Jaya Sharma

jayasharma-pqc.github.io | jaysh@dtu.dk | jayya-sharma

Introduction

I'm a PhD student in Cybersecurity Engineering at the Technical University of Denmark (DTU), working under the supervision of Dr. Christian Majenz. My PhD research lies at the intersection of theoretical cryptography and quantum computing, with a focus on the security of cryptographic constructions in the quantum random oracle model. So far, I have worked on the security of non-interactive zero-knowledge proofs and on post-quantum threshold signatures based on the hardness of group-based assumptions. My other specific interests include lattice-based cryptography, quantum information and quantum error correction.

Education

Technical University of Denmark (DTU) 2024–27
PhD Student, Cybersecurity Engineering Section, DTU Compute
Supervisor: Dr. Christian Majenz

Indraprastha Institute of Information Technology Delhi (IIITD) 2022–24
PhD Junior Research Fellow in the Department of Computer Science and Engineering
Area: Lattice-Based Cryptography and Quantum Computing

Indian Institute of Technology Roorkee (IITR) 2020–22
Master of Science in Mathematics
Grade: 8.675/10; All India Rank 122 of 30,942 (top 0.4%) in Joint CSIR-UGC national PhD fellowship exam.

University of Delhi – Lady Shri Ram College for Women (LSR) 2017–20
Bachelor of Science (Honours) in Mathematics
Grade: 9.081/10; All India Rank 143 of 14,374 (top 1%) in IIT JAM (national MSc entrance exam).

Research Visits/Internships

Centrum Wiskunde & Informatica (CWI), Amsterdam 09/2026–01/2027
Host: Dr. Serge Fehr
– Working on security proofs for post-quantum non-interactive zero-knowledge protocols.

QWorld Association – QIntern *(remote internship)* 07–09/2025
– Worked in an international team of four on a library (currently under review by the Qrisp developers) for efficient block-encoding of dense matrices via QRAM, using the Qrisp framework.

Indian Institute of Science, Bangalore (IISc) 06–07/2023
Host: Dr. Chaya Ganesh
– Studied the compression theory of sigma protocols and lattice-based sigma protocols.

Indian Institute of Science Education and Research Bhopal *(remote internship)* 06–08/2021
Host: Dr. Sanjay Singh
– Studied an introduction to algebraic function fields and applications in coding theory

Publications

Security of the Fischlin Transform in Quantum Random Oracle Model 2026
QCrypt'26 (contributed talk), IACR ASIACRYPT'26- Outstanding Paper
Christian Majenz, Jaya Sharma

Elliptic Curves over Complex Numbers 2022
Master's Thesis, IITR; Supervisor: Dr. A. Swaminathan

Brent–Dekker Method: An Attempt to Decode 2020
Eclat – A Mathematics Journal, Vol. 11, LSR College; Mentor: Dr. Monika Singh

Presentations

Fiat–Shamir Transform in QROM – Crypto Reading Group, DTU 10/2024
Lattice-Based Sigma Protocols – Theory Reading Group, IIITD 10/2023

Trapdoors for Hard Lattices and New Cryptographic Constructions – Theory Reading Group, IIITD 05/2023
A Survey on Quantum Error-Correcting Codes – Introduction to Quantum Computing, IIITD 05/2023

Academic Activities

Short Term Visit- Dr. Russell Lai , Aalto University, Finland 11/2026
Sub-Reviewer, Eurocrypt'27 2026
PhD Committee Member, DTU Compute 2025
Teaching Assistant
– Applied Cryptography, Discrete Mathematics, Graph Theory (DTU) 2024–25
– Introduction to Cryptography (IIT Delhi) 2023
– Discrete Mathematics (IIITD) 2022

Honours, Awards & Grants

IACR Asiacrypt Outstanding Paper Award 2026

Thomas B. Thriges Fond Grant, William Demant Fonden Grant, Otto Mønsteds Fond Grant 2026
– Secured three Danish grants to fund a research stay at CWI Amsterdam.

ACM-India Anveshan Setu Fellowship 2023
– Awarded by the Association for Computing Machinery (ACM) India to work at IISc.

Joint CSIR-UGC Junior Research Fellowship 2022
– Awarded a PhD research fellowship in Mathematical Sciences through the national exam conducted jointly by the Council of Scientific and Industrial Research (CSIR) and the University Grants Commission (UGC), India.

Workshops/Summer Schools/Conferences

Asiacrypt– Hong Kong 12/2026
ACM CCS– Young Scholar's Development Program- The Hague, Netherlands 11/2026
QCrypt – Ottawa, Canada 08/2026
Eurocrypt – Rome, Italy 05/2026
DQC Scientific Quantum Conference 2026 – Aalborg University, Denmark 04/2026
Theory of Cryptography Conference (TCC) 2025 – Aarhus, Denmark 12/2025
Workshop on Mathematics of Post-Quantum Cryptography – University of Zurich 06/2025
Quantum Safe Internet (QSI) Workshop – Technical University of Denmark, Lyngby 05/2025
IACR Summer School on Post-Quantum Cryptography – University of Warsaw 07/2024
ACM India Grad Cohort – IISc Bangalore 07/2023
CSE Research Symposium – IIT Bombay 03/2023
Vigyan Vidushi Mathematics Summer School – TIFR Mumbai 07/2021
Vigyan Vidushi Computer Science Summer School – TIFR Mumbai 06/2021

Other

Programming: C++, Python, Qiskit
Languages: English, Hindi (mother tongue), Danish (elementary)