Pratyush Ranjan Tiwari

Email : pratyushranjan.tiwari@gmail.com
Webpage: www.pratyush.site

I am a first year PhD student at Johns Hopkins University under the wonderful supervision of both Abhishek Jain and Matt Green. I am in general interested in cryptography and its applications, more specifically, verifiable computation, cryptography in the presence of quantum computers and privacy-preserving techniques. I am particularly interested in designing protocols with minimal trust requirements.

Education

- **Johns Hopkins University** Maryland, USA
  Ph.D. Computer Science *August 2020 - TBD*
- **Ashoka University Scholars Program** Haryana, India
  1 year PG by research (GPA 3.9/4.0) *August 2019 – May 2020*
- **Ashoka University** Haryana, India
  B.Sc. CS & Math (GPA: 3.6/4.0) *August 2016 – May 2019*

Research and Publications

- **CryptoWills: How to Bequeath Cryptoassets** pdf
  IEEE Security & Privacy on the Blockchain *2020*
- **SoK: A Billion Souls: A Security & Privacy Review of India's "Aadhaar" Biometric ID** pdf
  Manuscript in Preparation *2020*
- **Trading Accumulation Size for Witness Size in Merkle Tree Based Universal Accumulators** pdf
  IACR Eprint, under submission *2019*

Experience

- **New York University Abu Dhabi** Remote
  Cryptography Researcher @CSP Lab *June 2020 - July 2020*
  - **Proofs of Deletion**: Working on improving proofs of data deletion to enable a better, more private internet with Prof. Christina Poepper's group.
- **Thesis work on Cryptographic Accumulators** Ashoka University
  Under Prof. Mahabir P Jhanwar *November 2018- May-2020*
  - **Trading Accumulation Size for Witness Size: A Merkle Tree Based Universal Accumulator via Subset Differences**: Merkle tree based accumulator with guaranteed less than logarithmic membership and non-membership verification. Available on IACR eprint: **(link)**
  - **A full Implementation of Zero Knowledge Accumulators**: C and C++ based implementation of the Asiacrypt(2015) paper titled "Zero-Knowledge Accumulators and Set Operations". Pairing based operation are enabled by the PBC library in C and big integer arithmetic enabled by the NTL library in C++. This is the only public implementation of zero knowledge accumulators. **(Repository Link)**
- **Celo** Berlin, Germany
  Cryptography Engineering Intern *May 2019 - Aug 2019*
  - **Ultralight Client Sync**: Celo's Ultralight Client Sync enables users to download very small number of block headers to verify correctness of current validator set.
  - **Hash to Group**: Worked on the problem of making sure the Hash outputs are group elements. Celo uses Pedersen hashes. Implementation of Pedersen Hashes in *Rust* and *Sage* similar to the ZCash Protocol.
  - **Elliptic Curve Implementation**: Implemented Twisted Edwards and Montgomery Elliptic Curves in Sage.
  - **Cryptography Workshops**: Conducted Cryptography Workshops to help the organization understand the nuances of Elliptic Curves and Zero Knowledge Proofs. Made complex material accessible to employees with very different backgrounds.
- **Celo** celo.org
  Fellow *November 2018 - Feb 2018*

- ○ **Privacy Preserving Eigenvalue Computation**: Celo's algorithmically volume regulated stablecoin protocol requires each user to calculate their own Eigentrust score. Developing an efficient Zero Knowledge protocol to enable this. **Youngest fellow** among all the Celo fellows. Usually fellows are advanced Graduate students.

- **Dunya Labs** dunyalabs.io
  Blockchain Research Intern *Aug 2018 - Feb 2018*
  - ○ **Stablecoins**: Analysis of various stablecoins in different market condtions, attacks on security and robustness of stablecoin systems. Comparing existing and up and coming stablecoin models based on metrics we decided. Prepared a 7000 word comparison whitepaper. Secure link available on request to read the whitepaper.
  - ○ **Non- Interactive Zero Knowledge Proofs**: Explored possible applications of ZK Snarks on various chains. Possibility of off-chain computations using Zero Knowledge.
  - ○ **Protocol Analysis**: Deep dive into protocols of major and promising blockchain systems like Ethereum, EOS, ZCash, Tezos.
  - ○ **Eclipse testing**: Eclipse is a tool on the EOS blockchain to help users stake their tokens automatically. Wrote python code to test best ways to stake.
- **IIT Madras** Chennai, India
  Summer Research Intern *June 2018 - July 2018*
  - ○ **Cryptanalysis of Stream Ciphers**: Cryptanalysis of Stream Ciphers like Grain 128 and Trivium under Prof. Santanu Sarkar.
  - ○ **855-round key recovery attack on Trivium**: Worked alongside PhD students to implement 855-round key recovery attack on Trivium. Implementations in *C* and *Sage*.
- **Indian Academy of Sciences** Chennai, India
  Summer Fellow *May 2018 - June 2018*
  - ○ **Network Analysis of Indian stock markets**: Research on Network Analysis of pre and post crisis Indian stock markets using the Graph Networks. Focusing on the highest market cap companies listed at NSE. Performed network analysis using R.

Theoretical Projects

- **Cryptanalysis of NIST SHA-3 Finalists** Ashoka University
  Under Prof. Sumit Kumar Pandey *Jan 2018- April 2018*
  - ○ : Understood and presented existing techniques for Cryptanalysis of NIST SHA-3 Finalists
- **Independent Study Module** Ashoka Univeristy
  Combinatorial Optimization and Algorithms under Prof. Udayan B Darji *Aug 2017- Dec 2017*
  - ○ **Algorithms for Load Balancing problems on paths**: Studied combinatorial optimization problems under Prof. Udayan B Darji. Final project on Algorithms for Load Balancing problems on paths.

Teaching Experience

- **Teaching Assistant: Fall 2019** Ashoka University
  For Prof. Debayan Gupta *Aug 2019- Dec 2019*
  - ○ **A New Geography in the Information Age**: TA for this course based on technology scalability issues, ethics of AI, Cryptocurrency regulations.
- **Teaching Assistant: Spring 2020** Ashoka University
  For Prof. Debayan Gupta *Jan 2020- May 2020*
  - ○ **Computer Security and Privacy** : Will be holding Discussion Sections, advising all the projects for this course. This is a required course at Ashoka University and always has higher than average class size

Applied Projects

- ○ **NBA Game Results Predictor**: Achieved 89% accuracy in predicting 2018 season games using 2014-2017 statistics for training a deep neural network. Highest of all reported models online.
- ○ **Saarthi: Chatbot for Ashoka University**: A Natural language processing based chatbot for Ashoka University built using Dialogflow, Python and Heroku.

Programming Skills

- **Languages**: Python, Rust, C, C++, SAGE, MATLAB, R, Solidity

Achievements

- **Dean's List**: On the Dean's merit list for 4 out of 6 semesters attended at Ashoka University
- **FAST-SF Summer Fellowship** : Selected among top 30 students from all over India as the recipient of Focus Area in Science and Technology Summer Fellowship 2018
- **ACM ICPC Amritapuri regionals** Top team at Ashoka University for International Collegiate Programming Contest 2017