Mathematics Interdisciplinary Research **10** (4) (2025) 431 − 446

Original Scientific Paper

A Post-Quantum Zero-Knowledge Identification Scheme

Maryam Rezaei Kashi and Mojtaba Bahramian⋆

Abstract

In this paper, we introduce a zero-knowledge identification protocol designed for authentication within the supersingular isogeny Diffie-Hellman (SIDH) key exchange framework. The protocol allows both parties to participate as either the prover or the verifier, with the goal of proving that they know their private information. We show the completeness and soundness of the protocol by showing that the privacy of both the prover and the verifier depends on the difficulty of solving the extended isogeny logarithm problem. A new authentication protocol for SIDH is presented in this paper, that is secure against attacks from eavesdroppers.

Keywords: Supersingular isogeny, Post-quantum key exchange, Authentication, Zero-knowledge proof.

2020 Mathematics Subject Classification: 81P94, 14H52, 94A60, 14K02.

How to cite this article
M. Rezaei Kashi and M. Bahramian, A post-quantum zero-knowledge identification scheme, *Math. Interdisc. Res.* **10** (4) (2025) 431-446.

1. Introduction

In cryptography, a zero-knowledge proof is a method by which a prover can convince a verifier that they possess knowledge of a secret without disclosing any information about the secret itself. The notion of zero-knowledge proof was first presented by Goldwasser, Micali, and Rackoff in their 1989 publication [1]. The privacy-preserving nature of zero-knowledge proof is a key feature that has made

⋆Corresponding author (E-mail: bahramianh@kashanu.ac.ir)
Academic Editor: Seyfollah Mosazadeh
Received 4 November 2024, Accepted 14 February 2025
DOI: 10.22052/MIR.2025.255716.1483

it an important tool in cryptographic systems. Zero-knowledge proof can be used for authentication, where one party proves to another that he/she knows some confidential information related to the system, without revealing the information itself. For example, in [2] an algorithm is presented that uses zero-knowledge proof to know the factors of an RSA modulus, which can be used for authentication in an RSA cryptosystem. The zero-knowledge proof protocol relies on the hardness of certain mathematical problems, notably the integer factorization problem and the discrete logarithm problem. These problems are widely believed to be difficult to solve, providing a strong foundation for the security of zero-knowledge proofs. The security of numerous cryptographic systems is at risk due to the emergence of quantum computers, which can solve certain problems like the factoring large integers and solving DLP using Shor's algorithm [3]. To tackle this challenge, cryptographers have developed innovative cryptographic systems that can withstand quantum attacks.

One notable system is the Supersingular Isogeny Diffie-Hellman (SIDH) protocol, which serves as a quantum-resistant method for facilitating public key exchanges between two parties. The security of SIDH relies on the conjectured difficulty of discovering isogenies between supersingular elliptic curves. Once the two parties have successfully completed a key exchange using the SIDH protocol, they can use the resulting shared secret to encrypt and decrypt messages transmitted over an insecure channel. However, an attacker may try to impersonate one of the parties and disrupt the message exchange process. To prevent this, in this paper we present a simple and practical algorithm for authentication that can be used after the SIDH protocol. In this scheme, each party uses a commutative diagram to prove their knowledge of the secret isogenies using zero-knowledge proof.

1.1 Related works

Cryptography based on supersingular isogenies offers a promising method for securing against quantum threats. Due to the small size of keys and low communication cost, this is a significant field of study within post-quantum cryptography. The initial protocol using supersingular isogenies was a hash function proposed by Charles et al. in 2006, which used the supersingular isogeny graph [4]. Jao and De Feo's work in 2011 [5] explored a post-quantum cryptography, specifically presenting a key exchange and public-key system built upon supersingular elliptic curves. In 2012, Sun et al. introduced a robust designated verifier signature scheme grounded in isogenies between supersingular elliptic curves [6]. In 2014, an extended algorithm of the key exchange protocol was proposed by Jao et al., that included a zero-knowledge identification scheme [7]. These protocols depend on the difficulty of solving the problem of finding isogenies between supersingular elliptic curves to ensure their security. Since then, numerous papers have built upon this technique, including [8] and many others that further demonstrate its and relevance in the field.

Additional significant contributions to supersingular isogeny-based cryptogra-

phy include the undeniable signature scheme introduced by Jao et al. in 2014 [9]. Galbraith et al. introduced an authentication protocol and signature schemes in 2016, basing their security on the computational hardness of determining the endomorphism ring [10]. In 2017, Yoo et al. proposed a digital signature scheme based on supersingular elliptic curve isogenies, offering small key sizes and security against quantum attacks [11]. Srinath et al. extended the Jao-Soukharev undeniable signature scheme to support a blind signature scheme based on supersingular elliptic curve isogenies [12]. Peng et al. presented an identity-based signature scheme in 2020, which utilizes isogenies [13]. In 2022, Eslami and Bahramian introduced an efficient multi-secret sharing scheme utilizing the De Feo and Jao key exchange protocol [14], and Dey et al. designed a signcryption scheme employing isogeny-based cryptography [15].

1.2 Our motivation

The advent of quantum computers has weakened the security of numerous cryptographic systems, prompting cryptographers to develop new systems resilient to quantum attacks. Isogenies of supersingular elliptic curves are important tools in post-quantum cryptography, as they provide reduced communication costs and smaller public keys in comparison to other areas of post-quantum cryptography.

