PRATYUSH RANJAN TIWARI

CS PhD student @ Johns Hopkins University

pratyush@cs.jhu.edu www.pratyush.site

PUBLICATIONS

Conference Proceedings

- with, G. Beck, A. R. Choudhari, M. D. Green, and A. Jain (2023). "**Time-Deniable Signatures**: Formalizing and proposing a signature scheme such that signatures allow authentication up until some time in the future and not indefinitely." In: *Privacy Enhancing Technologies Symposium (PETS) '23*. Link to eprint. .
- with, D. Agrawal, P. Jain, S. Dasgupta, P. Datta, V. Reddy, and D. Gupta (2022). "**India's "Aadhaar" Biometric ID: Structure, Security, and Vulnerabilities**: Systematizes this massive citizen identification system for India. Uncovers the most impactful vulnerabilities on Aadhaar till date by leveraging some cryptographic flaws." In: *Financial Cryptography (FC) '22*.
- with, D. Feist, D. Khovratovich, M. Maller, and K. Olson (2022). "**Not So Slowth: Invertible VDF for Ethereum 2.0**: We present a VDF protocol that incorporate challenging requirements from the Ethereum ecosystem, which includes low-latency proof generation and VDF hardware that is both inexpensive and secure in post-quantum settings." In: *Stanford's Science of Blockchain Conference (SBC) '22*.
- with, I.A.Seres, and O. Shlomovits (2020). "**CryptoWills: How to Bequeath Cryptoassets**: Providing secure and private solutions to the problem of distributing cryptoassets to beneficiaries (declared in a will) post death." In: *IEEE Security & Privacy on the Blockchain @ EuroS&P 2020*.

Pre-prints Under Submission

- with and M. D. Green (2022). ***Algorithm-Substitution Attacks on Cryptographic Puzzles**: Cryptographic puzzles are heavily used as a building block for the consensus networks used by cryptocurrencies, where they include primitives such as proof-of-work, proof-of-space, and verifiable delay functions (VDFs). We propose attacks and defenses against black-box implementations of puzzle solving devices.* Link to eprint. .

EXPERIENCE

Research Grantee

Ethereum Foundation & 0xPARC

Mar 2022 - July 2022 Remote

- Research on verifiable machine learning using zero-knowledge proofs. Attended 0xPARC's working group on applied zk engineering. Repository with work on zk decision trees: zkDT. Blog post introducing the underlying ideas: zkML

Research Grantee/Intern

Ethereum Research

May 2021 - August 2021 Remote

RESEARCH PHILOSOPHY

"Solve challenging problems that scale to impactful applications"

EDUCATION

Ph.D. in CS

Johns Hopkins University

Sept 2020 – June 2025

Working under the wonderful supervision of Matthew Green and Abhishek Jain on applied cryptography research.

Post-Baccalaureate (Research)

Ashoka University

Sept 2019 – May 2020

Thesis on "Cryptographic Accumulators: Properties and Efficiency Improvements". Graduated Summa Cum Laude.

B.Sc. in Math & CS

Ashoka University

Sept 2016 – May 2019

Made the Dean's Merit List on most semesters attended.

ACCOMPLISHMENTS

Undergrad Research Excellence Award
Given by the CS dept. at Ashoka University to the graduating student with the best track record in academic research, evaluated on the basis of publications and thesis quality.

Celo Fellowship Grant 2018-19
Youngest fellow among all the Celo fellows. Usually fellows are advanced Graduate students. Received a $10,000 grant to work on "Privacy Preserving Eigenvalue Computation".

RESEARCH AREAS

Cryptography | Verifiable Computation | Privacy | Zero-Knowledge Proofs

- Research on building and attacking practical verifiable delay functions (VDFs). Will be the first VDF to be deployed on the Ethereum Beaconchain.

Research Assistant

New York University Abu Dhabi

June 2020 - July 2020 Remote

- Research on provable data deletion to enable a better, more private internet with Prof. Christina Poepper's group.

Cryptography Engineering Intern

Celo

May 2019 - Aug 2019 Berlin

- Worked on Celo's Ultralight Client Sync which enables users to download very small number of block headers to verify correctness of current validator set using Zero-Knowledge proofs.

Summer Research Intern

IIT MADRAS

June 2018 - July 2019 Chennai

- Cryptanalysis of Stream Ciphers Grain 128 and Trivium under Prof. Santanu Sarkar.

HOBBY PROJECTS

Quantum Crypto Reading Group

Johns Hopkins University

Fall 2020

Organized a Quantum Cryptography reading group. Starting with quantum computation basics and then covering seminal results in quantum crypto.

PROGRAMMING LANGUAGES

Go	●●●●●
circom	●●●●●
Python	●●●●●
C/C++	●●●●○
Rust	●●●○○

TOOLS USED

Python: sklearn, tsfresh

C/C++: NTL (number theory), Pairing-based crypto

Golang

TEACHING

Blockchains & Cryptocurrencies

Johns Hopkins University

Spring 2021, 2023

Head TA for the graduate and undergraduate computer science course on blockchains.