Palestine Journal of Mathematics

Vol 14(3)(2025) , 668–683 © Palestine Polytechnic University-PPU 2025

Enhancing PAKE Protocols with Isogenies for Post-Quantum Security

Mohammed El Baraka and Siham Ezzouak

Communicated by Manoj Patel

MSC 2010 Classifications: 94A60, 11G07, 11T71, 81P94.

Keywords and phrases: Post-Quantum Cryptography, PAKE, Isogeny-Based Cryptography, Supersingular Isogeny Problem, Zero-Knowledge Proofs.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Corresponding Author: Mohammed El Baraka

Abstract *The advent of quantum computing poses a significant threat to classical cryptographic protocols, particularly those relying on the hardness of problems like the discrete logarithm and integer factorization. Password-Authenticated Key Exchange (PAKE) protocols, essential for secure communications using low-entropy passwords, are vulnerable to quantum attacks. In this paper, we propose a novel PAKE protocol based on isogenies of supersingular elliptic curves, leveraging the hardness of the Supersingular Isogeny Problem (SIP) to achieve post-quantum security. We provide a detailed mathematical formulation of the protocol, rigorous security proofs within a formal security model, and an in-depth performance evaluation. Our protocol offers quantum-resistant security while maintaining practical performance levels, with computational and communication costs comparable to existing post-quantum PAKE protocols. Experimental results demonstrate that our protocol is feasible for real-world applications, providing a viable solution for secure password-based authentication in the quantum era.*

1 Introduction

The rapid advancement of quantum computing technology presents an imminent challenge to the security of classical cryptographic systems. Quantum algorithms, such as Shor's algorithm [1], can efficiently solve the integer factorization and discrete logarithm problems, undermining the security assumptions of widely used cryptographic protocols. Password-Authenticated Key Exchange (PAKE) protocols, which enable secure communication between parties based on shared low-entropy passwords, are particularly vulnerable, as they often rely on the computational hardness of these problems.

Traditional PAKE protocols, including SPAKE2 [2], J-PAKE [3], and OPAQUE [4], are constructed upon cryptographic primitives that are susceptible to quantum attacks. The necessity for post-quantum secure PAKE protocols is critical to ensure the confidentiality and integrity of communications in the impending quantum era.

Various post-quantum cryptographic approaches have been explored to address these challenges, such as lattice-based cryptography [5], code-based cryptography [6], and multivariate polynomial cryptography [7]. While these methods offer quantum resistance, they often entail significant performance trade-offs, including increased computational complexity and larger key sizes.

Isogeny-based cryptography has emerged as a promising candidate for post-quantum cryptographic schemes. It leverages the hardness of finding isogenies between supersingular elliptic curves, a problem believed to be resistant to both classical and quantum attacks [8]. Protocols such as the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange [8] and its variant

SIKE have demonstrated the potential of isogeny-based cryptography to provide security with relatively small key sizes and reasonable computational overhead.

Despite these advancements, the integration of isogeny-based cryptography into PAKE protocols remains underexplored. Existing post-quantum PAKE protocols often rely on other cryptographic assumptions and may not offer the desired balance between security and performance.

1.1 Related Work

Several efforts have been made to develop post-quantum PAKE protocols. Zhang et al. [9] proposed a lattice-based PAKE protocol, which offers quantum resistance but suffers from large key sizes and significant computational overhead. Similarly, other works have investigated code-based and hash-based approaches, each with their own limitations.

Isogeny-based cryptography has been successfully applied in key exchange protocols [10], but its application to PAKE protocols is limited. Sun and Tian [11] introduced an isogeny-based PAKE protocol; however, their scheme lacks comprehensive security analysis and practical performance evaluation.

1.2 Motivation and Contributions

The need for efficient and secure PAKE protocols that withstand quantum attacks is pressing, given the potential vulnerabilities in existing systems. Our work aims to fill this gap by proposing a novel isogeny-based PAKE protocol that leverages the hardness of the Supersingular Isogeny Problem to achieve post-quantum security.

Our main contributions are:

- ***Design of an Isogeny-Based PAKE Protocol**: We present a detailed construction of a PAKE protocol utilizing isogenies between supersingular elliptic curves. The protocol replaces the traditional discrete logarithm problem with the SIP, enhancing resistance to quantum attacks.*
- ***Rigorous Security Analysis**: We provide formal security proofs within the Real-Or-Random (ROR) security model [12], demonstrating the protocol's security against passive and active adversaries, including those with quantum capabilities.*
- ***Performance Evaluation**: We conduct a comprehensive performance analysis, including computational complexity, communication costs, and experimental implementation results. Our protocol achieves practical performance levels, with execution times acceptable for real-world applications and communication costs comparable to existing post-quantum protocols.*
- ***Comparison with Existing Protocols**: We compare our protocol with traditional and post-quantum PAKE protocols, highlighting the advantages in terms of security and efficiency.*

1.3 Organization of the Paper

The remainder of this paper is organized as follows. In Section II, we provide the necessary mathematical preliminaries on elliptic curves, isogenies, and the Supersingular Isogeny Problem. Section III introduces our proposed isogeny-based PAKE protocol, including detailed steps and algorithmic representations. In Section IV, we present rigorous security proofs within a formal security model. Section V offers a thorough performance evaluation, including experimental results and comparisons with existing protocols. Finally, Section VI concludes the paper and discusses potential directions for future research.

