The Start of a Great Project

CONTENTS

INTRODUCTION TO THE BOOK

A book on isogeny-based cryptography.

Part 0

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

BASICS OF ISOGENY-BASED CRYPTOGRAPY

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

ADVANCED TOPICS IN ISOGENY-BASED CRYPTOGRAPY

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

CRYPTOGRAPHIC CONSTRUCTIONS

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