

CURRICULUM VITAE

PERSONAL INFORMATION

Subham Das
subham.das@cispa.de, su8h.das@gmail.com
<https://cryptosubh.github.io/>

BRIEF INTRODUCTION

I am a doctoral candidate at the CISPA Helmholtz Center for Information security, supervised by Dr. Doreen Riepel. My current research interests are in foundations of real-world cryptography, provable security of Post-Quantum cryptographic schemes, and understanding contemporary theoretical frameworks and proof-techniques. Prior to joining CISPA, I graduated from the Indian Institute of Science Education and Research, Mohali and have completed a 5 years BS-MS Degree (Integrated Bachelor's and Master's Degree) majoring in Mathematics.

AFFILIATION

CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

Doctoral Candidate

Sep 2022 - Present

EDUCATION

Indian Institute of Science Education and Research, Mohali, India

Integrated BS-MS Program

Dec 2020 - June 2025

AWARDS

Stipendium Hungaricum Scholarship 2024/25

July 2024

Scholarship towards exchange studies in Cybersecurity at the Eötvös Loránd University, Budapest

PUBLICATIONS

Leveled Isogeny Problems with Hints, with R. Invernizzi, J. Meers, P. Kutas

PKC 2026

ACADEMIC SERVICE

External Reviewer, IEEE S&P 2026

External Reviewer, CRYPTO 2026