The SIDH is a post-quantum cryptographic algorithm designed to establish a secret key between two parties over an insecure communication channel. It operates on walks within a supersingular isogeny graph and features the smallest key size among all post-quantum key exchange methods, positioning it as a significant tool in post-quantum cryptography. Following a key exchange, one party usually encrypts a message using the shared key and transmits it to the other party.

However, a potential issue in message exchange is the possibility of a hacker interfering with the procedure and accessing information. To address this problem, digital signature algorithms and authentication technology can be used. A message that includes the sender's digital signature associates a public key with an identity, allowing verification that the public key indeed belongs to the sender. Authentication systems allow parties to prove their identities to each other. One of the commonly used authentication methods is zero-knowledge proof.

In this paper, an authentication protocol using zero-knowledge proof during message exchange in SIDH is proposed. Let's assume Alice and Bob perform a key exchange using SIDH. The main idea is that if a person can prove that they know some of the private information in SIDH of Alice or Bob, the other party can be sure that the person is indeed Alice or Bob. This authentication protocol enhances the security of the message exchange process and ensures that the parties involved are who they claim to be.

1.3 Outline of the paper

The organization of this study is detailed below:

In Section 1.3, we present the essential concepts related to elliptic curves, isogenies, supersingular isogeny graphs, and challenging problems in isogenies. Section 1.3 provides an examination of both the SIDH key exchange and its implementation within a public-key cryptosystem. The security of these protocols relies on the hardness of finding a path between two vertices in a graph of supersingular isogenies. In Section 1.3, we define zero-knowledge proofs and review a zero-knowledge protocol for identifying an isogeny, as introduced in [5]. Finally, in Section 1.3, we introduce our zero-knowledge identification scheme, which is founded on the hardness of the extended isogeny logarithm problem.

2. Preliminaries

2.1 Elliptic curves and isogenies

In this section, we review key concepts concerning elliptic curves and isogenies that are needed throughout the paper. For a more comprehensive study, we direct the reader to [16–19].

2.1.1 Elliptic curves

Let $\mathbb{F}_q$ denote the finite field with order $q = p^n$, where $p \neq 2, 3$ is a prime and n is a positive integer. An elliptic curve E over $\mathbb{F}_q$ is described by an equation of the form

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \overline{\mathbb{F}}_q$, the discriminant $\Delta = -16(4a^3 + 27b^2)$ of E is nonzero, and E includes an additional point $\mathcal{O}$, known as the point at infinity. The points on E form an Abelian group, with $\mathcal{O}$ as the identity element. The group operation on E is denoted additively; for two points P and Q, their sum is given by $P + Q$. For a point P and a positive integer m, $mP = P + \cdots + P$ (repeated m times). If $m < o$, $mP = (-m)(-P)$, and $0P = \mathcal{O}$. If a and b belong to an extension field K of $\mathbb{F}_q$, then we say that E is defined over K. The subgroup

$$E(K) = \{(x, y) \in K^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

of E is called the K-rational points on E. We focus on $E(\mathbb{F}_q)$ and denote it by E.

For a natural number m, let's define the m-torsion subgroup of E as the set of all points P in E such that mP is the identity element $\mathcal{O}$. In the case where m is not divisible by p, $E[m]$ takes the form $\mathbb{Z}_m \times \mathbb{Z}_m$. On the other hand, if p divides m, we write $m = p^r n$, $\gcd(n, p) = 1$, then $E[m] = \mathbb{Z}_n \times \mathbb{Z}_n$ or $\mathbb{Z}_m \times \mathbb{Z}_n$. Furthermore, if the p-torsion subgroup contains only the identity, the curve is said to be supersingular. Otherwise, it's classified as ordinary.

Hasse's theorem states that $|q+1-\#E(\mathbb{F}_q)| < 2\sqrt{q}$, the value $t = q+1-\#E(\mathbb{F}_q)$ is called the trace of E. For a supersingular elliptic curve E, $t \equiv 0 \pmod{p}$, equivalently $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$.

The point count on an elliptic curve can be computed in polynomial time [20], making it feasible to determine whether a curve is ordinary or supersingular. For an elliptic curve E given by the Weierstrass equation $y^2 = x^3 + ax + b$, the j-invariant of E is defined by $j(E) = 1728(4a^3)/(4a^3 + 27b^2)$. We say that two elliptic curves E and E' are isomorphic over $\overline{\mathbb{F}}_q$, if $j(E) = j(E')$. Therefore, the j-invariant is used to label the isomorphism classes. Each isomorphism class of supersingular curves has a representative over $\mathbb{F}_{p^2}$, hence, for a supersingular elliptic curve E, $j(E) \in \mathbb{F}_{p^2}$. In this case, $t \in \{0, \pm p, \pm 2p\}$ using Hasse's theorem.

2.1.2 Isogenies

An isogeny between two elliptic curves E and E' is a non-constant rational map $\phi : E \to E'$ that preserves the point at infinity, or equivalently, a surjective homomorphism between E and E'. By the first group isomorphism theorem, we have $E/(\ker(\phi)) \cong E'$. If the coefficients of ϕ are rational functions in a field K, then ϕ is said to be defined on K. For any isogeny $\phi : E(K) \to E'(K)$, there is an injection of function fields defined by $\phi^* : K(E') \longrightarrow K(E)$. The degree of ϕ is defined as $\deg(\phi) = [K(E) : \phi^* K(E')]$. The isogeny φ is called separable, if $K(E)/\phi^* K(E')$ is a separable extension; otherwise, it is called inseparable. Formally defined, an isogeny Φ can be represented as $\varphi(x, y) = \left(\frac{p_1(x)}{q_1(x)}, \frac{p_2(x)}{q_2(x)} y\right)$, where p_1 and q_1 are co-prime polynomials, and $\deg(\phi) = \max\{\deg p(x), \deg q(x)\}$. In the case that ϕ is separable, $\#\ker\phi = \deg\phi$. An ℓ-isogeny is an isogeny of degree ℓ. The composition of an ℓ_1-isogeny and an ℓ_2-isogeny is an $\ell_1\ell_2$-isogeny. Moreover, each isogeny can be expressed as a composition of isogenies with prime degrees.

