Curriculum Vitae

Personal Information

Subham Das
[redacted]
subhamdas965@gmail.com (PGP key here)
ms20121@iisermohali.ac.in
https://cryptosubh.github.io/

Brief Introduction

Currently I am a student at Indian Institute of Science Education and Research, Mohali and pursuing a BS-MS (Integrated Bachelor's and Master's Degree) in Mathematics. I am pursuing my Master's Thesis in Isogeny-based cryptography in the academic year 2024-2025. Prior to this, my academic interest has been predominantly in Algebraic geometry, especially in the geometry of vector bundles with a focus on moduli problems.

Education

Indian Institute of Science Education and Research, Mohali, India

Integrated BS-MS Program - [redacted]

Awards

[redacted]

Projects

Master's thesis *Jan 2024 - Present*

Investigations and cryptanalysis of isogeny-based cryptographic schemes
Supervisor : [redacted]
Aim : The broad theme of the MS-thesis shall be towards detailed analysis and investigations of the existing cryptographic schemes in this field which shall present a better understanding not only of the specific security assumptions of these schemes and their robustness, but also give insight to the underlying theory on which these schemes are built upon.

Vector Bundles over Algebraic Curves [redacted]
Supervisor : [redacted]
Participated in the course titled above remotely with exitensive discussions on Families of vector bundles, Cartier Divisiors, Degree of a Vector Bundle, Stability, Harder Narasimhan Filtrations. More details can be found on the course page [redacted]

Reading Project on Complex Algebraic Geometry [redacted]
Supervisor [redacted]
The topics covered here are the first three chapters of Claire Voisin's "*Complex Algebraic Geometry and Hodge Theory*". Emphasis was on examples and the theory of holomorphic vector bundles, Differential forms and complex analysis of several variables

Riemann Surfaces and related topics [redacted]
[redacted]
This project involved discussions on several related topics on Riemann surfaces, Morse theory and Abelian varieties. Details can be found [redacted]

Skills

Programming languages: Python (basic)

Office softwares: Microsoft Office, Open Office, LaTeX

Languages: English (C1, TOEFL '24 Score: [redacted]), Bengali (native), Hindi.

Courses taken

2021 : MTH101 Groups and Symmetry, MTH102 Analysis in One Variable, MTH201 Curves and Surfaces

2022 Spring Semester: IDC207 Number Theory and Cryptography, MTH202 Probability Theory

2022 Monsoon Semester: MTH301 Analysis in R^n, MTH302 Linear Algebra, MTH304 Group Theory, MTH303 Set Theory and Logic

2023 Spring Semester: MTH305 Complex Analysis, MTH306 Lebesgue Measure and Integration, MTH307 Topology, MTH308 Ring theory and Modules, MTH419 Number Theory

2023 Monsoon Semester: MTH401 Ordinary Differential Equations, MTH402 Functional Analysis, MTH403 Fields and Galois Theory, MTH424 Lie Algebra and Representation theory, MTH404 Commutative Algebra

2024 Spring Semester: MTH408 Algebraic Topology, MTH426 Algebraic curves

Extracurricular Activities

Playing bass guitar, harmonica, painting and occasionally writing haikus.