Aryan Nath

linkedin.com/aryan-nath

Email : 202602124@post.au.dk
Mobile : +4571574393
Github : github.com/natharyan

Education

- **Aarhus University** — Aarhus, Denmark
  M.Sc. in Computer Science (Cybersecurity) — *Aug. 2026 – Present*
- **Ashoka University** — Sonipat, India
  B.Sc. in Computer Science, Minor in Mathematics; Overall CGPA: 3.91/4.00 (9.775/10.0) (Gold Medalist in Computer Science) — *Aug. 2022 – May 2026*

Teaching Assistantships

- **Courses**: Teaching assistant for Information Security, Computer Networks, Data Structures and Algorithms, Discrete Mathematics, and Number Theory during my bachelor's degree. My responsibilities ranged from grading assignments and exams, creating weekly exercise sheets, and conducting office hours to conducting lab sessions using C and Wireshark.
- **ACM Summer School**: Lab assistant for writing zero-knowledge proof circuits using Circom in the 'Proof Systems II: SNARGs' session (IIT Bombay, 2025).

Publications

- **Stable Private Intersection with Consistency**. Manya Garg, Debayan Gupta, Arup Mondal, Aryan Nath[*1]. *Under submission.*
- **An Explainable Deep-Clustering Approach to Assess Climate Vulnerability in India**. Soumyajit Basu, Fiona Arora, Aryan Nath, Karan Kumar, Lipika Dey. PReMI 2025.

Bachelor's Thesis Project

- **Practical Post-Quantum Anonymous Credentials over Existing Credentials** — Ashoka University
  Advisors: Prof. Saravanan Vijayakumaran (IIT Bombay), Prof. Mahavir Jhawar (Ashoka University) — *2025 – 2026*
  - Developed a post-quantum secure **zero-knowledge proof** that enables holders of the Aadhaar identity credential to **selectively disclose** whether they are an adult, while providing a framework to generalise the proof to all other attributes of the credential. For this work, I modified the legacy Aadhaar credential to support the post-quantum Falcon signature scheme, and developed my own shim code to use **incrementally verifiable computation** (Latticefold) with the **Bellpepper** framework for **R1CS** circuits to make the proof generation practical for memory-constrained devices. Currently working on the pre-print for this work which I plan to submit to a conference.

Research & Professional Experience

- **DRDO, Defence Agency of the Govt. of India** — Delhi, India
  Software Developer — *Jan. 2026 – July 2026*
  - Developed a scalable **post-quantum key management framework** using **Django** and **Electron** frameworks for communication between officials of multiple labs of the Defence Research and Development Organisation of India. Made it scalable through a one-time offline setup and by enabling hierarchical certificate delegation through **TLS** and **OpenSSL**. All cryptographic operations, including creating **X.509 certificates** and encrypting communication messages, were handled by our own cryptographic library developed from scratch using C and Python.
- **Trust Lab, IIT Bombay** — Bombay, India
  Research Intern, advised by Prof. Saravanan Vijayakumaran — *May 2025 – July 2025*
  - Studied the Keccak **sponge construction** for the hash functions **SHA3-256, SHAKE128,** and **SHAKE256**. Designed and developed efficient **R1CS** circuits using the **Arkworks** framework in **Rust** to generate a **zero-knowledge argument of knowledge** for a preimage of these hash functions using **Groth16**. For this work, I developed my own gadget to emulate **unsigned 64-bit** representations for the hash function operations over the **BLS12-381** curve.

[1] indicates authors listed in alphabetical order following the Hardy-Littlewood rule.

- **Ashoka University** Sonipat, India
  Research Intern *May 2025 – Nov 2026*
  - Designed and developed a cryptographic protocol for a stronger version of **authenticated private set intersection** (APSI). PSI enables two parties to securely compute the intersection of their databases without revealing any non-intersection elements to the counter-party. APSI ensures that no party can manipulate their input over several sessions to instill a bias in the output or infer additional information from the intersection output by repeatedly changing their input over multiple PSI executions. We developed a protocol with stronger consistency guarantees for the Sender; in existing APSI protocols, the Sender can arbitrarily omit any of its elements from the intersection.

Projects

- **Intrusion detection system for cars (Ashoka University)**: Developed an intrusion detection system using an **autoencoder** machine-learning model and hand-picked features for **fingerprinting** radio-frequency signals to safeguard cars from replayed remote car key signals for unauthorised access to the vehicle. Prepared my own dataset for replay attacks on a real vehicle to test my model. Languages/Tools: **Python**, **scikit-learn**, and the **GNU Radio library** for Python.
- **Explainable deep clustering for climate vulnerability analysis (Ashoka University)**: Leveraged explainable deep clustering and conducted data analysis on district and administrative block-level datasets on climate data to develop an **interpretable numerical index** for climate vulnerability in the rural regions of India to identify those at most risk from climate change. Competed with this project at the ICH Hackathon at Harvard University in 2025 and placed **third in the final round**, as part of the only student-led team in the finals. Languages/Tools: **Python, Numpy, Pandas** for data analysis, and **scikit-learn** for implementing machine-learning models.
- **Tracer (independent project)**: Currently developing an **AI-native education app** with built-in features for writing assignments and a built-in browser and a personalised AI research assistant. Our motive is to allow students to use AI in their studies, but at the same time be accountable for how they use it. We leverage a fingerprint that is created as a student works on an assignment and share it with their teacher in a compressed and interpretable manner without revealing any private data. Our AI assistant is a Socratic learning model that never gives a direct answer to an assignment. Technologies: **TypeScript, React, Electron, PostgreSQL, LangChain/LangGraph, Supabase**.
- **Audio Visualizer using Chaotic Attractors (independent project)**: Developed an audio visualizer from scratch, in which the coordinates and colours of points tracing a chaotic attractor are updated based on the instantaneous amplitude of an audio file given as input. Languages/Libraries: **C++**, SFML.

Technical Skills, Certifications, and Awards

- **Programming languages**: Rust, Python3, C/C++, SQL, JavaScript.
- **Tools & Frameworks**: Wireshark, tcpdump, Git, OpenSSL, Arkworks, Circom, Bellpepper, AWS, React, Django, Linux, Scikit-learn, PyTorch.
- **Certifications**: Google Cybersecurity Professional Certificate (Certificate); Cryptography I by Stanford University (Certificate), IEEE Post Quantum Cryptography Workshop (Certificate).

Honours and Awards

- Awarded the Builder's Award for contributions to the computer science community as the President of the Computer Science society and as the student representative for the Computer Science department during my bachelor's degree.
- On the dean's list for every semester except the last of my bachelor's degree.
- Captain of the swimming team during the second year of my bachelor's degree.

Personal details

- **Hobbies**: Swimming (national-level swimmer during my schooling in India). Playing the guitar and singing (I have enjoyed performing as part of a band during my bachelor's).
- **Languages**: English (fluent), Hindi (native), Danish (beginner, currently taking lessons at A2B Sprogskole).