If $p \nmid m$, then $[m]$ is separable and its kernel is the torsion subgroup $E[m]$, so we have $\deg[m] = m^2$.

For an isogeny $\phi : E \to E'$, there exists a dual isogeny $\hat{\phi} : E' \to E$ that has the same degree. This dual isogeny satisfies: $\hat{\phi} \circ \phi = [\deg\phi]_E$, and $\phi \circ \hat{\phi} = [\deg\phi]_E$.

The q-power Frobenius homomorphism is defined as

$$\begin{aligned} \phi_q : E &\longrightarrow E \\ (x, y) &\longmapsto (x^q, y^q), \end{aligned}$$

and has degree q. It is inseparable and satisfies the equation $\phi_q^2 - [t]\phi_q + [q] = 0$, where t is the Frobenius trace. Using this equation we can obtain $\hat{\phi_q} = t - \phi_q$. Moreover, each isogeny can be considered as a composition of a power of ϕ_q and a separable isogeny.

According to Tate's theorem, elliptic curves E and E' are isogenous over $\mathbb{F}_q$, iff $E(\mathbb{F}_q)$ and $E'(\mathbb{F}_q)$ have the same order.

Let $\ell \neq p$ be a prime. The polynomial $\Phi_\ell(X, Y) \in \mathbb{F}_{p^2}[X, Y]$ known as the ℓ-th modular polynomial, has degree $\ell + 1$ in each variable. If E and E' are two ℓ-isogenous elliptic curves, then $\Phi_\ell(j(E), j(E')) = 0$. An isogeny from an elliptic curve to itself is known as an endomorphism. The set of endomorphisms of an elliptic curve, together with the zero map, is denoted by $End(E)$; this set forms

a ring under point-wise addition and function composition. One of the simplest endomorphisms is multiplication by an integer $m : P \longmapsto mP$. Hence, there exists a homomorphism between $\mathbb{Z}$ and $End(E)$. Since $\phi_q \notin \mathbb{Z}$, we have $End(E) \neq \mathbb{Z}[\phi_q]$. If E is an ordinary elliptic curve, then $End(E) = \mathbb{Z}[\phi_q]$. In the case of supersingular elliptic curves, however, the endomorphism ring is larger.

By applying Vélu's formula, we can compute a separable isogeny using its kernel. For a subgroup $G \subseteq E$, Vélu's formula allows us to construct a curve $E' \approx E/G$ and an isogeny $\phi : E \to E'$ such that $\ker \phi = G$. The computational cost is linearly dependent on the size of G. If G is invariant under the q-power Frobenius endomorphism, then both G and the corresponding isogeny with kernel G are defined over $\mathbb{F}_q$. If the degree of the isogeny is sufficiently smooth, it can be computed efficiently by decomposing it into isogenies with prime orders, and employing Vélu's formula to obtain them.

For a supersingular elliptic curve E with $\#E(\mathbb{F}_{p^2}) = (p \pm 1)^2$, the p^2-power Frobenius ϕ_{p^2} verifies

$$\phi_{p^2}^2 \pm [2p]\phi_{p^2} + [p^2] = 0 \Longrightarrow (\phi_{p^2} \pm [p])^2 = 0 \Longrightarrow \phi_{p^2} = [\pm p],$$

indicating that the p^2-power Frobenius acts as a multiplication map. If $\#\ker \phi = \ell$ is coprime to p, then $\ker \phi$ remains fixed by $[\pm p]$. In fact, $[\pm p]$ are permutations of $\ker \phi$.

2.2 Supersingular isogeny graphs

The ℓ-supersingular isogeny graph is a graph constructed over the finite field $\mathbb{F}_{p^2}$, where p and ℓ are two distinct prime numbers. The graph $G_\ell(\mathbb{F}_{p^2}) = (\mathcal{V}, \mathcal{E})$, is defined in the following way: the vertex set $\mathcal{V}$ consists of all the j-invariants of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, and the edge set $\mathcal{E}$ consists of the ℓ-isogenies that connect these j-invariants. Specifically, there is an edge between two vertices j and j', if there exists an ℓ-isogeny between E and E' such that $j(E) = j$ and $j(E') = j'$. Since there is also a corresponding dual isogeny $\phi : E' \to E$, the graph is undirected.

The order of the ℓ-supersingular isogeny graph is given by $\#\mathcal{V} = p/12 + \epsilon$, where ϵ depends on the residue class of p modulo 12. This expression derives from a counting argument rooted in the Weil conjectures, which connect the count of points on an elliptic curve over a finite field to its j-invariant. Additionally, the ℓ-supersingular isogeny graph is $(\ell + 1)$-regular, meaning that each vertex has precisely $\ell + 1$ neighboring vertices. In other words, every elliptic curve in $\mathbb{F}_{p^2}$ has exactly $\ell+1$ ℓ-isogenous elliptic curves. This property is essential for cryptographic applications of the graph, such as constructing key exchange protocols based on the Diffie-Hellman problem in the group of ℓ-isogenies.

