Archisman Dutta

archisman@cs.au.dk | archisman.org | github.com/DeviousCilantro

Research interests

Theoretical cryptography; pseudorandom correlations; indistinguishability obfuscation; complexity-theoretic techniques.

Education

Aarhus University — Aarhus, Denmark
Ph.D. in Computer Science — *Sep 2025 – present*

- Advisors: Peter Scholl and Diego F. Aranha.
- Selected coursework: Cryptographic Computing; Succinct Proofs; Cryptologic Protocol Theory; Randomized Algorithms.

Ashoka University — Sonipat, India
B.Sc. (Hons.) in Mathematics and Computer Science — *Sep 2021 – May 2024*

- Selected coursework: Algorithms; Theory of Computation; Symbolic Logic; Algebra; Probability and Statistics; Computer Security; Elliptic-Curve and Lattice-Based Cryptography.

University of Zurich — Zurich, Switzerland
Deep Dive into Blockchain summer school — *Jul 2023 – Aug 2023*

- Attended the UZH Blockchain Center summer school on a full scholarship; completed a group project on privacy-preserving CBDC auditing using Pedersen commitments and IPFS.

Manuscripts

- **ATAVISM: Private Originator Tracing in End-to-End Encrypted Messaging**, with Debayan Gupta and Arup Mondal. Manuscript, 2025.

Research experience

Aarhus University — Aarhus, Denmark
Graduate Research Assistant — *Sep 2025 – present*

- Working on pseudorandom correlation functions for VOLE from DCR-style assumptions, with possible applications to designated-verifier exponent-VRFs and threshold Schnorr signatures.

IIT Bombay Trust Lab — Mumbai, India
Pre-Doctoral Researcher — *Aug 2024 – May 2025*

- Studied circular-secure publicly verifiable time-lock puzzles and timed commitments from algebraic assumptions.
- Reviewed homomorphic and function secret sharing for branching and RMS programs, group correlations, and pseudorandom correlation generators.
- Participated in a reading group on proof systems, arguments, and zero knowledge.

IIT Bombay Trust Lab — Mumbai, India
Summer Research Intern — *May 2024 – Jul 2024*

- Investigated the complexity-theoretic hardness of TFNP subclasses including PPAD, PWPP, PPA, and PLS, with attention to cryptographically relevant Karp reductions.
- Studied lattice-based verifiable delay functions, time-lock puzzles, and proofs of sequential work.

Ashoka University — Sonipat, India
Undergraduate Research Assistant — *Jun 2023 – Jan 2024*

- Contributed to a WhatsApp-funded project on secure originator tracing for end-to-end encrypted messaging, focusing on deployability without revealing intermediate forwarding parties.
- Coauthored a manuscript formalizing and benchmarking the protocol against existing alternatives.
- Implemented prototype optimizations for number-theoretic transforms and fast modular arithmetic for

lattice-based cryptographic operations.

Questbook Remote / Palo Alto, CA
Security Research Intern *Aug 2023 – Mar 2024*

- Improved and benchmarked Groth16 proof generation for Circom R1CS-based circuits in the Reclaim Protocol.
- Compiled `rapidsnark` to platform-agnostic WebAssembly and evaluated proof-system libraries for browser and Node environments.
- Studied optimizations for AES and ChaCha20 circuits using arkworks and PLONKish arithmetization.

Teaching

Aarhus University Aarhus, Denmark
Graduate Teaching Assistant, Distributed Systems and Security *Jan 2026 – present*

- Grade assignments, hold discussion sessions, and answer student questions in office hours.
- Lab assistant, public-key cryptography, ACM India winter school on cryptography, IIT Madras, Dec 2024.
- Lab lead, fully homomorphic encryption with OpenFHE, ACM India summer school on theoretical foundations of cryptography, IIT Bombay, Jun 2024.

Talks

- Private Originator Tracing in End-to-End Encrypted Messaging. Aarhus Crypto Seminar, Jun 2025.
- Time-Lock Puzzles and Verifiable Delay Functions. Student seminar, Oct 2024.
- Fully Homomorphic Encryption Lab. ACM India summer school on theoretical foundations of cryptography, Jun 2024.

Service

- External reviewer / subreviewer: EUROCRYPT 2026; CRYPTO 2026.

Fellowships and travel support

- Research Excellence Program for Asia fellowship, Tel Aviv University, 2024 (declined).
- Industry scholarship, University of Zurich Blockchain Center summer school, 2023.
- Travel support: TCC 2025 (Aarhus University); RWC 2025 (IACR); TPMPC 2025 (IISc); ASIACRYPT 2024 (IIT Bombay Trust Lab).

Technical background

Rust, Python, C/C++, Go, Linux, shell scripting, Docker, WebAssembly, Circom, LaTeX.

Last updated: May 2026.