

# **The Start of a Great Project**



---

## CONTENTS

---

### INTRODUCTION TO THE BOOK

iii

### 0 Mathematical Foundations

### 1 Basics of Isogeny-based Cryptography

### 2 Advanced Topics in Isogeny-based Cryptography

### 3 Cryptographic Constructions



---

## INTRODUCTION TO THE BOOK

---

A book on isogeny-based cryptography.



Part o

MATHEMATICAL FOUNDATIONS





---

## MATHEMATICAL FOUNDATIONS

---

This part describes the mathematical foundations required to understand the other parts. This contains an overview of the necessary number theory, algebra, or other subjects.



## Part 1

# BASICS OF ISOGENY-BASED CRYPTOGRAPHY



This part describes basic topics in isogeny-based cryptography, such as elliptic curves, isogenies, pairings, and the class group action.



## Part 2

# ADVANCED TOPICS IN ISOGENY-BASED CRYPTOGRAPHY





This part describes advanced topics in isogeny-based cryptography, such as the Deuring correspondence, higher-dimensional isogenies, and generalized class group actions.



## Part 3

# CRYPTOGRAPHIC CONSTRUCTIONS



This part describes the cryptographic constructions, such as SQIsign or CSIDH, that are built on top of [Parts 1](#) and [2](#).