Another important property of the ℓ-supersingular isogeny graph is that it is Ramanujan [21], which means that the absolute value of the eigenvalues of its adjacency matrix, which measures the connectivity of the graph, are all bounded

by $2\sqrt{\ell}$. This property has important consequences for the spectral analysis of the graph and its applications in cryptography because it ensures that the graph has good expansion properties and a small diameter.

It is also worth noting that the ℓ-supersingular isogeny graph has many interesting algebraic and geometric properties that have been studied extensively in recent years. These properties include the existence of large Galois groups acting on the graph, the relationship between the graph and modular forms, and the connection between the graph and the arithmetic of quaternion algebras. These features have resulted in a more profound insight into the structure and characteristics of the graph, while also creating new opportunities for exploration in elliptic curve cryptography and its related areas.

An intriguing aspect of the ℓ-supersingular isogeny graph is its ability to be decomposed into connected component graphs corresponding to supersingular elliptic curves of orders p^2+1+t, where $t \in \{0, \pm p, \pm 2p\}$. For each value of t, there exists a distinct connected component graph; however, the first three graphs are relatively small. Notably, $G_\ell(\mathbb{F}_{p^2})$ is isomorphic to the graphs corresponding to $\pm 2p$. The ℓ-supersingular isogeny graph serves as a crucial entity in the exploration of elliptic curves and their applications in cryptography. Its characteristics, including being $(\ell+1)$-regular and Ramanujan, have significant implications for its cryptographic utility. Furthermore, the algebraic and geometric attributes of the graph have contributed to an enhanced comprehension of its structure and properties, paving the way for new research avenues in the field.

2.3 Hard problems in isogenies

In this section, $\mathcal{G}(1^k)$ is considered a prime generator that receives the parameter k as input and generates a k-bit prime p, where $p \equiv 3 \pmod 4$. The set $\mathbf{E}_{(p+1)^2}$ represents the collection of j-invariants in $G_\ell(\mathbb{F}_{p^2})$ that have $(p+1)^2$ points. Additionally, the set of isogenies $E \to E'$ is represented by $\mathbf{Iso}(E, E')$. The general isogeny problem involves finding an isogeny $\phi : E \to E'$, for supersingular elliptic curves E and E' over $\mathbb{F}_{p^2}$.
We now introduce some hardness assumptions associated with supersingular elliptic curves.

Assumption 1 (isogeny). Suppose $p \leftarrow \mathcal{G}(1^k)$ and $E, E' \leftarrow \mathbf{E}_{(p+1)^2}$. For any Probabilistic Polynomial-Time (PPT) adversary $\mathcal{A}$, the probability

$$Pr[\phi \leftarrow \mathcal{A}(p, E, E') : \phi \in \mathbf{Iso}(E, E')],$$

is negligible.

Specifically, the ℓ-power isogeny problem involves finding an exponent e and an ℓ^e-isogeny between two supersingular elliptic curves over $\mathbb{F}_{p^2}$. This problem is equivalent to finding a path between two specified vertices in an ℓ-isogeny graph of supersingular elliptic curves.

Assumption 2 (ℓ power-isogeny). Let ℓ be a prime number, and suppose $p \leftarrow \mathcal{G}(1^k)$ and $E, E' \leftarrow \mathbf{E}_{(p+1)^2}$. For any PPT adversary $\mathcal{A}$, the probability

$$Pr[e, \phi \leftarrow (\mathcal{A}, E, E') : \phi \in \mathbf{Iso}(E, E'), deg(\phi) = \ell^e],$$

is negligible.

In certain cases, both a point and its image are given in the problem. Let E and E' be two supersingular elliptic curves over $\mathbb{F}_{p^2}$, $P \in E$ and $Q \in E'$. The isogeny logarithm problem (ILP) is to find an exponent e and an isogeny $\phi : E \to E'$ of degree ℓ^e such that $\phi(P) = Q$.

Assumption 3 (ILP). Let let ℓ be a prime number, and suppose $p \leftarrow \mathcal{G}(1^k)$, $E, E' \leftarrow \mathbf{E}_{(p+1)^2}$, $P \in E$, and $Q \in E'$. For any PPT adversary $\mathcal{A}$, the probability

$$Pr[e, \phi \leftarrow (\mathcal{A}, E, E') : \phi \in \mathbf{Iso}(E, E'), deg(\phi) = \ell^e, \phi(P) = Q],$$

is negligible.

Now, let E and E' be two supersingular elliptic curves over $\mathbb{F}_{p^2}$, $P_1, \ldots, P_n \in E$ and $Q_1, \ldots, Q_n \in E'$. The Extended Isogeny Logarithm Problem (EILP) is to find an exponent e and an isogeny $\phi : E \to E'$ of degree ℓ^e, such that $\phi(P_i) = Q_i$, for all $i = 1, \ldots, n$.

Assumption 4 (EILP). Let ℓ be a prime number, and suppose $p \leftarrow \mathcal{G}(1^k)$, $E, E' \leftarrow \mathbf{E}_{(p+1)^2}$, and $P_1, \ldots, P_n \in E$ and $Q_1, \ldots, Q_n \in E'$. For any PPT adversary $\mathcal{A}$, the probability

$$Pr[e, \phi \leftarrow \mathcal{A}(E, E') : \phi \in \mathbf{Iso}(E, E'), deg(\phi) = \ell^e, \phi(P_i) = Q_i, i = 1, \ldots, n],$$

is negligible.

