



ADITYA MANE

Final Year Undergraduate
Indian Institute of Technology Kanpur

adityamane765
adityamane765@gmail.com
Portfolio LinkedIn

Year	Degree/Certificate	Institute	CPI/%
2023 - 2027	B.Tech (C.E.)	IIT Kanpur	7.8/10.0
2023	TSBIE (XII)	FIITJEE Jr. College, Hyderabad	92%
2021	CBSE (X)	New Vision Public School	96.5%

AWARDS & ACHIEVEMENTS

- Won **ETHOnline 2025** among 634 teams and the **Avail Nexus Best DeFi/Payments App** track prize
- Won the **Zama Builder Track** in Dec 2025 for building a decentralized privacy protocol with **TFHE-rs**
- Won multiple bounties across various ecosystems including **Ethereum, Solana, Starknet and Polkadot**
- Secured **All India Rank 5,999** in JEE Advanced 2023 among approximately **250,000** shortlisted candidates

WORK EXPERIENCE

Siphon Protocol

Founding Engineer

Oct '25 - Sep '26

- Designed and implemented a zero-knowledge **Groth16-based privacy pool**, covering deposits, note management, proof generation, and withdrawals
- Built a high-performance **RapidSnark proving relayer**, cutting withdrawal proving time from **~50s in-browser** to **sub-second** and simplifying private withdrawals
- Reduced wallet signature prompts from **7 to 2** using **ephemeral keys** for **auth delegation** and encrypted client-side storage across the end-to-end flow
- Designed and integrated a label-based **Association Set Provider workflow** for privacy-preserving compliance checks
- Integrated a **greedy note-selection algorithm** with the compliance model that satisfies withdrawal amounts while minimizing compliant notes consumed
- Built **privacy-safe Sentry observability** across Next.js and Python services, stripping spendable note secrets, request bodies, and stack-frame locals before export
- Provisioned **self-hosted Supabase on AWS EC2** with TLS and restricted service exposure; automated **age-encrypted, append-only S3 backups** and validated full restores

OPEN SOURCE WORK

DeFiLlama

Open-Source Contributor

- Authored **13 merged pull requests** across **5 repositories**, spanning bridge, yield, TVL, and chain-data pipelines
- Grouped /bridges volume lookups into one SQL query, removing roughly **100 database round trips per request**
- Added new API endpoints for **stale-bridge detection, bridge search, and cross-chain netflow comparison**
- Fixed unawaited writes and broken retries; added batched RPC calls, bounded concurrency, and **exponential backoff**

TECHNICAL SKILLS

- Languages:** Rust, TypeScript, Solidity, Circom, Python
- Cryptography:** ZK Proofs, FHE, elliptic-curve cryptography
- Web3 & Tooling:** Foundry, Hardhat, ethers.js, IPFS
- Development:** Node.js, Next.js, AWS, Git, SQL, Docker

RELEVANT COURSES

Applied Cryptography (CS698G)*
Applied Probability and Statistics (HSO201)*
Ordinary Differential Equations (MSO203)
Fundamentals of Computing I & II (ESC111 & ESC112)

PROJECTS

402.fhe

Apr'26 - May'26

- Built a **confidential x402 payment layer** using middleware routing, a shared escrow pool, and FHE to conceal which agent or user calls which API and how often
- Designed **non-bilateral state channels** with signed off-chain call proofs and batched settlement, avoiding per-call transactions
- Implemented **homomorphic conditional settlement** for buyer debits, merchant credits, and fees without decrypting balances
- Built **HTTP 402 challenge-response**, concurrency guards, and KMS-verified self-service withdrawals

Side-Channel Attack using CPA

Jul'25

Course Project, Prof. Udaya Parampalli

- Performed **Correlation Power Analysis on real hardware traces** using Hamming-weight leakage models and Pearson correlation to recover AES round-key bytes
- Reverse-engineered **8-bit and 32-bit AES implementations** to locate key-dependent leakage regions in the recorded traces
- Reconstructed the original encryption key by **reversing the AES key schedule** from recovered round-key bytes
- Compared **AddRoundKey** and **SubBytes** leakage, finding clearer correlation peaks from nonlinear S-box intermediates

CircuitForge

Feb'26

- Built a **visual ZK circuit editor** with 18 Blockly blocks for arithmetic, hashing, logic, constraints, inputs, and outputs
- Wrote a **Blockly-AST-Cairo pipeline** for type checks and real-time code generation from connected blocks
- Added **circuit testing**, gas estimation, data-flow visualization, and templates for hash, Merkle, and range proofs
- Built an **IPFS-backed circuit marketplace** for publishing and importing reusable designs by CID, alongside Scarb export and Starknet Sepolia deployment

Setmatch

Aug'26

- Implemented **mutual private set intersection** in Rust using a **commutative Diffie-Hellman protocol**
- Built a **prepare-respond-finalize CLI** that exchanges blinded curve points instead of plaintext values or ordinary hashes
- Added session-bound transcripts, malformed-point checks, protected state files, and **leakage-focused protocol tests**

POSITIONS OF RESPONSIBILITY

Senior Technical Member

Mar'24 - Apr'26

Society of Automotive Engineers, IITK Motorsports | IIT Kanpur

- Contributed to the team's **Overall National EV Champions** title at **Formula Imperial 2024**
- Secured **1st place in the Formula Bharat 2026 Rulebook Quiz** among 40+ FSAE teams across India
- Contributed to **chassis and aerodynamics research, design, and fabrication** for the team's formula student vehicle
- Designed **timelines and documentation** to streamline sub-system coordination and tracking, coordinated the recruitment process and onboarding of **44 junior team members**

i: ONGOING, *: EXCELLENT PERFORMANCE

Cryptographic Protocols (CS715)ⁱ
Linear Algebra (MTH113)
Partial Differential Equations (MTH114)
Multivariable Calculus (MTH111/112)