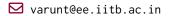
# **Varun Thakore**

MTech(RA), EE, IIT Bombay



varunthakore.github.io





## **Research Interests**

Applied Cryptography, Zero-Knowledge Proofs, Blockchains

### **Education**

2021 - 2024	<b>Indian Institute of Technology Bombay</b>	GPA = 9.04/10.0
(expected)	Master of Technology, Electrical Engineering.	
	Specialisation in Communication Engineering.	
2015 – 2019	Sardar Patel College of Engineering	GPA = 7.58/10.0
	Bachelor of Technology, Electrical Engineering.	

## **Publications and Drafts**

MProve-Nova: A Privacy-Preserving Proof of Reserves Protocol for Monero Varun Thakore and Saravanan Vijayakumaran.

# **Research Experience**

2022-23 Proof of Reserves for Monero 🕻 🗘

EE, IIT Bombay

Prof. Saravanan Vijayakumaran | MTech Project - Stage I

- Developed a **privacy-preserving** proof of reserves (POR) protocol for Monero based on **Nova**, such that the exchanges do not reveal the addresses and the amounts that they own.
- Implemented it in **Rust** which involves working with **non-native field** and **Merkle trees**.
- The protocol has a proving time of about **8Hrs** for **10,000** addresses. The verification time **(2.19s)** and proof size **(12KB)** are **constant** irrespective of the number of addresses.
- Implemented a **non-collusion** protocol to prevent exchanges from colluding to generate POR.
- 2022 Review of Elliptic Curve Pairings

EE, IIT Bombay

Prof. Saravanan Vijayakumaran | MTech Seminar

- Studied **elliptic curves** including their representations, **Group law** and other properties.
- Surveyed literature on **bilinear pairings** including **Divisors** which are used to define pairings, **Weil pairing**, **Tate pairing** and **Miller's Algorithm** which is used to compute pairings.
- 2023-\* Proof of Reserves for ERC-20\*

EE, IIT Bombay

Prof. Saravanan Vijayakumaran | MTech Project - Stage II

- Study **Ethereum** transactions, types of accounts and data stored within a block.
- Design a **privacy-preserving** proof of reserves protocol for ERC-20 tokens based on **Nova**.
- Write rank-1 constraint system for **Keccack-256**, ECDSA signature verification on **secp256k1** and proof of membership for **Merkle Patricia trie** using bellpepper Rust library.

\*Currently in progress

# Work Experience

2021–24 System Administrator (Part-time), EE Department

EE, IIT Bombay

- **Headed** the transition of department Mail, Proxy, LDAP and Web Servers from Physical systems to **Virtual Machines** using virtualization platforms like **Proxmox VE**.
- Responsible for configuring and securing Dept. Mail Servers and Network Infrastructure.
- 2019-21 Proposals Engineer Hybrid and Energy Storage

Sterling and Wilson Pvt Ltd

## **Key Projects**

2023 Nova SHA-512 (7) D

Guide: Prof. Manoj Prabhakaran

Course Project: Cryptography and Network Security (Submitted at ZK MOOC Hackathon)

- Implemented R<sub>1</sub>CS for computation of **SHA-512** using **Rust** and **bellpepper** library. Number of constraints for SHA-512 compression function are **67,123**.
- Studied **Nova** folding scheme, used to fold two R<sub>1</sub>CS instances into one. Implemented **SHA-512 compression function** as the step function within the Nova computation.
- For input of size **64 bytes**, proving time is **5.9s**, proof size is **10KB** and verification time is **268ms**.

Guide: Prof. Manoj Prabhakaran

Course Project: Adv. Tools from Modern Cryptography

- Implemented R<sub>1</sub>CS circuit for **ECDSA** signature verification on **secp256k1** curve using **Rust** and **bellpepper** library. Involves writing circuit for curve operations in the base field of **secp256k1**.
- Circuits for point addition and scalar multiplication implemented in **36** and **3343** number of constraints, respectively and circuit for signature verification implemented in **3389** constraints.
- 2022 Data Augmentation using Generative models

Guide: Prof. Sunita Sarawagi

Course Project: Advanced Machine Learning

- Employed CGAN & VAE to generate novel data, diverging from conventional data augmentation.
- Analyzed the effect of data augmentation on variable size MNIST dataset using CNN classifier.
- Observed an accuracy improvement of **82.74**% with **VAE** model and **78.77**% with **CGAN** model, in contrast to **78.34**% accuracy without augmentation, with a training set size of **100** samples.
- 2021 📕 Cloud Cover Prediction Shell.ai Hackathon 📙

Guide: Prof. Preethi Jyothi

Course Project: Foundations of Machine Learning

- Cloud coverage impacts Solar PV power production. The task was to use **time series forecasting** techniques to predict cloud cover for next 20, 60, 120 minutes using the given historical data.
- Implemented several models including Linear Regression, Multi Layered Perceptron and Long Short Term Memory Networks. Achieved an accuracy of 89.44% using MLP.

### **Extracurricular Activities**

- Won 2<sup>nd</sup> prize for "Category 2: Circuits/R1CSs for Recursive SNARKs" of ZK MOOC Hackathon hosted by UC Berkeley RDI, which had 600 participants from over 60 countries.
- Teaching Assistant, ACM Winter School on Digital Trust, Trust Lab, IIT Bombay
  Teaching Instructor: Prof. Saravanan Vijayakumaran
  - Assisted in conducting a workshop on **Smart Contract Development** for over **50** students.
  - Workshop covered Solidity, compiling & deploying contracts using Remix IDE and Hardhat
- Finalist in Shell.ai Hackathon 2021 which had 2,000 registration from more than 50 countries.

### **Technical Skills**

Programming Rust, Python, Bash, Solidity, C, C++

Software & Tools | Bellpepper, Arkworks, Git, Lagrange, Pytorch, NumPy, Pandas, SciPy and Matplotlib

### **Relevant Coursework**

Cryptography and Network Security Adv. Tools from Modern Cryptography Game Theory and Mechanism Design Foundations of Machine Learning Advanced Machine Learning Information Theory and Coding Error Correcting Codes Communication Networks Statistical Signal Analysis