3. SIDH key exchange

In this section, we will discuss the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol and its application in a public key cryptosystem. The protocols were introduced in [5], and their security relies on the comptational difficulty of determining a path between two specified vertices in a graph of supersingular isogenies.

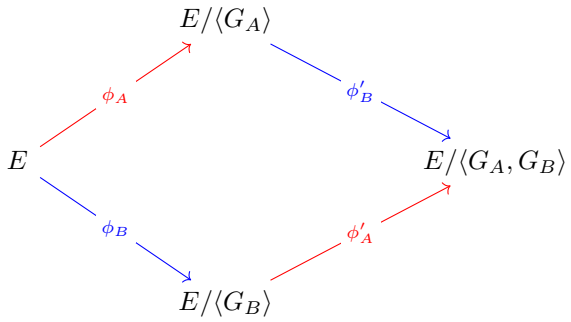
The SIDH protocol uses supersingular elliptic curves with smooth orders. Although discrete logarithms on these curves are easy, they are unsuitable for cryptography. However, this does not affect the security of the SIDH protocol because the hardness of the discrete logarithm problem is not important in this scenario. Constructing curves of smooth order is easy in supersingular cases, and a large number of easily computable isogenies can be obtained.

A prime generator $\mathcal{G}_{\ell_1,\ell_2}(1^k)$ outputs primes p of size k and of the form $\ell_1^{e_1}\ell_2^{e_2}f - 1$, where ℓ_1 and ℓ_2 are small primes, f is a small cofactor, and $\ell_1^{e_1} \approx \ell_2^{e_2} \approx O(p^{1/2})$.

Let ℓ_A and ℓ_B be two different prime numbers, and let a prime p obtained from the generator $\mathcal{G}_{\ell_A,\ell_B}(1^\lambda)$. We also have a supersingular elliptic curve E such that $E \leftarrow \mathbf{E}_{(p+1)^2}$.

The public parameters for the SIDH protocol consist of the supersingular elliptic curve E, the points P_A, Q_A such that $\langle P_A, Q_A\rangle = E[\ell_A^{e_A}]$, and the points P_B, Q_B such that $\langle P_B, Q_B\rangle = E[\ell_B^{e_B}]$. The key exchange between Alice and Bob is performed through the following steps:

1. Alice selects two random elements m_A and n_A from $\mathbb{Z}_{\ell_A^{e_A}}$, such that at least one of them is not divisible by ℓ_A. Then, she computes an isogeny $\phi_A : E \to E_A$ with kernel $\langle G_A\rangle := \langle [m_A]P_A + [n_A]Q_A\rangle$.
2. Bob randomly chooses $m_B, n_B \in \mathbb{Z}_{\ell_B^{e_B}}$, such that at least one of them is not divisible by ℓ_B, and computes an isogeny $\phi_B : E_0 \to E_B$ with the kernel $\langle G_B\rangle := \langle [m_B]P_B + [n_B]Q_B\rangle$.
3. Alice computes $\{\phi_A(P_B), \phi_A(Q_B)\}$, and sends $\{\phi_A(P_B), \phi_A(Q_B), E_A\}$ to Bob.
4. Similarly, Bob sends $\{\phi_B(P_A), \phi_B(Q_A), E_B\}$ to Alice.
5. Alice computes an isogeny $\phi'_A : E_B \to E_{AB}$ with kernel $\langle [m_A]\phi_B(P_A) + [n_A]\phi_B(Q_A)\rangle$.
6. Bob computes an isogeny $\phi'_B : E_A \to E_{AB}$ with kernel $\langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B)\rangle$.



Alice and Bob can then use the common j-invariant of E_{AB} for their secret key exchange, which is given by:

$$\begin{aligned} E_{AB} &= \phi'_B(\phi_A(E_0)) \\ &= \phi'_A(\phi_B(E_0)) \\ &= E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B\rangle. \end{aligned}$$

The security of the SIDH protocol is based on the difficulty of the ℓ-power isogeny problem, which is believed to be hard, and there is no known efficient algorithm for

solving it. While traditional cryptographic protocols such as the Diffie-Hellman key exchange and elliptic curve cryptography are vulnerable to attacks by quantum computers, the SIDH protocol is designed to resist quantum attacks. This makes it a promising candidate for post-quantum cryptographic applications. Moreover, the SIDH protocol offers a quantum-resistant alternative to traditional cryptographic protocols such as the Diffie-Hellman key exchange and elliptic curve cryptography.

3.1 Public-key encryption based on SIDH

The protocol discussed in Section 1.3 can be used in a public key cryptosystem. The details are given below:

Setup: Alice and Bob select parameters $p \leftarrow \mathcal{G}_{\ell_A,\ell_B}(1^\lambda)$, $E_0 \leftarrow \mathbf{E}_{(p+1)^2}$, $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$, with small primes ℓ_A and ℓ_B. They also chooses a family of hash functions $\mathcal{H} = \{H_k\}_{k\in K}$, where K is a finite index set and $H_k : \mathbb{F}_{p^2} \to \{0,1\}^w$, for a fixed integer $w > 0$.

Key Generation: Alice randomly chooses m_A and n_A from $\mathbb{Z}_{\ell_A^{e_A}}$, such that $\gcd(m_A, \ell_A) = 1$ or $\gcd(n_A, \ell_A) = 1$. She then computes E_A, $\phi_A(P_B)$, and $\phi_B(Q_B)$ as described in Section 1.3, and randomly chooses an element $k \in_R K$. She publishes $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$, and keeps (m_A, n_A, k) as her private key.

