PRATYUSH RANJAN TIWARI

CS PhD student @ Johns Hopkins University

@ ptiwari4@jhu.edu ☎ +1-667-2940017 🌐 www.pratyush.site

PUBLICATIONS

Work in Progress/ Under submission

- with, D. Gupta, and D. Agrawal (2021). ***Security & Privacy of AADHAAR: World's largest Biometrics-based ID system**: Systematizes this massive citizen identification system for India. Contains the most impactful attack on Aadhaar till date by leveraging some cryptographic flaws. Currently embargoed, waiting for government approval.*
- with, G. Beck, et al. (2021). ***Time-deniable Signatures**: Formalizing and proposing a signature scheme such that signatures allow authentication up until some time in the future and not indefinitely.*
- with, M. Humbert (2021). ***Stronger Membership Inference Attacks on Aggregate Location and Genomic Data**: New techniques for membership inference attacks with adversarial prior reduced considerably compared to prior work.*

Conference Proceedings

- I.A.Seres, O. Shlomovits, and P.R.Tiwari (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*.

EXPERIENCE

Research Collaborator

Ethereum Research

May 2021 - August 2021 Remote

- Research on building and attacking practical verifiable delay functions (VDFs).

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.

RESEARCH PHILOSOPHY

"Solve challenging theoretical problems which scale to impactful applications"

EDUCATION

Ph.D. in CS

Johns Hopkins University

Sept 2020 – June 2025

Working under the wonderful supervision of Abhishek Jain and Matt Green on problems at the intersection of Cryptography, Privacy and Machine Learning.

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 · Quantum Computation · Privacy · ML · Trustworthy AI

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

Organizing a Quantum Cryptography reading group. Starting with quantum computation basics and then covering seminal results in quantum crypto. Giving the first 5 talks.

PROGRAMMING LANGUAGES

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

TOOLS USED

- Python: sklearn, tsfresh
- C/C++: NTL (number theory), Pairing-based crypto
- Golang