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

Research Interests

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

Education

Indian Institute of Technology, Bombay, Mumbai, India
Bachelor and Master of Technology, Electrical Engineering — Aug, '15 - Jun, '20 (*Expected*)

- Cumulative Performance Index (CPI): 8.70/10.00
- Specialising in Communication and Signal Processing

Publications

[1] Revelio+: An Efficient MimbleWimble Proof of Reserves Protocol
Under review at *International Conference on Financial Cryptography and Data Security, 2020*
Suyash Bagad and Saravanan Vijayakumaran.

Research Experience

Efficient Proof of Reserves for Cryptocurrency Exchanges — Master's Thesis
Guide: Prof. Saravanan Vijayakumaran, IIT Bombay

MimbleWimble-based Cryptocurrencies — May, 2019 - Sept, 2019

- Designed *Revelio+*, a novel proof of reserves protocol for MimbleWimble-based cryptocurrencies *scalable* to the entire Blockchain
- Accomplished a proof size of $\mathcal{O}(\log(n))$ in the anonymity set size, *outperforming* $\mathcal{O}(n)$ of the only existing proof of reserves protocol Revelio, thus enabling frequent audits by exchanges
- Strengthened the *privacy* of an exchange's outputs (addresses) by scaling the anonymity set to the entire set of UTXOs for a particular *blockchain state*
- Enhanced *non-collusion* guarantees between exchanges by linking blockchain state to the proof of reserves, solving a major drawback of Revelio

Monero — Jul, 2019 - present

- Conceptualized a *complete privacy-preserving* proof of reserves protocol for Monero, overcoming the limitations of MProve, the first proof of reserves for Monero
- Addressed the issue of revealing key-images in MProve to achieve *better privacy* of exchange-owned addresses, which was absent in MProve
- Proposed an alternative way to solve the above issue using accumulator and cross-domain proofs
- In process of submitting the findings to *Privacy Enhancing Technologies Symposium, 2020*

Bulletproofs — Jan, 2019 - present

- Surveyed a variety of range proofs with a focus on Bulletproofs, the state-of-art range proof
- Reviewed the Omniring (a RingCT protocol for Monero) framework to analyze the extension of Bulletproofs in construction of a ring signature
- Presented a *generalization* of Bulletproofs for proving knowledge of aggregated statements based on Discrete-Logarithm and Decisional Diffie-Hellman assumptions
- Currently working on devising a protocol for *secure* outsourcing of Bulletproofs' proof generation to a cloud for addressing the practical issues with $\mathcal{O}(n)$ proof generation time

Bitcoin — May, 2019 - Jun, 2019

- Proposed inclusion of P2PKH addresses in Provisions, the first proof of reserves for Bitcoin using *Cross-domain* proofs, making Provisions more practical for exchanges

Neuromorphic Computing R&D Project
Guide: Prof. Udayan Ganguly, IIT Bombay

Dynamic Boltzmann Machines Jan, 2019 - April, 2019

- Analyzed energy-based models of Dynamic Botlzmann Machines and devised an initial framework for its *hardware* realisation
- Modelled neuronal dendrites and axons as the *eligibility traces* and *conduction delays* respectively to draw parallels between Dynamic Boltzmann Machines and biological neuronal networks
- *Outperformed* LSTMs in time-series prediction with comparable accuracy and 40x faster learning

Plasticity-based Learning in DNNs Aug, 2019 - Nov, 2019

- Incorporated brain-inspired *Hebbian plasticity* in Deep Neural Networks enhancing *performance* coupled with drastic reduction in *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
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
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
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 times of financial crisis via Dalbaen's theorem and stressed on cruciality of *convexity* of risk measure

Smart-shoes for Physiotherapy Diagnosis
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
- Built an inteface showing the heat-map of a patient's foot for continuous remote-monitoring of the patient's progress and gauge the effects of medication, using Bluetooth communication

Filter Design & Mono to Stereo Audio Conversion
Guide: Prof. Vikram Gadre, IIT Bombay Feb, 2018 - Apr, 2018

- Designed & simulated a series of discrete-time filters to extract/suppress given bands of a signal
- Explored FIR filter based *mono to stereo* conversion in time for audio quality enhancement

Achievements

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
Maharashtra Talent Search Examination Scholarship 2011

Computer Skills

Programming					
Python	● ● ● ● ●	C++	● ● ● ● ○	Rust	● ● ● ○ ○
C#	● ● ● ○ ○	LaTeX	● ● ● ● ●	VHDL	● ● ○ ○ ○
Packages and OS					
Curv (Rust)	● ● ● ● ○	Matlab	● ● ● ● ○	OpenCV	● ● ● ● ○
Scilab	● ● ● ● ○	TI CCS	● ● ● ○ ○	Quartus	● ● ○ ○ ○
Linux	● ● ● ● ●	Windows	● ● ● ● ○	SolidWorks	● ● ● ○ ○

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
- 15% increase in participation, started volunteering in 2 new NGOs, 3 sensitization workshops
- 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

Media & Design Head, National Service Scheme, IIT Bombay Apr, 2017 - Mar, 2018

- Worked in a 12-member Core Team in planning & executing several public welfare activities
- Led a team of 4 for outreach of NSS initiatives through social, print media impacting 3L+ people
- Innovated & organized the 1^{st} ever *NSS Summit* for collaborative work; 15 colleges participated

Teaching Assistant, Cryptocurrency and Blockchain Technologies
Instructor: Prof. Saravanan Vijayakumaran, IIT Bombay Aug, 2019 - Nov, 2019

- Appointed as the sole TA, mentoring students with the content and the project implementation
- Responsible for evaluation of assignments, exams and designing model solutions of the same

Notable Coursework

Applied Math	**Signal Processing**	**Miscellaneous**
Number Theory & Cryptography	Computer Vision	Intro to Machine Learning
Introduction to Optimization	Image Processing	Neuromorphic Engineering
Real Analysis in Engineering	Digital Signal Processing	Complex Analysis
Matrix Computations	Error Correcting Codes	Strategic Management

Extra Curricular Activities

- Educated students of grades 3th to 12th as a volunteer under National Service Scheme (NSS)
- Volunteered in *Cashless India Awareness campaign* as per the directive of the MHRD, GoI
- Elementary proficiency in *French*, completed 5 year long course in French Language in school
- Completed the Beginners' Squash Camp and participated in the 'Freshie Squash Open 2015'
- Former inter-school district-level cricketer for years 2012-13