Encryption: In order to transmit a message $m \in \{0,1\}^w$ to Alice, Bob chooses two random elements m_B and n_B from $\mathbb{Z}_{\ell_B^{e_B}}$, such that at least one of them is not divisible by ℓ_B. He computes $j(E_{AB})$ as described in Section 1.3, and then computes

$$h = H_k(j(E_{AB})), \quad c = h \oplus m.$$

He sends $(E_B, \phi_B(P_A), \phi_B(Q_A), c)$ to Alice.

Decryption: Alice computes the j-invariant $j(E_{AB})$ and puts

$$h = H_k(j(E_{AB})), \quad m = h \oplus c.$$

She recovers the message m by XORing h with the ciphertext c.

Note that the security of this public key cryptosystem is fundamentally based on the difficulty of the SIDH problem, which is the underlying problem used in the key exchange protocol.

4. Zero-knowledge proof

A zero-knowledge proof is a protocol that enables a prover to demonstrate to a verifier that a particular statement holds true, without disclosing any information beyond the statement's validity itself. In essence, the verifier gains no knowledge regarding the content of the statement or the proof, aside from knowing that it is valid. Generally, a zero-knowledge proof consists of several rounds of interaction between two parties, the prover and the verifier, wherein the verifier issues challenges to the prover, who then replies with a message. The verifier assesses the reply and subsequently decides whether to accept or reject it.

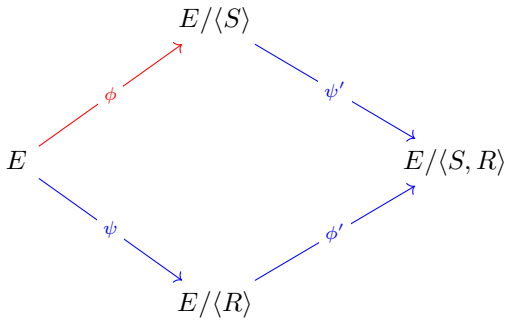
The goal of a zero-knowledge proof is to satisfy two conditions:
Completeness: When the statement is accurate, a truthful prover is capable of persuading the verifier of its correctness.
Soundness: When the statement is false, no prover, even one with unbounded computational power, can convince the verifier of its truth with probability greater than a negligible amount.

Zero-knowledge proofs have important applications in cryptography and information security, such as authentication, identification, and privacy-preserving computations.

4.1 Isogeny zero-knowledge proof

We review a zero-knowledge protocol of an isogeny, presented in [7]. Let E and $E/\langle S\rangle$ be public elliptic curves, and suppose that Alice knows the isogeny $\phi : E \to E/\langle S\rangle$ of degree $\ell_1^{e_1}$. She aims to prove to Bob that she possesses the generator S without disclosing its actual value.

Alice and Bob utilize the following diagram, where $\langle R\rangle$ represents a cyclic subgroup of the elliptic curve E of order $\ell_2^{e_2}$:



Alice applies Vélu's formula, $R' = \phi(R)$ and $S' = \psi(S)$ to compute the isogenies:

1. $\psi : E \to E_2 \cong E/\langle R\rangle$,
2. $\psi' : E_1 \to E_1/\langle R'\rangle \cong E/\langle R, S\rangle$,
3. $\phi' : E_2 \to E_2/\langle S'\rangle \cong E/\langle R, S\rangle$.

Here is the zero-knowledge protocol for ϕ:

Protocol

Secret parameters: A supersingular elliptic curve E defined over $\mathbb{F}_q$, has a primitive $\ell_1^{e_1}$-torsion point S that defines an isogeny $\phi : E \to E/\langle S\rangle$.
Public parameters: The elliptic curves E and $E/\langle S\rangle$, with $\{P, Q\}$ as a generator

set of $E[\ell_1^{e_1}]$, and their images $\phi(P), \phi(Q)$.
Identification: Repeat m times:

1. Alice randomly selects a point R of order $\ell_2^{e_2}$.
2. Alice sends $E_2 = E/\langle R\rangle$, $E' = E/\langle S, R\rangle$ and $\ell_2^{e_2}$ to Bob.
3. Bob randomly selects a bit b, and sends it to Alice.
4. In the case where $b = 0$, Alice discloses the points R and $\phi(R)$. Bob will accept these points if they both possess an order of $\ell_2^{e_2}$ and generate the kernels of the respective isogenies $E \to E_2$ and $E/\langle S\rangle \to E'$.
5. When $b = 1$, Alice discloses the point $\psi(S)$. Bob will accept if it has order $\ell_1^{e_1}$ and generates the kernel of the isogeny $E_2 \to E'$.

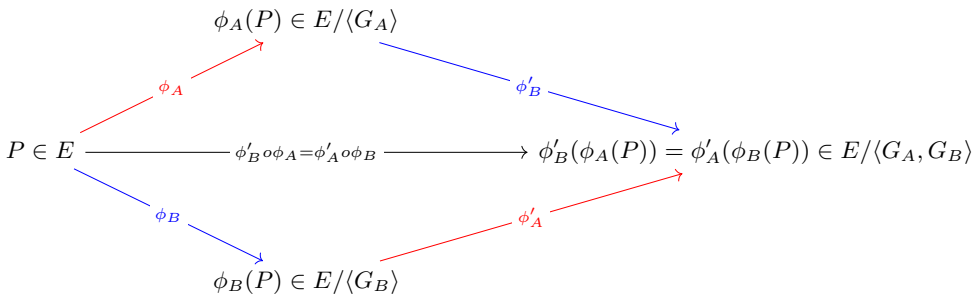
5. Our scheme

A zero-knowledge proof or protocol is a cryptographic protocol involving two parties: a prover and a verifier. In this protocol, the prover demonstrates to the verifier that they possess certain knowledge without revealing any information about it. The verifier is assured of the truth of the fact being claimed, but does not acquire any additional information from the proof.