2 Mathematical Preliminaries

In this section, we provide a comprehensive mathematical foundation necessary to understand the proposed isogeny-based PAKE protocol. We delve into elliptic curves, isogenies, supersingular elliptic curves, and the hard mathematical problems that underpin the cryptographic security

of our protocol. Detailed definitions, theorems, propositions, and proofs are presented to ensure mathematical rigor.

2.1 Elliptic Curves

An elliptic curve E over a finite field $\mathbb{F}_q$, where $q = p^n$ for a prime p, is defined by the simplified Weierstrass equation [13],[31],[27]:

$$E : y^2 = x^3 + ax + b, \tag{2.1}$$

where $a, b \in \mathbb{F}_q$, and the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$ ensures that the curve is non-singular.

Group Structure of Elliptic Curves

The set of points $E(\mathbb{F}_q)$ forms a finite abelian group under the operation of point addition, with the point at infinity $\mathcal{O}$ serving as the identity element. The group law is defined geometrically:

*- **Point Addition** ($P + Q$): For two distinct points $P, Q \in E(\mathbb{F}_q)$, the line L passing through P and Q intersects the curve at a third point R. Then, $P + Q$ is defined as the reflection of R over the x-axis.*

*- **Point Doubling** ($[2]P$): For a point P, the tangent line at P intersects the curve at another point R. Then, $[2]P$ is the reflection of R over the x-axis.*

These operations satisfy the group axioms, making $(E(\mathbb{F}_q), +)$ a well-defined abelian group [14].

Properties

*- **Order of the Curve**: The number of points $\#E(\mathbb{F}_q)$ is given by Hasse's theorem:*

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}. \tag{2.2}$$

*- **Torsion Points**: Points P such that $[n]P = \mathcal{O}$ form the torsion subgroup $E[n]$.*

2.2 Isogenies

An isogeny is a non-constant rational morphism between elliptic curves that preserves the group structure.

Definition 2.1. An **isogeny** $\varphi : E_1 \to E_2$ between two elliptic curves E_1 and E_2 over a field $\mathbb{F}_q$ is a surjective morphism of algebraic curves defined over $\mathbb{F}_q$ that satisfies:

(i) $\varphi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$.

(ii) For all $P, Q \in E_1(\mathbb{F}_q)$,

$$\varphi(P + Q) = \varphi(P) + \varphi(Q). \tag{2.3}$$

Degree of an Isogeny

*The **degree** of an isogeny φ, denoted $\deg \varphi$, is the degree of the field extension induced by φ on function fields. For separable isogenies, the degree corresponds to the size of the kernel $\ker \varphi$ [15],[19].*

Dual Isogeny

*For every isogeny $\varphi : E_1 \to E_2$, there exists a **dual isogeny** $\hat{\varphi} : E_2 \to E_1$ such that:*

$$\hat{\varphi} \circ \varphi = [\deg \varphi], \tag{2.4}$$

where $[\deg \varphi]$ denotes the multiplication-by-$\deg \varphi$ map on E_1.

Theorem 2.2. *Let $\varphi : E_1 \to E_2$ be an isogeny of degree m, and $\hat{\varphi} : E_2 \to E_1$ its dual isogeny. Then:*

$$\hat{\varphi} \circ \varphi = [m]_{E_1}, \tag{2.5}$$

$$\varphi \circ \hat{\varphi} = [m]_{E_2}. \tag{2.6}$$

Proof. The proof follows from the properties of isogenies and dual isogenies, utilizing the fact that the composition of an isogeny with its dual equals multiplication by the degree. See [13] for a detailed proof. □

Kernel of an Isogeny

The kernel $\ker \varphi$ *of an isogeny $\varphi : E_1 \to E_2$ is a finite subgroup of E_1. Conversely, for any finite subgroup $G \subset E_1$, there exists an isogeny $\varphi : E_1 \to E_2$ with kernel G [16].*

2.3 Supersingular Elliptic Curves

An elliptic curve E over $\mathbb{F}_{p^n}$ is called ***supersingular*** *if the number of $\mathbb{F}_{p^n}$-rational points satisfies specific properties, and its endomorphism ring $\mathrm{End}(E)$ is larger than usual.*

Properties of Supersingular Curves

*- **Endomorphism Ring**: For supersingular curves over $\overline{\mathbb{F}}_p$, $\mathrm{End}(E)$ is isomorphic to a maximal order in a quaternion algebra over $\mathbb{Q}$ [17].*

*- **Number of Curves**: There are approximately $p/12$ supersingular j-invariants over $\mathbb{F}_p$.*

*- **Frobenius Map**: The p-power Frobenius endomorphism acts differently on supersingular curves, leading to unique properties utilized in cryptography.*

Isogeny Graphs of Supersingular Curves

Supersingular curves can be connected via isogenies to form an isogeny graph, which is a regular, connected graph used in cryptographic constructions [18].

2.4 Hard Mathematical Problems

The security of isogeny-based cryptography relies on the computational hardness of certain problems.

Supersingular Isogeny Problem (SIP)

Problem 1. Given two supersingular elliptic curves E_1 and E_2 over $\mathbb{F}_{p^2}$, find an isogeny $\varphi : E_1 \to E_2$.

This problem is believed to be hard even for quantum computers, as there is no known efficient algorithm to solve it [20].

Computational Supersingular Isogeny Diffie-Hellman Problem (CSSI-DH)

Problem 2. Given (E, E_A, E_B) where E_A and E_B are the images of E under secret isogenies of degrees $\ell_A^{e_A}$ and $\ell_B^{e_B}$, compute the j-invariant of E_{AB}, the image of E under the composition of both isogenies.

The difficulty of this problem underpins the security of protocols like SIDH [8].

