An Implementation of SIDH Using Maple

By

Akifa Batool
BSMS1-21-06

Supervised By:
Dr. Athar Kharal

A Report Submitted to
Center for Advanced Studies in Pure and Applied Mathematics
Bahauddin Zakariya University, Multan

Abstract

With the advancement of quantum computing, the need for secure cryptographic protocols that can withstand quantum-based attacks has increased considerably. This paper describes detailed implementation of Supersingular Isogeny Diffie-Hellman (SIDH) protocol using Maple. SIDH is a key exchange mechanism that works by computing isogenies between elliptic curves.

Contents

Listings

Chapter 1

Introduction

The Supersingular Isogeny Diffie-Hellman (SIDH) algorithm is an innovative cryptographic approach in the post-quantum cryptography landscape, designed to be secure against quantum attacks. This document provides an intuitive overview and explanation of the implementation of SIDH using Maple. Chapter 1 provides the general overview about the working mechanism of SIDH. Chapter 2 walkthrough the mathematical foundations and Maple code for the SIDH Protocol. Chapter 3 provides a working example of SIDH using the demonstrated Maple code.

1.1 Background: Supersingular Elliptic Curves and Isogenies

SIDH relies on properties of *supersingular elliptic curves* and *isogenies* between them. In cryptography, elliptic curves are mathematical structures that enable secure encryption methods. Supersingular curves, in particular, have unique characteristics, such as a finite number of specific maps (isogenies) connecting one curve to another. Unlike ordinary elliptic curves, these supersingular curves possess structures that quantum algorithms struggle to break efficiently.
These isogenies serve as the cryptographic "trapdoor" in SIDH, allowing for the creation of secure key exchanges. The hardness of computing isogenies between supersingular elliptic curves forms the core of the security assumption in SIDH. What makes them especially useful in post-quantum cryptography is their resistance to Shor's algorithm, which can break many traditional cryptographic schemes. Moreover, the underlying mathematical structures are rich and well-studied, offering both theoretical depth and practical applicability. As a result, supersingular elliptic curves

and their isogenies have become foundational tools in designing quantum-resistant cryptographic protocols.
See figure 1.1 for further elaboration:

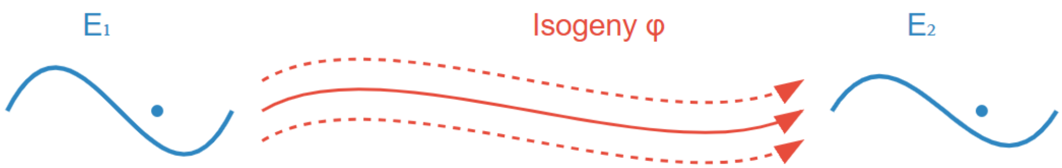

Figure 1.1: The concept of an Isogeny

1.2 Isogenies as a "Hard Problem"

An *isogeny* is a special type of function that maps points from one elliptic curve to another while preserving the group structure. The crucial idea here is that given two supersingular elliptic curves, finding a direct isogeny (if it exists) is computationally challenging. This hardness forms the basis for SIDH's security, much like how factoring large numbers is difficult in traditional RSA cryptography.

1.3 Key Exchange via Isogenies

SIDH builds on the classic Diffie-Hellman key exchange but replaces exponentiation (in groups) with isogenies. Here's an outline of the process:

- **Key Generation**: Alice and Bob each select random secret isogenies based on private points on an initial elliptic curve. Using these secret isogenies, they transform the starting curve into new, derived elliptic curves.
- **Public Key Sharing**: Each party computes a public value (new curve and some additional information) and sends this to the other. This public value encodes the "directions" taken via the isogenies but not the exact path, making it hard to reverse-engineer.
- **Shared Secret Creation**: When Alice receives Bob's public key (his curve and auxiliary points), she uses her private isogeny to apply transformations to

Bob's curve. Bob does the same with Alice's public key. Both end up at the same elliptic curve due to the structure of their isogenies, establishing a shared secret without directly revealing their private transformations.

See figure 1.2 for further elaboration:

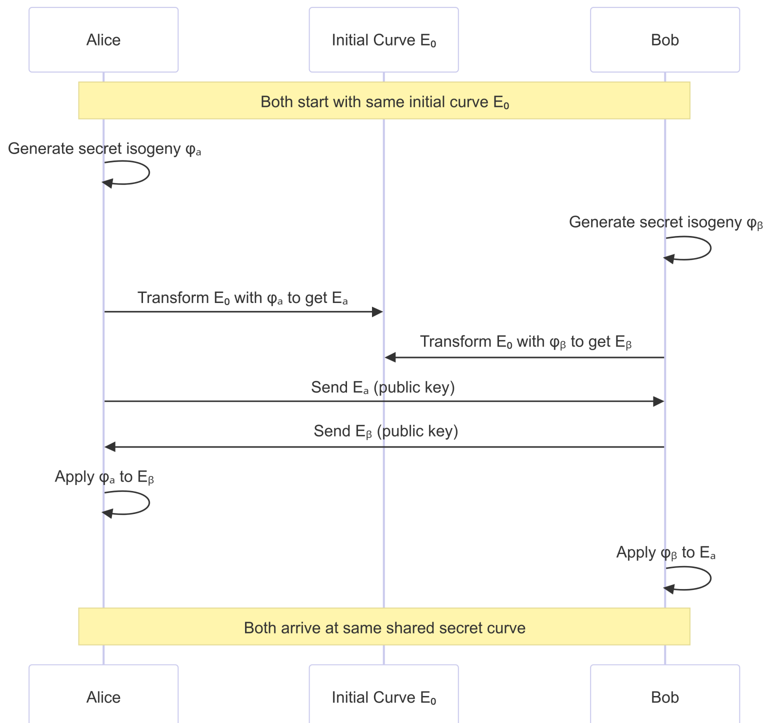

Figure 1.2: Key Exchange Process

1.4 Why Quantum-Resistant?

SIDH is resistant to Shor's algorithm, the powerful quantum algorithm that can break many conventional cryptographic schemes. The complex structure of supersingular isogenies makes it difficult even for a quantum computer to trace back the isogeny mappings, thereby preserving the security of the key exchange. This resistance arises from the unique nature of the isogeny problem, which lacks a known efficient solution on both classical and quantum computers. While traditional systems rely on number-theoretic problems now vulnerable to quantum attacks, SIDH's reliance on isogeny paths in supersingular elliptic curve graphs introduces a level of complexity that current quantum techniques cannot exploit. Unlike more predictable algebraic structures, the landscape of supersingular isogenies is intricate and lacks the algebraic shortcuts that quantum algorithms typically exploit. This complexity is what gives SIDH its quantum-resistant edge, positioning it as a forward-looking solution in cryptographic design.

1.5 Challenges and Limitations

While SIDH offers promise as a quantum-secure algorithm, it is computationally demanding and requires careful parameter selection. It has also faced challenges in security scrutiny, as further research exposed potential vulnerabilities in some configurations.

SIDH creatively leverages the hard-to-reverse property of isogenies between supersingular elliptic curves to achieve secure key exchange that withstands quantum decryption attempts. This makes it a valuable candidate in post-quantum cryptography.