Suyash Bagad

Contact Information

Bharti Centre for Communication
Department of Electrical Engineering
Indian Institute of Technology, Bombay
Mumbai - 400076, India

(+91) 750-741-0474
suyashbagad@iitb.ac.in
suyash67.github.io/homepage
github.com/suyash67

Research Interests

Applied Cryptography, Cryptocurrencies, Security & Privacy in Blockchain, Zero-Knowledge Proofs

Education

Indian Institute of Technology, Bombay, Mumbai, India — *Grade* (CPI): 8.80/10.0
Bachelor and Master of Technology, Electrical Engineering — Aug, 2015 - June, 2020

- Specialising in Communication and Signal Processing (Specialisation CPI: 9.52/10.00)
- Awarded *Undergraduate Research Award* (among 1% in the batch) for outstanding work in thesis
- Minor in Management Studies

Publications

[1] Performance Trade-offs in Design of MimbleWimble Proofs of Reserves [Paper, Code]
Accepted at *IEEE Security & Privacy on Blockchain (IEEE S&B)*, 2020
Suyash Bagad and Saravanan Vijayakumaran.

[2] On the Confidentiality of Amounts in Grin [Paper, Slides, Video]
Presented at *Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2020
Suyash Bagad and Saravanan Vijayakumaran.

[3] MProve+: Privacy-Enhancing Proof of Assets Protocol for Monero
In preparation for submission to *IEEE Trans. on Information Forensics & Security* (IF: 6.21)
Arijit Dutta, **Suyash Bagad** and Saravanan Vijayakumaran.

[4] A Proof of Reserves Protocol with Short Proofs and a Method to Estimate Amount Upper Bounds for MimbleWimble (*Master's Thesis*) [Report, Slides, Video]
Suyash Bagad.

Research Experience

Shorter Privacy-Preserving Proof of Reserves Protocols and More — Master's Thesis
Guide: Prof. Saravanan Vijayakumaran, IIT Bombay

MimbleWimble-based Cryptocurrencies [Report, Slides, Code] — May, 2019 - Jan, 2020

- Designed *RevelioBP*, a novel proof of reserves protocol for MimbleWimble-based cryptocurrencies
- Accomplished a proof size of $\mathcal{O}(\log(n))$ in the anonymity set size, *outperforming* $\mathcal{O}(n)$ of the existing state-of-the-art proof of reserves (PoR) protocol Revelio
- Strengthened the *privacy* of an exchange's outputs (addresses) by scaling the anonymity set to the entire set of unspent outputs (UTXOs) for a particular *blockchain state*
- Devised a robust cryptographic technique to enforce non-sharing of outputs by exchanges
- Implemented the protocol from scratch in Rust over secp256k1 curve; achieved 3X *faster* proof verification than generation using a single multi-exponentiation check

CryptoNote-based Monero — Jan, 2020 - Present

- Conceptualized *MProve+*, a *log-sized* PoR for Monero outclassing the state-of-the-art MProve
- Alleviated a privacy flaw of MProve to prevent zero mix-in transactions of exchange's addresses
- Implemented MProve+ and MProve from scratch in Rust over Edwards and Ristretto curves
- *Boosted* proof generation and verification in MProve+ by 5X and 20X using multi-exponentiation
- Exhibited conversion of Monero keys from Edwards to Ristretto to avert small subgroup attack

Confidentiality of Amounts in Grin — Feb, 2020 - April, 2020

- Derived *upper bounds* on the amounts hidden in the outputs (Pedersen commitments) of Grin
- Performed a first-hand *graph*-based analysis of the Grin blockchain using graph database Neo4j
- Identified 983 (out of 110,149) UTXOs which hide ≤ 1800 grin ($\approx$ \$800) proving that the transaction structure could reveal amount information in perfectly hiding Pedersen commitments

Generalising Bulletproofs [Report, Slides] Jan, 2019 - Apr, 2019

- Surveyed a variety of range proofs with a focus on Bulletproofs, the state-of-art range proof
- *Generalized* Bulletproofs for proving knowledge of aggregated statements with DL assumption

Open Source Contributions - Bulletproofs+ and More [GitHub] May, 2020 - Jun, 2020

- Implemented aggregated Bulletproofs+, a novel range proof technique building on Bulletproofs
- Speeded up verification of Bulletproofs and Bulletproofs+ by 30% using multi-exponentiation
- Formulated and implemented Inner-Product argument and Weighted Inner-Product argument for secret vectors of any general size (including non-powers of 2) upto 2^{64}

Neuromorphic Computing R&D Project

Guide: Prof. Udayan Ganguly, IIT Bombay

Dynamic Boltzmann Machines (DyBM) [Report, Slides] Jan, 2019 - April, 2019

- Devised an initial framework for *hardware* realisation of energy-based models of DyBMs
- Modelled neuronal dendrites and axons as the *eligibility traces* and *conduction delays* respectively to draw parallels between DyBMs and biological neuronal networks
- *Outperformed* LSTMs in time-series prediction with comparable accuracy and 40X faster learning

Plasticity-based Learning in DNNs [Report, Poster] Aug, 2019 - Nov, 2019

- Incorporated brain-inspired *Hebbian plasticity* in DNNs boosting *performance*, *memory footprint*
- Proposed a training strategy for the plasticity-fused models using back-propagation resulting in accuracy comparable to that of the state-of-the-art CNNs
- Manifested superior *noise robustness* in pattern recongnition and image classification tasks