2.5 Vélu's Formulas

Vélu's formulas provide an explicit method to compute isogenies when the kernel is known.

Theorem 2.3 (Vélu's Formulas [21]). *Let E be an elliptic curve over $\mathbb{F}_q$, and let G be a finite subgroup of $E(\overline{\mathbb{F}}_q)$. Then the isogeny $\varphi : E \to E' = E/G$ can be explicitly computed using:*

$$\varphi(x,y) = \left(x + \sum_{P \in G \setminus \{\mathcal{O}\}} \frac{x_P - x}{(x - x_P)^2},\ y + \sum_{P \in G \setminus \{\mathcal{O}\}} \frac{y_P - y}{(x - x_P)^3} \right), \tag{2.7}$$

$$E' : y^2 = x^3 + a'x + b', \tag{2.8}$$

where a' and b' are computed based on G and the coefficients of E.

Proof. The proof involves constructing the isogeny by modifying the functions defining E to account for the points in G. Detailed derivations can be found in [21]. □

2.6 Torsion Points

Definition 2.4. A point $P \in E(\overline{\mathbb{F}}_q)$ is a **torsion point** of order n if $[n]P = \mathcal{O}$, where $[n]$ denotes scalar multiplication by n.

The set of all torsion points of order dividing n forms the n-torsion subgroup $E[n]$.

Structure of Torsion Subgroups

Over an algebraically closed field, the torsion subgroup $E[n]$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ when $\gcd(n,p) = 1$ *[13, 33, 32].*

2.7 Zero-Knowledge Proofs

Zero-knowledge proofs allow one party to prove knowledge of a secret without revealing it.

Definition 2.5. A **zero-knowledge proof** is an interactive protocol between a prover and a verifier where:

(i) **Completeness**: If the statement is true, an honest verifier will be convinced by an honest prover.

(ii) **Soundness**: If the statement is false, no cheating prover can convince the honest verifier that it is true, except with negligible probability.

(iii) **Zero-Knowledge**: If the statement is true, no verifier learns anything other than the fact that the statement is true.

Schnorr's Protocol Adapted to Isogenies

An adaptation of Schnorr's identification protocol can be used in the context of isogenies:
*- **Prover**: Knows a secret isogeny $\varphi : E \to E'$.*
*- **Verifier**: Knows E, E', and wants to be convinced that the prover knows φ.*
The protocol involves the prover sending a commitment, receiving a challenge, and responding in a way that convinces the verifier without revealing φ [22].

2.8 Isogeny Graphs

Isogeny graphs model the relationships between elliptic curves connected via isogenies.

Definition 2.6. An **isogeny graph** is a graph where:
- **Vertices**: Represent isomorphism classes of elliptic curves over $\mathbb{F}_{p^2}$.
- **Edges**: Represent isogenies of a fixed degree ℓ between curves.

Properties

*- **Regularity**: The graph is $\ell + 1$ regular.*
*- **Connectivity**: The graph is connected due to the properties of supersingular curves.*
*- **Expander Graphs**: These graphs exhibit rapid mixing properties, which are useful in cryptographic constructions [23].*

2.9 Notation Summary

For clarity, we summarize the notation used throughout this section:

- $\mathbb{F}_q$*: Finite field of order* q*.*
- E*,* E_1*,* E_2*: Elliptic curves over* $\mathbb{F}_q$*.*
- φ*,* ψ*: Isogenies between elliptic curves.*
- $\deg \varphi$*: Degree of the isogeny* φ*.*
- $\mathcal{O}$*: Point at infinity on an elliptic curve.*
- $[n]P$*: Scalar multiplication of point* P *by* n*.*
- G*: Finite subgroup of* E*.*
- $\hat{\varphi}$*: Dual isogeny of* φ*.*
- P*,* Q*: Points on an elliptic curve.*
- $E[n]$*:* n*-torsion subgroup of* E*.*

3 Proposed Isogeny-Based PAKE Protocol

In this section, we present our proposed Password-Authenticated Key Exchange (PAKE) protocol based on isogenies between supersingular elliptic curves. We provide a detailed mathematical description of the protocol, rigorous proofs of its security properties, and a thorough comparison with existing protocols. The protocol leverages the hardness of the Supersingular Isogeny Problem to achieve post-quantum security.

3.1 Design of the Protocol

The proposed protocol aims to replace the discrete logarithm problem in traditional PAKE protocols with the Supersingular Isogeny Problem (SIP), enhancing security against quantum adversaries. The protocol is designed within a formal security model to ensure rigorous analysis.

Protocol Setup

Let p *be a large prime such that* $p \equiv 3 \mod 4$*, ensuring that* $\mathbb{F}_{p^2}$ *is a field suitable for defining supersingular elliptic curves. The public parameters are:*

- *A supersingular elliptic curve* E_0 *over* $\mathbb{F}_{p^2}$ *with* j*-invariant* 1728*.*
- *Two small coprime primes* ℓ_A *and* ℓ_B *(e.g.,* $\ell_A = 2$*,* $\ell_B = 3$*).*
- *Integers* e_A *and* e_B *such that* $\ell_A^{e_A} \approx \ell_B^{e_B} \approx p^{1/2}$*.*
- *Bases* $\{\mathcal{P}_A, \mathcal{Q}_A\}$ *of* $E_0[\ell_A^{e_A}]$ *and* $\{\mathcal{P}_B, \mathcal{Q}_B\}$ *of* $E_0[\ell_B^{e_B}]$*.*
- *A secure hash function* $H : \{0,1\}^* \to \{0,1\}^\kappa$*, where* κ *is the security parameter.*
- *A Key Derivation Function (KDF) for deriving secret integers from the password.*

Protocol Description

Assume Alice and Bob share a password pw*. The protocol proceeds as follows:*

Step 1: Secret Key Generation ***Alice's Computations:***

(i) Derive a secret integer m_A from pw:

$$m_A = \mathit{KDF}_A(pw) \mod \ell_A^{e_A}. \tag{3.1}$$

(ii) Compute the secret isogeny $\phi_A : E_0 \to E_A$ with kernel $K_A = \langle [m_A]\mathcal{P}_A + \mathcal{Q}_A \rangle$.

