NIPES

Journal of Science and Technology Research

Journal homepage: www.nipesjournals.org.ng

A Supersingular Elliptic Curve Isogeny-Based Quantum Resistant Cryptographic Key Exchange Scheme

[1]Tom, J. J.,[*], [2]Onyekwelu, B. A., [3]Anebo, N. P. [4]Nwanze, A. C. [5]Akpan, A. G. [6]Ejodamen, P. U.

[1,2] Department of Computer Science and Cyber Security, Elizade University, Ilara, Nigeria

[3]Department of Computer Science, Federal University, Otuoke, Nigeria, [4]Department of Computer Science, Dennis Osadebe University, Asaba, Nigeria, [5]Department of Computer Science, School of Computing and Information Technology, Federal University of Technology, Ikot Abasi, Nigeria [6]Department of Computer Sciences, Admiralty University of Nigeria, Ibusa, Nigeria.

Corresponding author's email address: [1]joshua.tom@elizadeuniversity.edu.ng, +234-0803-078-1045, [2]bukola.onyekwelu@elizadeuniversity.edu.ng, [3]nlerumpa@fuotuoke.edu.ng, [4]nwanze.ashioba@dou.edu.ng, [5]abasakpan@futia.edu.ng, [6]piusejodamen@adun.edu.ng

Article Info

***Keywords*:** *Authenticated key exchange, eCK, eSIDH, Perfect forward privacy, Post quantum cryptography, SIDH, SI-Gap Deffie Hellman, SI-Decisional Deffie Hellman, SIKE, Supersingular Elliptic Curve Isogeny.*

Received 25 March 2024
Revised 20 April 2024
Accepted 22 April 2024
Available online 28 April 2024

https://doi.org/10.5281/zenodo.11081039

Abstract

In the past decades, cryptographers tried to validate that a cryptographic universe exists by instantiating its components from concrete computational assumptions. Presently, a large set of public key primitives is built from Deffie Hellman (DH), factorization and lattice-based assumptions. Unfortunately, no corresponding amount of progress is made in building such a large set of crypto primitives from quantum cryptosystem derivatives including code based, multi-variate based, or isogeny-based assumptions. This retarded progress is attributed to the quantum-based primitives not being mainstream assumptions yet. This is not good for the security requirement of the future as the DH or factorization assumptions are not post-quantum secure. Additionally, it is unwise to trust one single post-quantum solution given the recent advances in lattices cryptanalysis. Therefore, it is wise to diversify the set of possible post-quantum secure assumptions to build rich crypto primitives. In readiness for a possible cryptographic tsunami in the next couple of years, we propose a post quantum key exchange scheme based on supersingular elliptic curve isogeny known as Quantum Resistant Supersingular Isogeny Key Exchange scheme, which is based on eSIDH. The scheme employs Montgomery and Edward models that allow performing arithmetic operations faster.

1. Introduction

Cryptographic security has the objective of utilizing well-defined hard mathematical problems that are impossible to solve. Such security is provided by current public key cryptography-based cryptosystems such as RSA, ECDH, ECDSA, etc. are current cryptographic systems deployed in higher level and real-world security solutions like Transport Layer Security (TLS) protocol use in secure internet browsing with https, PGP, automatic updates of software using public key digital signatures for the purpose of authentication [1]. These higher-level security applications provide confidentiality, integrity, availability, and nonrepudiation ser-vices to governments and private businesses including the financial sector. The secure services hitherto enjoyed would in no time become elusive due to quantum computing. Many post quantum cryptosystems are developed in readiness for a possible cryptographic tsunami in the next couple of years. Calling what the

cryptography universe looks like, we have the world of minicrypt where the one-way functions exist, cryptomania where the public key encryption exist, and the obfustopia where the indistinguishability obfuscation exist which can be described as a crypto dream world. In the past few decades, cryptographers have attempted to validate the existence of these worlds by instantiating them from concrete computational assumptions. Therefore, these concrete hardness assumptions in some sense act as a crypto atlas for these worlds. In some more details, cryptomania typically consists of many public key primitives and these have been built from many different assumptions. Now the state-of-the-arts look something like this, a very large public key primitive with rich functionalities have been built from Diffie Hellman (DH) assumption, factorization assumption and more recently from lattice-based assumption. Unfortunately, not similar amount of progress has been made in building such a large set of crypto primitives from code based, multivariate based, hash-based, symmetric key quantum resistance or isogeny-based assumptions. This retarded progress can be attributed to the fact that these quantum cryptosystem derivatives are not yet mainstream cryptographic assumptions. This is not a good shade of affair because it is well known that the construction based on the DH or factorization assumptions are not post-quantum secure. In addition, given the recent advances in lattices cryptanalysis, it is perhaps unwise to put all our crypto eggs into one single post-quantum bag. In other words, it is interesting and perhaps important question to diversify the set of possible post-quantum se-cure assumptions from which we can be rich crypto primitives in cryptomania. Among the post-quantum secure assumptions are code-based, lattice-based, multivariate based, symmetric quantum resistance based and isogeny-based assumptions. Code based cryptography relies on the hardness assumption of problems in coding theory such as the syndrome decoding and the learning parity with noise problems. [2] came forward with a code-based post-quantum cryptographic scheme called hybrid universal network-coding cryptosystem that guarantees computational security in networks were using PKE over all network links is not possible. Instead, the scheme sufficiently encrypts a single selected link and by so doing ensures a desirable computational security over all paths with appreciable information rate in the network. [3] contributed in the understanding of code-based cryptography by carrying out a survey on the most recent development in this area. Based on their work, publications by most researches in this area showed that code-based cryptography is mainly adopted in developing encryption schemes, signature schemes, and identification schemes. The work of [4] goes to confirm the application direction of the code-based quantum cryptographic approach. In a comparison of post quantum cryptographic algorithms, the authors confirmed their position in [3] by showing that code-based cryptography has usefulness in encryption/decryption and digital signatures.

