# An Implementation of SIDH Using Maple

Student
**Akifa Batool**
Supervisor
**Dr. Athar Kharal**

Center for Advanced Studies in Pure and Applied Mathematics
Bahhaudin Zakariya University, Multan

May 19, 2025

# Overview

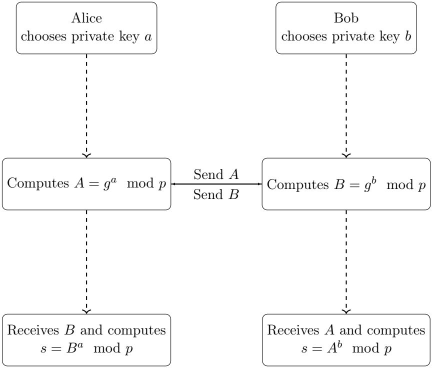
# Why Post-Quantum Cryptography Matters?

- Threat to classical cryptographic systems.
- To ensure digital security in presence of qunatum computers

# Introduction

- SIDH is a post-quantum key exchange protocol based on isogenies between supersingular elliptic curves.
- It replaces traditional exponentiation (as in classic Diffie–Hellman) with hard-to-compute isogeny maps.
- The security of SIDH relies on the difficulty of finding isogenies between supersingular curves.

# Diffie-Hellman Workflow




**Result:** Both compute the same shared secret $s = g^{ab} \mod p$ without ever sending $a$ or $b$

Figure 1: Diffie–Hellman Key Exchange Workflow

# SIDH Workflow

- Both parties agree on a starting elliptic curve $E_0$ with public parameters.
- Alice and Bob each choose private keys and compute isogenies $\phi_A$ and $\phi_B$ using their respective torsion bases.
- They exchange public keys that include the new elliptic curves $E_A$ and $E_B$ along with transformed points.
- Each applies their private isogeny to the received curve to compute a common curve $E_{AB}$, from which a shared secret (the $j$-invariant) is derived.

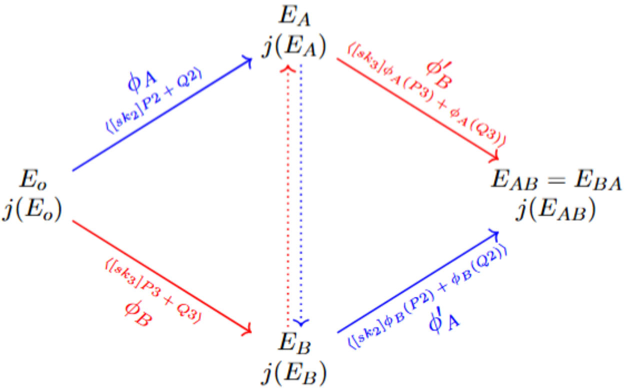



Figure 2: SIDH key exchange diagram

# Mathematical Bacground

- **Montgomery Curve:** A special form of elliptic curve used in SIDH, defined as $By^2 = x^3 + Ax^2 + x$, chosen for efficient arithmetic operations.
- **Supersingular Curve:** A type of elliptic curve with no $p$-torsion over $\mathbb{F}_p$; offers strong security due to the difficulty of computing isogenies between such curves.
- **Isogeny:** A structure-preserving map between elliptic curves that maintains group operations. It is hard to invert, which underpins SIDH's security.
- **$j$-invariant:** A value that uniquely classifies elliptic curves up to isomorphism. In SIDH, both parties compute the same $j$-invariant as the shared secret.

The following figure illustrates the results based on Maple implementation of SIDH Protocol.

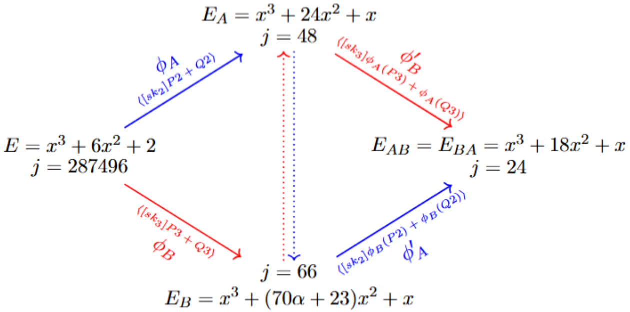



Figure 3: SIDH key exchange diagram

This implementation is based on the SIDH proposal submitted to **NIST's Post-Quantum Cryptography Standardization Project (Round 3)**.

# References I


- David Jao, et al. *Supersingular Isogeny Key Encapsulation.* Submission to the NIST Post-Quantum Cryptography Standardization Project, 4th Round, 2022.
- David Jao, & Luca De Feo. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-Quantum Cryptography, Springer, 2011.
- Joseph H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition.* Graduate Texts in Mathematics, Springer, 2009.
- Morris J. Dworkin. *SHA-3 standard: Permutation-based hash and extendable-output functions.* Federal Inf. Process. Stds. (NIST FIPS) – 202, 2015.
- G. Bertoni, et al. *The KECCAK reference, Version 3.0.* 2011.