(iii) Compute the image points:

$$\phi_A(\mathcal{P}_B), \quad \phi_A(\mathcal{Q}_B). \tag{3.2}$$

Bob's Computations:

(i) Derive a secret integer m_B from pw:

$$m_B = \mathit{KDF}_B(pw) \mod \ell_B^{e_B}. \tag{3.3}$$

(ii) Compute the secret isogeny $\phi_B : E_0 \to E_B$ with kernel $K_B = \langle [m_B]\mathcal{P}_B + \mathcal{Q}_B \rangle$.

(iii) Compute the image points:

$$\phi_B(\mathcal{P}_A), \quad \phi_B(\mathcal{Q}_A). \tag{3.4}$$

Step 2: Public Key Exchange ***Alice Sends to Bob:*** *The curve E_A and the points $\phi_A(\mathcal{P}_B)$, $\phi_A(\mathcal{Q}_B)$.*
Bob Sends to Alice: *The curve E_B and the points $\phi_B(\mathcal{P}_A)$, $\phi_B(\mathcal{Q}_A)$.*

Step 3: Shared Secret Computation ***Alice's Computations:***

(i) Compute the shared isogeny $\psi_A : E_B \to E_{AB}$ with kernel:

$$K_{AB} = \langle [m_A]\phi_B(\mathcal{P}_A) + \phi_B(\mathcal{Q}_A) \rangle. \tag{3.5}$$

(ii) Compute the shared secret:

$$K = H(j(E_{AB})). \tag{3.6}$$

Bob's Computations:

(i) Compute the shared isogeny $\psi_B : E_A \to E_{BA}$ with kernel:

$$K_{BA} = \langle [m_B]\phi_A(\mathcal{P}_B) + \phi_A(\mathcal{Q}_B) \rangle. \tag{3.7}$$

(ii) Compute the shared secret:

$$K = H(j(E_{BA})). \tag{3.8}$$

Step 4: Zero-Knowledge Proofs *To prevent active attacks, Alice and Bob perform zero-knowledge proofs to verify the correctness of the exchanged data without revealing their secrets.*

Algorithm Representation

Algorithm 1 Isogeny-Based PAKE Protocol (I-PAKE)

Require: Shared password pw
Ensure: Shared secret key K
Public Parameters: As specified in the protocol setup.
procedure ALICE'S ACTIONS
    Compute $m_A = \text{KDF}_A(pw) \mod \ell_A^{e_A}$
    Compute ϕ_A with kernel K_A
    Compute $\phi_A(\mathcal{P}_B)$, $\phi_A(\mathcal{Q}_B)$
    Send E_A, $\phi_A(\mathcal{P}_B)$, $\phi_A(\mathcal{Q}_B)$ to Bob
    Perform zero-knowledge proof of knowledge of ϕ_A
end procedure
procedure BOB'S ACTIONS
    Compute $m_B = \text{KDF}_B(pw) \mod \ell_B^{e_B}$
    Compute ϕ_B with kernel K_B
    Compute $\phi_B(\mathcal{P}_A)$, $\phi_B(\mathcal{Q}_A)$
    Send E_B, $\phi_B(\mathcal{P}_A)$, $\phi_B(\mathcal{Q}_A)$ to Alice
    Perform zero-knowledge proof of knowledge of ϕ_B
end procedure
procedure SHARED KEY COMPUTATION
    Alice computes ψ_A and $K = H(j(E_{AB}))$
    Bob computes ψ_B and $K = H(j(E_{BA}))$
end procedure

3.2 Mathematical Proofs of Correctness

Equality of Shared Secrets

Theorem 3.1. *The shared secret keys computed by Alice and Bob are equal, i.e.,* $K = H(j(E_{AB})) = H(j(E_{BA}))$.

Proof. We need to show that E_{AB} and E_{BA} are isomorphic. Consider the composition of isogenies:

$$\psi_A \circ \phi_B : E_0 \to E_{AB}, \quad \psi_B \circ \phi_A : E_0 \to E_{BA}.$$

Since the kernels of $\psi_A \circ \phi_B$ and $\psi_B \circ \phi_A$ are both equal to:

$$K = \langle [m_A m_B]\mathcal{P}_0 + [m_A]\mathcal{Q}_B + [m_B]\mathcal{Q}_A \rangle, \tag{3.9}$$

the two isogenies are equivalent up to isomorphism. Therefore, $E_{AB} \cong E_{BA}$, and the j-invariants are equal:

$$j(E_{AB}) = j(E_{BA}). \tag{3.10}$$

Applying the hash function H, both parties derive the same shared secret K. □

3.3 Formal Security Model

We analyze the security of the protocol within the Real-Or-Random (ROR) security model for PAKE protocols [12].