Zero-knowledge protocols have various uses in cryptography, including authentication and identification. In this paper, we provide a zero-knowledge identification protocol that can be used in SIDH key exchange to authenticate the parties involved. The protocol allows both parties, Alice and Bob, to participate as either the prover or the verifier, with the goal of proving that they know their private information, such as isogenies ϕ_A, ϕ'_A for Alice and ϕ_B, ϕ'_B for Bob. After exchanging the key, Bob intends to send a message to Alice. However, Since the messages are exchanged over an unsecured channel, it is possible for someone else to intercept the message and pose himself/herself as Alice. To ensure that he is communicating with real Alice, Bob can ask her to prove her identity by demonstrating knowledge of private information that only Alice should know. For example, Alice could prove that she knows certain isogenies, such as ϕ_A and ϕ'_A.

To carry out the protocol, Alice and Bob repeat the following steps several times:

1. Bob selects a point $P \in E \setminus E[N_A] \cup E[N_B]$ and sends $\{P, \phi_B(P)\}$ to Alice. (challenge)
2. Alice responds by sending $\{\phi_A(P), \phi'_A(\phi_B(P))\}$ to Bob. (response)
3. Bob checks whether $\phi'_A(\phi_B(P))$ is equal to $\phi'_B(\phi_A(P))$. If they are not equal, Bob concludes that the other side is not Alice.



Theorem 5.1. *If Bob (Alice) is able to find a point P that belongs to the kernel of ϕ_A (ϕ_B), then he (she) can obtain the generator of the kernel of ϕ_A (ϕ_B).*

Proof. Suppose Bob obtains $P \in ker(\phi_A)$. In this case, $ker(\phi_A) \subset E[N_A] = \langle P_A, Q_A \rangle$, where $\{P_A, Q_A\}$ is a generator of N_A-torsion $E[N_A]$. Bob can obtain the integers k_1 and k_2 such that $P = [k_1]P_A + [k_2]Q_A$ by solving a discrete logarithm problem. Furthermore, Bob can obtain m_A and n_A using integer factorization as follows: $P = [k]([m_A]P_A + [n_A]Q_A)$. In this case, Bob obtains the generator $G_A = [m_A]P_A + [n_A]Q_A$ of $ker(\phi_A)$. However, G_A is secret for Alice. Similarly, if $P \in ker(\phi_B)$, Alice can obtain the generator of $ker(\phi_B)$ by solving a discrete logarithm problem and an integer factorization. □

Remark 1. To prevent Bob (Alice) from obtaining the generator of $ker(\phi_A)$ ($ker(\phi_B)$), P must be chosen such that $P \notin E[N_A] \cup E[N_B]$. This ensures that P does not belong to any subgroup of E that is generated by $\{P_A, Q_A\}$ ($\{P_B, Q_B\}$). Therefore, Bob (Alice) cannot use P to obtain the generators of the kernel of ϕ_A (ϕ_B) (Theorem 5.1).

Completeness: If Alice's claim is true, meaning she knows the isogenies ϕ_A and ϕ'_A, then she can accurately compute $(\phi_A(P), \phi'_A(\phi_B(P)))$ for any P chosen by Bob. Therefore, she can respond to all of Bob's challenges, and Bob should accept Alice's responses at every stage of the repetition.

Soundness: If Alice's claim is not true, meaning she doesn't know the isogenies ϕ_A and ϕ'_A, then she cannot accurately compute $(\phi_A(P), \phi'_A(\phi_B(P)))$. In fact, if $|E_A|$ and $|E'|$ are orders of E and E', respectively, then she can only guess $(\phi_A(P), \phi'_A(\phi_B(P)))$ with probability $1/(|E_A||E'|)$. After repeating the steps n times, she can accurately respond to all stages with probability $p = 1/(|E_A|^n|E'|^n)$. Therefore, Bob accepts all of the prover's responses with probability p, which becomes very small and approaches zero as n increases.

The security of the protocol

Privacy of prover:

Theorem 5.2. *Alice's privacy in the protocol is based on the EILP (Assumption 4).*

Proof. If Bob can obtain ϕ_A or ϕ'_A, then Bob's privacy is compromised. Suppose Alice and Bob repeat the steps n times. Bob chooses $P_1 \dots P_n$ and sends $(P_1, \phi_B(P_1)) \dots (P_n, \phi_B(P_n))$ to Alice. Alice responds by sending

$$(\phi_A(P_1), \phi'_A(\phi_B(P_1))) \dots (\phi_A(P_n), \phi'_A(\phi_B(P_n))),$$

to Bob. Hence, Bob must use

$$(P_1, \phi_A(P_1)), \dots, (P_n, \phi_A(P_n)),$$

and

$$(\phi_B(P_1), \phi'_A(\phi_B(P_1))), \dots (\phi_B(P_n), \phi'_A(\phi_B(P_n))),$$

two instances of the Extended Isogeny Logarithm Problem to solve two instances of the EILP to obtain ϕ_B and ϕ'_B. Therefore, Alice's privacy in our protocol depends on the hardness of the EILP. □

