Varun Thakore

Cryptography Engineer, zkSecurity

vrnthakore@gmail.com
varunthakore.github.io
in/varunthakore
varunthakore

Research Interests

Theoretical and Applied Cryptography, Zero-Knowledge Proofs, Blockchain Technology, Privacy-Preserving Protocols.

Education

2021 – 2024	**Indian Institute of Technology Bombay**, Mumbai, India Master of Technology, Electrical Engineering	GPA: 9.33/10.0
2015 – 2019	**Sardar Patel College of Engineering**, Mumbai, India Bachelor of Technology, Electrical Engineering	GPA: 7.58/10.0

Publications

1 **V. Thakore** and S. Vijayakumaran, "MProve-Nova: A Privacy-Preserving Proof of Reserves Protocol for Monero," *Proceedings on Privacy Enhancing Technologies*, vol. 2025, no. 2, DOI: `10.56553/popets-2025-0078`.
Received the Distinguished Artifact Award (Runner-up)

Research Experience

2025–Present **Memory Checking Arguments over Binary Fields** *zkSecurity*
– Design a memory-checking argument over binary fields for verifying read/write operations.
– Encode accesses as tuples and enforce correctness via permutation and comparison check.
– Use multiset-equality techniques for permutation and a read-once branching program for ordering.
– Build a binary field PCS via ring-switching from an extension field PCS.

2022–2023 **Privacy-Preserving Proof of Reserves for Monero** *IIT Bombay*
Advisor: Prof. Saravanan Vijayakumaran | MTech Thesis | Accepted at PoPETs 2025
– Developed a privacy-preserving proof of reserves (POR) protocol for Monero, based on Nova.
– Implemented the protocol in Rust, working with non-native field arithmetic and Merkle trees.
– Achieved < 7 hr proving for 10,000 addresses, with constant 4.3 sec verification and 28KB proof.
– Proving scales linearly with addresses, while verification time and proof size remain independent.
– Designed a non-collusion protocol to prevent exchanges from colluding to generate the PoR.

2022 **Review of Elliptic Curve Pairings** *IIT Bombay*
Advisor: Prof. Saravanan Vijayakumaran | MTech Seminar
– Studied elliptic curves including their representations, group law and algebraic properties.
– Surveyed literature on bilinear pairings, including Weil pairing, Tate pairing, and Miller's algorithm.

Industry Experience

2024–Present **Cryptography Engineer** *zkSecurity*
Research and implement cryptography projects, audit and review cryptography codebases for security vulnerabilities and write technical blogs explaining complex concepts in an accessible way.

2021–2024 **System Administrator (Part-time), EE Department** *IIT Bombay*
Managed and upgraded department servers and network infrastructure, including migrating mail, web and authentication services to virtual machines and ensuring their smooth, secure operation.

2019–2021 **Proposals Engineer - Hybrid and Energy Storage** *Sterling and Wilson Pvt Ltd*

Selected Projects

2025 **zkVM Fuzzing for Detecting Security Vulnerabilities** | *Ongoing Project* *zkSecurity*
– Design novel fuzzing techniques to detect soundness and completeness bugs in RISC-V zkVMs.
– Implement an automated testing framework to improve security and reliability of zkVMs.

S-two Book *zkSecurity*
– Wrote documentation detailing the theory and implementation of StarkWare's S-two (Circle STARK) prover.
– Explained the system architecture, protocols and proving pipeline for clarity and developer understanding.

zkVM Benchmarks *zkSecurity*
– Built a benchmarking suite to compare performance across multiple zkVM implementations.
– Designed workloads to measure proof generation time, verification time, proof size and memory usage.

2024 **Pumice: Rust Implementation of Stone Prover** *zkSecurity*
– Implemented a portable Rust version of StarkWare's Stone Prover, translating key C++ components.
– Studied and implemented code-based commitment schemes (FRI Protocol) to ensure correctness.

Nova EdDSA: High Throughput Ed25519 Signature Verification *IIT Bombay*
– Implemented R1CS circuit for Ed25519 signature verification with field emulation and proving with Nova.
– Enabled efficient batch verification: 32 signatures in 68 sec proving time, with < 1 sec verification, 11KB proof.

2023 **Nova SHA-512** *IIT Bombay*
Won the ZK MOOC Hackathon
– Implemented the SHA-512 compression function as R1CS circuit, followed by proof generation using Nova.
– Achieved 5.9 sec proving time, 10KB proof size and 268 millisec verification for 64-byte inputs.

R1CS Circuits for Merkle Tree Variants *IIT Bombay*
– Implemented R1CS circuits for regular Merkle trees to verify inclusion proofs using bellpepper.
– Extended to indexed Merkle trees with efficient insertion, inclusion, and non-inclusion verification circuits.

Technical Writings

2025 **Circle Group** *zkSecurity Blog*
Authored educational content on the foundations of circle groups and polynomials with animations.

Circle FFT *zkSecurity Blog*
Developed comprehensive guide to FFT algorithms on circle groups with SageMath implementations.

Circle FRI *zkSecurity Blog*
Authored technical exposition of the Circle FRI protocol and Circle STARK proving system.

KZG Polynomial Commitment Scheme *zkSecurity Blog*
Wrote comprehensive guide to KZG commitments, covering batched and zero-knowledge variants.

2023 **Understanding Field Extensions** *Personal Blog*
Developed educational tutorial on finite field extension construction using irreducible polynomials.

Teaching Experience

2022 **Teaching Assistant, ACM Winter School on Digital Trust** *Trust Lab, IIT Bombay*
Instructor: Prof. Saravanan Vijayakumaran
– Conducted hands-on workshop sessions on Smart Contract Development for 50+ students.
– Delivered tutorials on Solidity programming and deployment using Remix IDE and Hardhat.

Honors and Awards

2025 **PETS 2025** – Distinguished Artifact Award (Runner-up)
2024 **ZK Hack IV** – Ranked 11th globally in a competitive cryptography puzzle competition
2023 **2nd Prize, ZK MOOC Hackathon** – Hosted by UC Berkeley with 600 participants from 60+ countries
2021 **Finalist, Shell.ai Hackathon** – Selected from 2,000 registrations across 50+ countries