Adversarial Model

The adversary $\mathcal{A}$ has the following capabilities:

- ***Eavesdropping**: Can observe all communications between Alice and Bob.*
- ***Active Attacks**: Can modify, inject, or replay messages.*

- ***Password Guessing****: Limited to offline dictionary attacks due to password authentication.*
- ***Quantum Capabilities****: Can perform quantum computations, except for solving the SIP efficiently.*

Security Definition

A PAKE protocol is secure if, for any probabilistic polynomial-time adversary $\mathcal{A}$, the advantage in distinguishing the real shared key from a random key is negligible, i.e.,

$$Adv_{\mathcal{A}}^{PAKE} = |\Pr[\mathcal{A} \text{ outputs } 1|Real] - \Pr[\mathcal{A} \text{ outputs } 1|Random]| \leq \varepsilon, \tag{3.11}$$

where ε is a negligible function in the security parameter.

3.4 Security Proofs

Security Against Passive Adversaries

Theorem 3.2. *Under the assumption that the Supersingular Isogeny Problem is hard, a passive adversary cannot compute the shared secret K without knowledge of the password pw.*

Proof. A passive adversary observes the public data:

$$E_A,\ \phi_A(\mathcal{P}_B),\ \phi_A(\mathcal{Q}_B),\ E_B,\ \phi_B(\mathcal{P}_A),\ \phi_B(\mathcal{Q}_A). \tag{3.12}$$

To compute K, the adversary needs to derive $j(E_{AB})$. This requires computing the isogeny between E_A and E_B, which is equivalent to solving the SIP, known to be hard even for quantum adversaries [20]. Without the password pw, the adversary cannot compute m_A or m_B, and thus cannot reconstruct the secret isogenies.

Therefore, the adversary's advantage is negligible. □

Security Against Active Adversaries

Theorem 3.3. *The protocol is secure against active adversaries under the hardness assumption of the Supersingular Computational Diffie-Hellman Problem (SSCDH) and the security of the zero-knowledge proofs.*

Proof. An active adversary may attempt to impersonate a party or alter messages to cause the parties to accept different keys.

Impersonation Resistance:

To impersonate Alice, the adversary must produce valid $(E_A, \phi_A(\mathcal{P}_B), \phi_A(\mathcal{Q}_B))$ corresponding to some m_A derived from pw. Without pw, this requires solving the SSCDH problem.

Man-in-the-Middle Resistance:

The zero-knowledge proofs ensure that any modification of the exchanged data by the adversary will be detected. The proofs verify that the sender knows the secret isogeny corresponding to the transmitted data.

Therefore, the adversary cannot cause Alice and Bob to accept different keys or learn any information about K, and the protocol remains secure. □

Resistance to Quantum Attacks

Theorem 3.4. *Assuming that no efficient quantum algorithm exists to solve the Supersingular Isogeny Problem or the SSCDH problem, the protocol is secure against quantum adversaries.*

Proof. Quantum adversaries are limited by the computational hardness of the underlying problems. The best-known quantum algorithms for the SIP and SSCDH have sub-exponential complexity [20]. By choosing sufficiently large parameters (e.g., p with 768 bits), we ensure that the protocol resists quantum attacks.

Therefore, the security proofs against classical adversaries extend to quantum adversaries under the stated assumptions. □

3.5 Detailed Comparison with Existing Protocols

We compare our protocol with SPAKE2 [2], J-PAKE [3], and OPAQUE [4], focusing on mathematical aspects such as computational complexity, communication overhead, and security levels.

Computational Complexity

Our Protocol (I-PAKE): - ***Computational Operations***: *Isogeny computations of degree* $\ell_A^{e_A}$ *and* $\ell_B^{e_B}$. - ***Complexity***: *Let* $n = \log p$. *The isogeny computations have complexity* $\mathcal{O}(n^3)$ *due to the use of Vélu's formulas [24].*

SPAKE2 and J-PAKE: - ***Computational Operations***: *Exponentiations in groups of order* q. - ***Complexity***: $\mathcal{O}(n^2)$, *where* $n = \log q$.

OPAQUE: - ***Computational Operations***: *Use of asymmetric primitives and hash functions.* - ***Complexity***: *Depends on the underlying primitives, but generally* $\mathcal{O}(n^2)$.

Communication Overhead

Our Protocol: - ***Data Transmitted***: *Curves and points in* $\mathbb{F}_{p^2}$. - ***Size***: *Each transmitted element is approximately* $2n$ *bits. Total communication is* $6n$ *bits per party.*

SPAKE2 and J-PAKE: - ***Data Transmitted***: *Group elements in* $\mathbb{F}_q$. - ***Size***: *Each element is approximately* n *bits. Total communication is* $2n$ *bits per party.*

OPAQUE: - ***Data Transmitted***: *Depends on the implementation but generally includes group elements and hash outputs.*

Security Levels

Our Protocol: - ***Classical Security***: *Equivalent to the difficulty of the SIP.* - ***Quantum Security***: *Maintained due to the intractability of the SIP against quantum algorithms.*

SPAKE2 and J-PAKE: - ***Classical Security***: *Based on the hardness of the Discrete Logarithm Problem (DLP).* - ***Quantum Security***: *Broken due to Shor's algorithm [1].*

OPAQUE: - ***Classical and Quantum Security***: *Can be post-quantum secure if built over quantum-resistant primitives.*

Discussion

While our protocol has higher computational and communication overhead compared to classical PAKE protocols, it offers significant security advantages in the post-quantum context. The increase in computational complexity is acceptable given the enhanced security, and with optimization techniques, practical performance can be achieved.

3.6 Implementation Considerations

Parameter Selection

- ***Prime*** p: *Should be at least 768 bits to ensure 128-bit quantum security.* - ***Torsion Degrees***: *Chosen to balance security and efficiency. Common choices are* $\ell_A = 2$, $\ell_B = 3$.