Privacy of verifier:

Theorem 5.3. *Bob's privacy in the protocol is based on hardness of the EILP (Assumption 4).*

Proof. If Alice can obtain ϕ_B or ϕ'_B, then the privacy of Bob is compromised. Suppose Alice and Bob repeat the steps n times. Bob chooses $P_1 \dots P_n$ and sends $(P_1, \phi_B(P_1)) \dots (P_n, \phi_B(P_n))$ to Alice. Alice must solve the EILP to obtain ϕ_B. Therefore, the privacy of Bob in the protocol depends on hardness of the EILP. □

6. Research achievements

This paper presents a zero-knowledge identification protocol that can be used for authentication in message exchange in SIDH protocol. The security of our protocol relies on the difficulty of the EILP. We have shown that the privacy of both Alice and Bob in our protocol depends on hardness of the EILP. Our protocol provides a secure and efficient way to authenticate users in message exchange in the SIDH protocol. This result contributes to the development of practical and secure post-quantum cryptographic schemes based on isogenies.

Conflicts of Interest. The authors declare that they have no conflict of interests regarding the publication of this article.

References

[1] S. Goldwasser, S. Micali and C. Rackoff, The knowledge complexity of interactive proof-systems, *SIAM J. Comput.* **18** (1989) 186 – 208.

[2] M. Rezaei Kashi and M. Bahramian, Proof of knowing the prime factors of a number using zero-knowledge proof, *Iran. J. Math. Sci. Inform.* **15** (2020) 33 − 46 (in Persian).

[3] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, *Proc. 35th Annu. Symp. Found. Comput. Sci., IEEE* (1994) 124 − 134.

[4] D. X. Charles, K. E. Lauter and E. Z. Goren, Cryptographic hash functions from expander graphs, *J. Cryptology* **22** (2009) 93 − 113, https://doi.org/10.1007/s00145-007-9002-x.

[5] D. Jao and L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, In PQCrypto, *Lecture Notes in Computer Science* **7071** (2011) 19−34, https://eprint.iacr.org/2011/506/20110918:024142.

[6] X. Sun, H. Tian and Y. Wang, Toward quantum-resistant strong designated verifier signature from isogenies, *in Proc. 4th Int. Conf. Intell. Netw. Collaborative Syst., Bucharest, Romania* (2012) 292 − 296.

[7] L. De Feo, D. Jao and J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *J. Math. Cryptol.* **8** (2014) 209 − 247.

[8] M. El Baraka and S. Ezzouak, Proposal of a new isogeny-based cryptographic protocol formal analysis and comparison, *Math. Interdisc. Res.* **10** (2025) 111 − 132, https://doi.org/10.22052/MIR.2024.255405.1476.

[9] D. Jao and V. Soukharev, Isogeny-based quantum-resistant undeniable signatures, *In Post-Quantum Cryptography, Michele Mosca (Ed.), Springer International Publishing, Cham* (2014) 160 − 179.

[10] S. D. Galbraith, C. Petit and J. Silva, Identification protocols and signature schemes based on supersingular isogeny problems, *Proceedings of Asiacrypt (1), Lecture Notes in Computer Science 10624*, (2017) 3 − 33.

[11] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao and V. Soukharev, A post-quantum digital signature scheme based on supersingular isogenies, *Cryptology ePrint Archive*, Report 2017/186, (2017), http://eprint.iacr.org/2017/186.

[12] M. S. Srinath and V. Chandrasekaran, Isogeny-based quantum-resistant undeniable blind signature scheme, *IACR Cryptol. ePrint Arch.* **20** (2018) 9−18, https://doi.org/10.6633/IJNS.201801.20(1).02.

[13] C. Peng, J. Chen, L. Zhou, K. K. R. Choo and D. He, CsiIBS: a post-quantum identity-based signature scheme based on isogenies, *J. Inf. Secur. Appl.* **54** (2020) #102504.

[14] K. Eslami and M. Bahramian, An isogeny-based quantum-resistant secret sharing scheme, *Filomat* **36** (2022) 3249 – 3258, https://doi.org/10.2298/FIL2210249E.

[15] K. Dey, S. K. Debnath, P. Stanica and V. Srivastava, A post-quantum sign-cryption scheme using isogeny-based cryptography, *J. Inf. Secur. Appl.* **69** (2022) #103280, https://doi.org/10.1016/j.jisa.2022.103280.

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

[17] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Boca Raton, 2008.

[18] J. H. Silverman, J. Pipher and J. Hoffstein, *An Introduction to Mathematical Cryptography*, Springer, New York, 2008.

[19] J. Silva Velón, Zero-Knowledge Proofs and Isogeny-Based Cryptosystems, Doctoral dissertation, Universitat Pompeu Fabra, 2021.

[20] L. Dewaghe, Remarks on the Schoof-Elkies-Atkin algorithm, *Math. Comp.* **67** (1998) 1247 – 1252.

[21] A. K. Pizer, Ramanujan graphs and Hecke operators, *Bull. Amer. Math. Soc. (N.S.)* **23** (1990) 127 – 137.

Maryam Rezaei Kashi
Department of Pure Mathematics,
Faculty of Mathematical Sciences,
University of Kashan,
Kashan, I. R. Iran
e-mail: mrezaei.k@grad.kashanu.ac.ir

Mojtaba Bahramian
Department of Pure Mathematics,
Faculty of Mathematical Sciences,
University of Kashan,
Kashan, I. R. Iran
e-mail: bahramianh@kashanu.ac.ir