Hash-based cryptography takes its security assurance from the assumption of irreversibility of hash functions. This security assurance characterizes hash functions as one-way functions, collision resistant, and second pre-image attacks. Based on these properties, hash-based cryptography is a promising candidate for providing post quantum cryptographic security. Most researches on hash-based cryptography reveal that the approach is principally, deployed in signature schemes. [5] presented a classification and discussion on the different hash-based signature solutions. The authors' discussed on the advance made in the area of hash-based signatures, which aims to analyze the different hash-based signature categories including possible direction for development of hash-based signatures. In [4], hash-based cryptography is shown to be mainly applicable in the design of digital signature schemes. [6] showed the strategic role of hash functions in signatures by investigating the application of hash-based signatures in IoT devices security in post quantum era. According to the authors, the appropriateness of the selection was based on the constraints of design and optimization requirements of the scheme. Another signature scheme named chameleon signature scheme was proposed in [7]. This hash-based quantum-resistant scheme is designed as an alternative to number theoretic methods including the one presented by Krawczyk and Rabin. Lattice-based cryptography is perhaps the most studied post quantum cryptographic approach. The security of lattice-based post quantum schemes is premised on some fundamentally hard lattice

problems namely, shortest vector problem (SVP), closest vector problem (CVP), short integer solution problem (SIS), and learning with errors (LWE). Research works in this area show that lattice-based cryptography is used to implement encryption/decryption algorithms, signature algorithms, and key exchange schemes [4]. However, this post-quantum cryptography approach is supposedly bedeviled by brute force attack, meet-in-middle attack, lattice reduction attack, and chosen cipher text attack. [8] clarified that though these attacks have been used in security evaluation of the lattice-based cryptosystems, the results have not been satisfactory as the evaluations were based on too simple assumptions. This either overestimates or underestimates the security of lattice-based schemes, hence current estimates in terms of security are not dependable and are unclear. To solve this puzzle, the author based his improved runtime analysis of the attacks on more concrete assumptions and further evaluated the security against the attacks for the lattice-based schemes. His result validated the fact of the overestimation or underestimation of lattice-based schemes e.g. NTRU, BLISS, etc. This concern is actually our main motivation to adopting isogeny-based approach for designing a key exchange scheme in this paper. The other motivating factor to adoption of isogeny-based cryptography in this work is that supersingular elliptic curve isogeny is existentially suitable for a key exchange scheme. [9] made the first effort in the search for a scheme to replace the quantum-vulnerable Diffie Hellman key exchange (DHKE) protocol in 2011. The duo came up with a quantum-resistant key exchange protocol named supersingular isogeny Diffie Hellman (SIDH) whose security is based on the mathematical hardness problem of finding isogenies between supersingular elliptic curves as opposed to the hardness of solving the (ordinary) elliptic curve discrete logarithm, which formed the basis of security for the traditional DH.

Our Contribution:

As our contribution, we proposed an authenticated key exchange algorithm based on eSIDH that is secure against quantum cryptanalysis in the enhanced Canetti-Krawczyk (eCK) security model with perfect forward security against active adversary under the gap Diffie-Hellman (GDH) assumption [10]. We explore ways of ensuring that a select curve has unknown endomorphism ring or computing the isogeny between any two supersingular curves is exponentially difficult. Our scheme is based on eSIDH to ensure that the two factors that fans the embers of breaking SIDH are to the best our knowledge discouraged. The common attack on isogeny-based schemes is powered by known endomorphism ring of the supersingular elliptic curve. Therefore, if knowledge of the endomorphism ring is made public, it becomes a common tool to attack this class of schemes. Obviously, we incorporate generating a SECUER in our scheme as solution to combat this at-tack and encourages use of a curve whose endomorphism ring is unknown. Random curves have unknown endomorphism. Curves with known endomorphism create potentials for backdoor. To solve the problem of SIDH's vulnerability due to knowledge of the endomorphism ring, we instantiate our scheme with SECUER. Other schemes which have used SECUER include [11] and [12]. Computing endo-morphism rings has implications for the security of isogeny-based cryptosystems. Systems that we hope to replace quantum deprecated cryptosystems are based on supersingular elliptic curves believed to be exponentially hard to compute isogenies between them. Finding isogenies between two supersingular elliptic curves is equivalent to calculating endomorphism rings. This is because attackers with knowledge of endomorphism rings can effectively construct isogenies and hence compromise the system.