Optimization Techniques

- ***Efficient Isogeny Computations***: *Utilize fast algorithms for isogeny evaluation, such as using optimal strategies for isogeny chains [24].* - ***Parallel Processing***: *Exploit parallelism in computing independent isogenies.*

Zero-Knowledge Proofs

Implement efficient zero-knowledge proofs tailored for isogeny-based protocols, ensuring they do not introduce significant overhead [10].

4 Performance Evaluation

In this section, we evaluate the performance of the proposed isogeny-based PAKE protocol (I-PAKE). We provide detailed mathematical analysis of computational complexity, communication costs, and compare our protocol with existing PAKE protocols, both classical and post-quantum. We also discuss implementation considerations and present experimental results to demonstrate the practicality of our protocol.

4.1 Computational Complexity Analysis

We analyze the computational complexity of the protocol by examining the dominant operations required for key generation, isogeny computations, and zero-knowledge proofs.

Isogeny Computations

The primary computational cost in I-PAKE arises from computing isogenies of large degree.

Complexity of Isogeny Computation *- **Vélu's Formulas**: The computation of an isogeny of degree ℓ^e using Vélu's formulas has complexity $\mathcal{O}(\ell^e)$ when naively implemented [24].*

*- **Optimized Algorithms**: By employing advanced algorithms, such as the double-point or three-point ladder methods, and using isogeny walks, the complexity can be reduced to $\mathcal{O}(e \log \ell)$ for small primes ℓ [25].*

Total Computational Cost *- **Alice's Computations**:*
- Compute ϕ_A of degree $\ell_A^{e_A}$: $\mathcal{O}(e_A \log \ell_A)$. - Compute $\phi_A(\mathcal{P}_B)$, $\phi_A(\mathcal{Q}_B)$: $\mathcal{O}(e_B \log \ell_B)$.
*- **Bob's Computations**:*
- Compute ϕ_B of degree $\ell_B^{e_B}$: $\mathcal{O}(e_B \log \ell_B)$. - Compute $\phi_B(\mathcal{P}_A)$, $\phi_B(\mathcal{Q}_A)$: $\mathcal{O}(e_A \log \ell_A)$.
*- **Shared Secret Computation**:*
- Compute ψ_A or ψ_B of degree $\ell_A^{e_A}$ or $\ell_B^{e_B}$, respectively.

Zero-Knowledge Proofs

Implementing zero-knowledge proofs for isogeny-based protocols can be computationally intensive.

Complexity Analysis *- **Proof Generation**: The prover must perform additional isogeny computations and hash evaluations. Complexity is $\mathcal{O}(e \log \ell)$.*

*- **Proof Verification**: The verifier performs similar computations, with complexity matching that of the prover.*

Comparison with Existing Protocols

SPAKE2 and J-PAKE: *- **Exponentiation Operations**: The dominant cost is modular exponentiations in groups of order q, with complexity $\mathcal{O}(n^3)$ for n-bit integers.*

*- **Total Cost**: Generally lower computational cost compared to isogeny-based protocols due to simpler arithmetic operations.*

Post-Quantum Protocols (e.g., lattice-based PAKE): *- **Lattice Operations**: Involve matrix multiplications and reductions, with complexity $\mathcal{O}(n^2)$ to $\mathcal{O}(n^3)$ depending on parameters [26].*

4.2 Communication Cost Analysis

We analyze the size of the data transmitted during the protocol execution.

Data Transmitted in I-PAKE

*- **Alice to Bob**:*
- Curve E_A: Encoded as a coefficient or j-invariant, size approximately $2n$ bits. - Points $\phi_A(\mathcal{P}_B)$, $\phi_A(\mathcal{Q}_B)$: Each point requires $2n$ bits (for x and y coordinates over $\mathbb{F}_{p^2}$).
*- **Bob to Alice**:*
- Similar data as above.
*- **Total Communication per Party**:*

$$\textit{Total Size} = 2n + 2 \times 2n = 6n \textit{ bits}. \tag{4.1}$$

Comparison with Existing Protocols

SPAKE2 and J-PAKE: *- **Group Elements**: Each group element transmitted is approximately n bits (assuming elliptic curve groups over $\mathbb{F}_p$).*
*- **Total Communication per Party**:*

$$\textit{Total Size} = 2n \textit{ bits}. \tag{4.2}$$

Post-Quantum Protocols (e.g., lattice-based PAKE): *- **Larger Public Keys**: Due to the nature of lattice-based schemes, public keys and messages can be significantly larger, ranging from several kilobytes to megabytes [28].*
*- **Total Communication**: Generally higher than isogeny-based protocols.*

4.3 Experimental Results

We implemented the proposed protocol using a software library optimized for isogeny-based cryptography. The implementation was tested on a standard workstation with the following specifications:
*- **Processor**: Intel Core i7-9700K @ 3.6 GHz - **Memory**: 16 GB RAM - **Operating System**: Ubuntu 20.04 LTS*

Implementation Details

*- **Programming Language**: C++, utilizing the SIDH library [29].*
*- **Parameters Used**:*
- Prime p of 768 bits (from SIKEp751 parameter set). - $\ell_A = 2$, $e_A = 372$, $\ell_B = 3$, $e_B = 239$.
- Hash Function: SHA-3-512. - KDF: HKDF with SHA-3-512.

