequences.

Treesize: File-system management software with new visualizations and cache based scans in **React**, **Tauri**, and **Rust**.

Chaos Attractors: Coded an Audio Visualiser for Chaotic Motion (Chaos Attractors) in **C++** using the **SFML** graphics . module.

Structure From Motion: Implemented the structure from motion pipeline from scratch in **C++** and used it to render 3D environments from mobile camera images.

Honours and Awards

2025 **Finalist, Data Analysis** at the **India Conference at Harvard** Developed a vulnerability index to identify rural regions most at risk from climate change. One of 4 teams selected from 401 globally; secured 3rd place and was part of the only student-led team in the finals.

2025 **Builder's Award for Service Excellence, Ashoka University** for significant contributions to enhancing the quality of the undergraduate program and strengthening the Computer Science department.

2022 - 2025 **Dean's List, Ashoka University** Awarded in all semesters for academic excellence.

2017-2025 **National Level Swimmer** Placed Top 10 in 50m Freestyle at the swimming nationals held in Pune, 2017. Received the **Most Valuable Player (MVP) - Swimming** award at **Ashoka University** for 2 years consecutively.

Teaching Experience

2025 **Teaching Assistant for ACM Summer School on Cryptography, IIT Bombay.** Assisted Prof. Saravanan Vijayakumaran in teaching **Circom** to undergraduate (2nd–4th year B.Tech/B.Sc.) and postgraduate students.

2024 - 2025 **3X Undergraduate Teaching Assistant, Ashoka University** for Discrete Mathematics, Data Structure & Algorithms, and Computer Networks. Conducted Weekly discussion sessions and office hours. Was responsible for evaluating assignments for 50+ students across courses (Student Feedback: 4.91/5.0)

2023 **Mathematics Teaching Assistant, Lodha Genius Program at Ashoka University.** Worked closely with professors from IIT Delhi, the Indian Statistical Institute and JNU to prepare and deliver a course on learning Number Theory through problem solving.

Leadership Positions & Extracurriculars

2024 - 2025 **Computer Science Student Representative** for the CS Department at **Ashoka University**.

2023 - 2024 **President, Computer Science Society** Spearheaded the society and led the transformation of CS culture at **Ashoka University** (Annual Report). Received the **Most Enterprising Society award** for the session 2023-2024.

2023 - 2024 **Captain, Swimming Team**. Led a team of 13 national and state level swimmers. Won the overall runner-up trophy at IIIT Delhi's annual sports fest.

2021 **Grade 8 Guitarist**, certified by Trinity College London examinations for Rock & Pop.

Certifications

Google Cybersecurity Specialization Certifying Authority: Google. Instructor: Google Career Certificates.

Post Quantum Cryptography Workshop Certifying Authority: IEEE Student Branch, IIT Indore. Instructors: Researchers from IITs, IISc, IIIT, UNSW Sydney, and UWaterloo.

Cryptography 1 Certifying Authority: Stanford University. Instructor: Dan Boneh.

Technical Skills

Programming: Python3, C/C++, Rust, JavaScript, Haskell, Dafny.

Technologies & Tools: Arkworks, Circom, Bellpepper, WireShark, Git, LaTeX, PyTorch, Numpy, Pandas, Matplotlib, React, Node.js, Flask.

Last updated: November 30, 2025