Professional Experience

Cadence Design Systems | Fast 3D Convolution on HiFi4™ DSP Pune, India

Guide: Mr.Vijay Pawar, Principal Design Engineer May, 2018 - Jul, 2018

- Devised algorithms to implement *optimal* 3D and Depth Separable Convolution on HiFi4 DSP
- Achieved 40x and 24x *faster* fixed and floating-point implementations respectively compared to high-level C++ implementation of 3D convolution on HiFi4
- Designed efficient modules to implement CNN models on HiFi4 for Automatic Speech Recognition

Academic Projects

Neurapse - An open-source Spiking Neural Network package [GitHub]

Guide: Prof. Udayan Ganguly, IIT Bombay Aug, 2018 - Nov, 2018

- Synthesized an open-source python package equipped with fundamental blocks of biologically-inspired Spiking Neural Networks such as spikes, neurons, synapses and networks
- Adaptive to neuronal models like LIF, AEF, HH & STDP rules for Dynamic Random Networks
- Easily extensible and customizable to support computational simulation of neuronal networks

Enhancement of Low-light and Hazy Images [Report, Slides]

Guide: Prof. Amit Sethi, IIT Bombay Aug, 2018 - Nov, 2018

- Designed algorithms for hazy image enhancement using Luminance map and Dark Channel Prior
- Accomplished 12x *faster* implementation in luminance approach enabling real-time processing in applications such as automated surveillance, remote sensing and medical imaging

Mathematical Analysis of Financial Crises [Slides]

Guide: Prof. Jayakrishnan Nair, IIT Bombay Aug, 2018 - Nov, 2018

- Presented analysis of reasons like model uncertainty, flawed assumptions behind financial crises
- Explained the emergence of the financial crisis of 2008 due to CDOs using Banach-Tarski theorem
- Illustrated failure of VaR (Value at risk) as a measure of *heavy-tailed* risks in financial crisies via Dalbaen's theorem and stressed on cruciality of *convexity* of risk measure

Smart-shoes for Physiotherapy Diagnosis [Report, Slides]

Guide: Prof. Siddharth Tallur, IIT Bombay Jan, 2018 - Apr, 2018

- Fabricated a low-power, wireless *shoe-sole* for diagnosing physiotherapeutic disorders like flatfoot, costing 24X lesser than conventional pressure mats
- Demonstrated the heat-map of a patient's foot for continuous remote-monitoring of patients

Achievements

Awarded 10/10 grade in all *five* credit research projects including the thesis project 2020
Selected participant in workshop *Foundational Aspects of Blockchain Tech*, TIFR, Bangalore 2020
Commendation by the **Dean, Student Affairs** for exceptional contribution to NSS, IITB 2018
Bagged 99.4% and 99.9%ile in **JEE** Advanced and JEE Main resp. in 1,500,000 candidates 2015
Kishore Vaigyanik Protsahan Yojana Fellowship, ranked 251^{st} in 100,000 candidates 2014

Notable Coursework

Applied Math	**Signal Processing**	**Miscellaneous**
Number Theory & Cryptography	Computer Vision	Intro to Machine Learning
Advanced Cryptography†	Image Processing	Neuromorphic Engineering
Real Analysis in Engineering	Digital Signal Processing	Complex Analysis

Teaching Assistance

Introduction to Number Theory & Cryptography (130) Jan, 2020 - Present
Cryptocurrency and Blockchain Technologies (22) Aug, 2019 - Nov, 2019
Instructor: Prof. Saravanan Vijayakumaran, IIT Bombay

- Responsible for evaluation of assignments, exams and designing model solutions of the same
- Mentored students with the course content and the project implementation

Computer Skills

Programming					
Python	● ● ● ● ●	Rust	● ● ● ● ○	C++	● ● ● ○ ○
C#	● ● ● ○ ○	LaTeX	● ● ● ● ●	SQL	● ● ● ○ ○
Packages and OS					
Curv (Rust)	● ● ● ● ○	Matlab	● ● ● ● ○	OpenCV	● ● ● ● ○
Dalek-Crypto (Rust)	● ● ● ○ ○	Neo4j	● ● ● ○ ○	Xtensa (Cadence)	● ● ● ○ ○
TI CCS	● ● ● ○ ○	Linux	● ● ● ● ○	Windows	● ● ● ● ○

Postions of Responsibility

Overall Coordinator, National Service Scheme, IIT Bombay Apr, 2018 - Mar, 2019
Largest student-volunteer body in IITB serving 100,000+ people | Led a 3-tier team of 400 volunteers

Outreach
- Guided 1000+ freshmen to help choose NSS for course NOCS presenting the impact of our work
- **O**pen **L**earning **I**nitiative's (1L+ subs) videos hosted on several MHRD and state govt. portals
- Led 'Letters of Love' in IITB, a global campaign for motivating refugee kids in Syria, Iraq, Iran

Initiatives
- Collaborated with *Nalanda project* to educate 5000+ needy kids across India using OLI videos
- Pioneered *field visits* encouraging 50+ farmers to save water using smart farming technologies
- Launched *Tarang*, a YT channel to sensitize youth on sustainability, impacting 750+ BMC kids

Reforms
- Introduced *Sustainable Social Development* focusing on imbibing sustainability in our lifestyle
- Revamped NSS website (105% rise in visits), initiated NSS Instagram handle (500+ followers)
- Accentuated *conservation* of nature via Green Diwali, Plastic & paper reuse and tree-plantation

Extra Curricular Activities

- Educated students of grades 3th to 12th as a volunteer under National Service Scheme (NSS)
- Elementary proficiency in *French*, completed 5 year long course in French Language in school
- Qualified *Elementary* & *Intermediate* Drawing Examinations with grades *A* and *B* respectively
- Completed the Beginners' Squash Camp and participated in the 'Freshie Squash Open 2015'