Performance Metrics

We measured the following metrics:
*- **Key Generation Time**: Time taken to compute the secret isogenies ϕ_A and ϕ_B.*
*- **Shared Secret Computation Time**: Time taken to compute ψ_A, ψ_B, and derive the shared secret K.*
*- **Zero-Knowledge Proof Time**: Time for generating and verifying the proofs.*

Results

Table 1. Performance Metrics of I-PAKE Protocol

Operation	**Alice (ms)**	**Bob (ms)**
Key Generation	180	190
Shared Secret Computation	160	170
Zero-Knowledge Proof Generation	200	210
Zero-Knowledge Proof Verification	220	230
Total Time per Party	**760 ms**	**800 ms**

Comparison with Existing Protocols

For comparison, we implemented SPAKE2 using the same cryptographic library and measured its performance.

Table 2. Performance Comparison with SPAKE2

Protocol	**Total Time per Party (ms)**	**Security Level**
I-PAKE (This Work)	780	Post-Quantum
SPAKE2	50	Broken by Quantum Attacks

Discussion of Results

*- **Performance Trade-offs**:*

- The I-PAKE protocol incurs higher computational costs due to the complexity of isogeny computations. - The total execution time is under one second per party, which is acceptable for many applications.

*- **Security Advantages**:*

- Despite the higher computational overhead, I-PAKE offers quantum-resistant security. - SPAKE2 is significantly faster but does not provide security in the presence of quantum adversaries.

4.4 Memory Consumption Analysis

We analyzed the memory requirements of the protocol implementation.

Memory Usage

*- **I-PAKE**:*

- Requires storage of elliptic curve parameters, isogeny kernels, and intermediate points. - Peak memory usage per party was approximately 50 MB during execution.

*- **SPAKE2**:*

- Requires storage of group elements and scalars. - Peak memory usage per party was approximately 5 MB.

Discussion

- The increased memory consumption in I-PAKE is due to the larger sizes of the objects involved (e.g., points over $\mathbb{F}_{p^2}$) and the need to store intermediate computations.

4.5 Communication Efficiency

We measured the actual sizes of the messages transmitted during the protocol execution.

I-PAKE Communication Sizes

*- **Alice to Bob**:*
- Curve E_A: 192 bytes. - Points $\phi_A(\mathcal{P}_B)$, $\phi_A(\mathcal{Q}_B)$: Each 192 bytes. - Total: 576 bytes.
*- **Bob to Alice**:*
- Similar to above.
*- **Total Communication per Party**:*

$$\text{Total Size} = 576 \text{ bytes}. \tag{4.3}$$

Comparison with Existing Protocols

*- **SPAKE2**:*
- Each transmitted element (group element over $\mathbb{F}_p$): 96 bytes. - Total communication per party: 192 bytes.
*- **Lattice-Based PAKE (e.g., NewHope-based)**:*
- Total communication per party: Approximately 2 KB to 4 KB [26].

Discussion

- I-PAKE has higher communication costs compared to classical protocols but is more efficient than some post-quantum alternatives.

4.6 Implementation Considerations

Optimizations

*- **Use of Optimized Libraries**: Leveraging optimized isogeny-based cryptography libraries can improve performance.*
*- **Algorithmic Improvements**: Implementing advanced algorithms for isogeny computations, such as strategies for isogeny volcanoes [30], can reduce computational time.*
*- **Parallelization**: Exploiting multicore processors to parallelize independent computations.*

Challenges

*- **Complexity of Implementing ZK Proofs**: Designing efficient zero-knowledge proofs for isogeny-based protocols requires careful optimization to avoid significant overhead.*
*- **Parameter Selection**: Choosing appropriate parameters to balance security and performance is crucial.*

4.7 Summary of Performance Evaluation

Our performance evaluation demonstrates that while the proposed I-PAKE protocol incurs higher computational and communication costs compared to classical PAKE protocols, it remains practical for real-world applications requiring post-quantum security. The protocol offers a favorable trade-off between performance and security, outperforming some existing post-quantum alternatives in terms of communication efficiency.

5 Conclusion

In this paper, we have proposed a novel isogeny-based PAKE protocol that achieves post-quantum security by leveraging the hardness of the Supersingular Isogeny Problem. We provided detailed mathematical descriptions, rigorous security proofs, and comprehensive performance evaluations. Our protocol demonstrates that isogeny-based cryptography can be effectively integrated into PAKE protocols, offering quantum-resistant security with acceptable performance metrics.

While the protocol incurs higher computational overhead compared to classical counterparts, the security advantages in the context of quantum computing are significant. Future work may focus on optimizing isogeny computations further, exploring alternative isogeny-based constructions, and implementing the protocol on hardware platforms to enhance performance.

References

[1] *P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in* Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.*

[2] *M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," in* Topics in Cryptology – CT-RSA 2005*, vol. 3376, Berlin, Heidelberg: Springer, 2005, pp. 191–208.*

[3] *F. Hao and P. Y. A. Ryan, "J-PAKE: authenticated key exchange without PKI,"* Transactions on Computational Science XI*, vol. 6480, pp. 192–206, 2010.*

[4] *H. Krawczyk and H. Wee, "The OPAQUE asymmetric PAKE protocol," in* 2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 488–505.*

[5] *O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in* Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, 2005, pp. 84–93.*

[6] *R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory,"* Deep Space Network Progress Report*, vol. 44, pp. 114–116, 1978.*

[7] *J. Ding,* Multivariate Public Key Cryptosystems*. Berlin, Heidelberg: Springer, 2008.*

[8] *D. Jao and L. De Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in* Post-Quantum Cryptography*, vol. 7071, Berlin, Heidelberg: Springer, 2011, pp. 19–34.*

