Archisman Dutta

archismandutta@proton.me | deviouscilantro.github.io

Research statement

My research interests span theoretical and practical aspects of cryptography with particular focus on verifiable computation and MPC.

Education

Ashoka University *Sonipat, India*

B.Sc. (Hons.) in Mathematics and Computer Science *Sep 2021 – May 2024*

- *CGPA*: 3.42/4.00
- *Relevant coursework*: Computer Security and Privacy, Elliptic Curves and Cryptography, Lattice-based Cryptography, Algebra 1, Probability and Statistics, Discrete Mathematics, Statistical Inference, Linear Algebra, Algorithm Design and Analysis, Theory of Computation, Applied Category Theory, Symbolic Logic, Data Structures

University of Zurich *Zurich, Switzerland*

Summer abroad *Jul 2023 - Aug 2023*

- Participated in the 'Deep Dive into Blockchain' summer school hosted by the UZH Blockchain Center on a full ride (**Source**)
- Implemented a privacy-focused CBDC auditing model in Rust using Pedersen commitments and IPFS storage/retrieval, coauthored the final report and gave a technical presentation for the group project

Experience

IIT Bombay Trust Lab *Mumbai, India*

Pre-Doctoral Researcher *Aug 2024 – Present*

- Conducting research into constructing circular-secure publicly verifiable time-lock puzzles and timed commitments from algebraic assumptions
- Performing a literature review into homomorphic and function secret sharing schemes for branching and RMS programs as well as group correlations and PCGs
- Contributing to 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 syntactic sub-classes like PPAD, PWPP, PPA and PLS inside TFNP with implications in Karp-reducible problems of cryptographic interest
- Studied and analyzed the security and concrete efficiency of lattice-based verifiable delay functions, time-lock puzzles and proofs of sequential work

Questbook *Remote / Palo Alto, CA*

Security Research Intern *Aug 2023 – Mar 2024*

- Conducted research into improving the performance of Groth16 zk-SNARK proof generation for the Reclaim Protocol and incorporated optimizations in code
- Benchmarked and tested a number of zero-knowledge proving systems and libraries to integrate with Circom R1CS-based circuits
- Modified and compiled rapidsnark to platform-agnostic WebAssembly for compatibility with Node and browser environments
- Investigated methods to enhance custom AES and ChaCha20 circuits designed for verifiable private key ownership proofs using arkworks and PLONKish arithmetization

Ashoka University *Sonipat, India*

Undergraduate Research Assistant *Jun 2023 – Jan 2024*

- Contributed to research funded by WhatsApp to design, implement and benchmark a secure originator tracing protocol integrable in end-to-end encrypted messaging platforms without undermining the privacy of intermediate parties in a forwarding chain
- Coauthored a paper currently in submission that proposes, formalizes and compares the protocol against existing alternatives to highlight the feasibility of real-world deployment on thin clients
- Investigated and implemented proof-of-concept algorithmic optimizations for polynomial multiplication using number-theoretic transforms with butterfly interleaving and fast modular operations for efficient lattice-based cryptographic operations

Subconscious Compute *Remote / Bengaluru, India*

System Engineer (Kernel) *Dec 2022 – Jan 2023*

- Created a systems hardening tool for user-defined seccomp-BPF filtering of syscalls spawned by userland applications on Linux to minimize the attack surface of the kernel and enforce the principle of least privilege
- Designed a wrapper around the Linux port of OpenBSD's pledge/unveil sandboxing mechanisms for restricting the operational capabilities of processes while granting access to essential filesystem paths
- Incorporated support for communicating through a Unix IPC socket to facilitate remote code interaction

Manuscripts

- *ATAVISM: Private Originator Tracing in End-to-End Encrypted Messaging* (with Debayan Gupta and Arup Mondal) (**Source**)

Projects

Applied Cryptography *Mar 2023 – Dec 2023*

- Implemented open-source toy variants of numerous cryptosystems and security protocols in Rust as proof-of-concept with minimal use of external libraries to verify correctness and demonstrate intrinsic understanding of their respective functionality (**Source**)

Secure Systems Administration *Jun 2021 – Feb 2023*

- Managed multiple hardened server nodes for securely hosting publicly available web services as Docker containers with support for real-time monitoring and Cloudflare tunneling
- Researched various solutions for reducing the exposed attack surface of Unix-based networked systems at the kernel and application layer

Write-ups

- A Privacy-Preserving CBDC Auditing Model using Pedersen Commitments, Filecoin and IPFS (**Source**)
- On the Foundations of Lattice-based Cryptography (**Source**)
- CCC: Applying Category Theory to Cryptography (**Source**)
- seccomp-pledge: Enforce principle of least privilege in Linux kernel (**Source**)

Volunteering

IIT Madras *Dec 2024*

- Coordinated and assisted in a lab session on public-key cryptography at the ACM winter school on cryptography

IITB Trust Lab *Jun 2024*

- Coordinated and led a lab session on Fully Homomorphic Encryption at the ACM summer school with specific focus on using OpenFHE's Python bindings for performing rudimentary algebraic operations

Indian Statistical Institute, Kolkata *Oct 2023 – Jun 2024*

- Helped a PhD student at ISI Kolkata with implementing a complete simulation of Sybil attacks in blockchain and statistical testing of image classification across ML models and probability distributions as part of their dissertation

Scholarships

- Research Excellence Program for Asia (RExPA) fellowship - *Tel Aviv University* (declined) *Mar 2024*
- Industry scholarship - *University of Zurich* *Jul 2023*

Certifications

Cryptography I *Stanford Online*

Skills

Rust · Python · Linux · Shell · Docker · WebAssembly · Typst · BSD · LaTeX · C/C++ · Vim · Nix · Javascript/Typescript · Circom · JSON

Awards

- Three-time SOF National Cyber Olympiad Gold Medalist and Class Topper *2016 – 2018*
- SOF National Cyber Olympiad International Rank 43, Zonal Rank 4 *2017*

Travel Grants

- RWC 2025 - granted by IACR *Mar 2025*
- TPMPC 2025 - granted by IISc *Feb 2025*
- Asiacrypt 2024 - granted by Trust Lab *Dec 2024*