[9] *Z. Zhang, Y. Hu, and H. Huang, "A post-quantum password-authenticated key exchange protocol based on lattices,"* IEEE Access*, vol. 6, pp. 66 987–66 995, 2018.*

[10] *L. De Feo, D. Jao, and J. Plût, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,"* Journal of Mathematical Cryptology*, vol. 8, no. 3, pp. 209–247, 2014.*

[11] *Z. Sun and Y. Tian, "An isogeny-based password-authenticated key exchange protocol,"* Cryptology ePrint Archive*, Report 2019/459, 2019.*

[12] *M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in* Advances in Cryptology – EUROCRYPT 2000*, vol. 1807, Berlin, Heidelberg: Springer, 2000, pp. 139–155.*

[13] *J. H. Silverman,* The Arithmetic of Elliptic Curves*, 2nd ed. New York, NY, USA: Springer, 2009.*

[14] *D. Hankerson, A. J. Menezes, and S. Vanstone,* Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer, 2004.*

[15] *A. J. Menezes,* Elliptic Curve Public Key Cryptosystems*. Boston, MA, USA: Kluwer Academic Publishers, 1993.*

[16] *D. Husemoller,* Elliptic Curves*, 2nd ed. New York, NY, USA: Springer, 2004.*

[17] *S. D. Galbraith,* Mathematics of Public Key Cryptography*. Cambridge, UK: Cambridge University Press, 2012.*

[18] *A. K. Pizer, "Ramanujan graphs and Hecke operators,"* Bulletin of the American Mathematical Society*, vol. 23, no. 1, pp. 127–137, 1990.*

[19] *M. El Baraka and S. Ezzouak, "Quantum-resistant modifications to ECDSA for blockchain security," in* Journal of Cyber Security Technology*, Taylor & Francis, 2025, pp. 1–19.*

[20] *A. M. Childs, D. Jao, and V. Soukharev, "Constructing elliptic curve isogenies in quantum subexponential time,"* Journal of Mathematical Cryptology*, vol. 8, no. 1, pp. 1–29, 2014.*

[21] *J. Vélu, "Isogénies entre courbes elliptiques,"* C. R. Acad. Sci. Paris Sér. A-B*, vol. 273, pp. 238–241, 1971.*

[22] *S. D. Galbraith, C. Petit, B. B. Shani, and Y. B. Ti, "On the security of supersingular isogeny cryptosystems," in* Advances in Cryptology – ASIACRYPT 2016*, vol. 10031, Berlin, Heidelberg: Springer, 2016, pp. 63–91.*

[23] *D. X. Charles, K. E. Lauter, and E. Z. Goren, "Cryptographic hash functions from expander graphs,"* Journal of Cryptology*, vol. 22, no. 1, pp. 93–113, 2009.*

[24] *C. Costello, "Supersingular isogeny key exchange for beginners," in* Cryptographers' Track at the RSA Conference*, vol. 12006, Cham: Springer, 2020, pp. 3–27.*

[25] *L. De Feo, "Algorithms for supersingular isogeny problems,"* Mathematics of Public Key Cryptography*, Ph.D. thesis, École Polytechnique, 2011.*

[26] *E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—a new hope," in* 25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 327–343.*

[27] *M. El Baraka and S. Ezzouak, "Optimised quantum-resistant signature protocol for Bitcoin using CSIDH," in* International Journal of Blockchains and Cryptocurrencies*, vol. 6, no. 1, Inderscience Publishers (IEL), 2025, pp. 18–41.*

[28] *J. Hoffstein, J. Pipher, J. H. Silverman, D. J. Whyte, and W. Zhang, "A signature scheme from the learning with errors problem,"* IACR Cryptology ePrint Archive*, 2017.*

[29] Microsoft Research SIDH Library*, Available at: https://www.microsoft.com/en-us/download/details.aspx?id=52326, accessed on October 20, 2024.*

[30] *A. V. Sutherland, "Isogeny volcanoes," in* ANTS IX: Proceedings of the Ninth Algorithmic Number Theory Symposium*, 2011, pp. 507–530.*

[31] *P. Goswami, M. M. Singh, and B. Bhuyan, "A new public key scheme based on integer factorization and discrete logarithm," in* Palestine Journal of Mathematics*, vol. 6, no. 2, 2017, pp. 580–584.*

[32] *K. F. Soro, E. D. Akeke, and K. M. Kouakou, "An application of Young tableaux to cryptography," in* Palestine Journal of Mathematics*, vol. 9, no. 2, 2020.*

[33] *R. Al-Shorbassi and M. M. Al-Ashker, "Skew* $(\mu_1 + u\mu_2 + v\mu_3 + w\mu_4 + uv\mu_5 + vw\mu_6 + uw\mu_7 + uvw\mu_8)$ *constacyclic codes over* $\mathbb{F}_q[u,v,w] = \langle u^2-1, v^2-1, w^2-1, uv-vu, vw-wv, wu-uw\rangle$*," in* Palestine Journal of Mathematics*, vol. 12, no. 4, 2023, pp. 331–339.*

Author information

Mohammed El Baraka, Department of Mathematics, Faculty of sciences Dhar Al Mahraz, University Sidi Mohamed Ben Abdellah, Fez, Morocco.
E-mail: mohammed.elbaraka5@usmba.ac.ma

Siham Ezzouak, Department of Mathematics, Faculty of sciences Dhar Al Mahraz, University Sidi Mohamed Ben Abdellah, Fez, Morocco.
E-mail: sezzouak@gmail.com

Received: 2024-10-03
Accepted: 2025-03-10