2.0 Review of Literature

2.1 Related Works

As we approach the realization of quantum computers and algorithms, many researchers have embarked on a search for replacements for the present cryptographic primitives which have been proven vulnerable to attacks using quantum computers and quantum related algorithms e.g. Shor's and Grover's algorithms. The present cryptosystem primitives such as AES, RSA, Elgamal, ECDH, and ECDSA are dependent on the hardness of the factorization problem, discrete logarithm problem,

and ECDLP. With the hardness of these problems, higher-level applications using these primitives such as SSL, TLS, https, PGP etc., are secure. However, with the power of the quantum computer, this mathematical hardness has been broken hence the search for replacements. Among the secure post quantum cryptosystems (PQC) are the lattice based, code-based, multivariate based, isogeny based, symmetric key quantum resistance, and hash-based cryptography. Researchers have designed PQC systems using the above mention quantum attack resistant cryptographic systems. The state of the arts applications of this post quantum crypto is categorized into those deployed in encryption/decryption, digital signature, authentication, and key exchange or key establishment. In this paper, we carry out a systematic literature review to cover some of the researches carried out by authors in these directions. To offer a general understanding of the hard mathematical problems that forms the basis of a PQC capable of addressing the looming quantum-based threats, [13] assessed the existing researches done in this area with the view to identifying any research gaps for future works in pursuant of the readiness for a PQC life. Their assessment highlighted six categories of anti-quantum mathematical problems on which the PQC cryptosystems could be based including lattice based, code-based, multivariate based, isogeny based, symmetric key quantum resistance, and hash based. [14] did a more detailed work by analyzing all the existing cryptosystem primitives (RSA, AES, Elgamal, DH, ECDH, and ECDSA, to ascertain their individual vulnerabilities to quantum hacking based on their respective underlying mathematical problems. The paper mathematically expounded six advanced hard mathematical problems, viz., lattice based, code-based, multivariate based, isogeny based, symmetric key quantum resistance, and hash-based problems that form the basis of security against the power of quantum computers and algorithms in the post quantum era. The mathematical analysis of the six anti-quantum hard problems provides a high-level confidence in the security promised for the post quantum era to replace today's cryptographic primitives in future security applications. Now, we look at research works focusing attention on key exchange application specific deployment of the supersingular elliptic curve isogeny. Supersingular isogeny based key exchange is a Diffie Hellman (DH) variant designed in the wake of the traditional DHKE's vulnerability to quantum attacks. [15] proposed two key exchange protocols based on supersingular isogenies characterized as one-round DH-type authenticated key exchange (AKE). The authors deployed the CK and the CK+ models of security to proof the security of their proposed protocols. In the CK model, the first protocol is secure against an attacker with quantum capabilities under the supersingular isogeny variant based on the decisional DH assumption, which is to ensure indistinguishability security of the shared keys. The second protocol is secure in the CK+ model given an attacker equipped with classical computing resources under the supersingular isogeny variant based on the gap DH assumption. Having a simple one-round DH structure, both protocols are efficient and applicable practically. However, both protocols only provide limited security in the face of an attack. For example, they only provide wPFS and are not capable of total PFS. Aiming to find a new way to design a provably secure AKE based on supersingular isogeny, [16] presented two supersingular isogeny-based AKEs that used a double-key PKE, and prove their security in the CK+ model. The contributions of the work in Xu et al.'s paper is viewed in three proposals. Firstly, the paper proposed a PKE (2-PKE) secure against OW-CCA based on the supersingular isogeny decisional Diffie Hellman (SIDDH) assumption. Secondly, they proposed a two-round AKE namely SIAKE_2, based on the SIDDH assumption by using the modified Fujisaki-Okamoto transformation on KEM as a primitive to obtain a SIDH-based KEM protocol that is secure against OW-CCA and OW-CPA. Thirdly, they modified the primitive to be secure against the 1-oracle SIDH assumption and used it to propose a three-round AKE called SIAKE_3 and proved that both SIAKE_2 and SIAKE_3 are CK+ secure in the random oracle. Their schemes compete favorably with existing isogeny-based AKEs.

Originally, [9] was the first to introduce the SIDH key exchange protocol in 2011. Thereafter, the many security researchers have developed quantum-resistant cryptographic schemes based on SIDH, which has produced SIKE, one of the candidate schemes that has pass the second round of

the NIST post-quantum standardization project. [17] proposed a variant of the SIDH key exchange protocol tagged, extended SIDH (eSIDH). An elliptic curve can be viewed as two separate curves symmetric along the x-axis. Given that, isogenies map a point on one side of the curve onto a corresponding point on the other side of the curve, supersingular curves used in SIDH are primarily defined over a finite field, $\mathbb{F}_{p^2}$, where p is a very large prime number expressed as $p = 4^{e_A}3^{e_B} - 1$ and e_A and e_B are positive integers such that 4^{e_A} and 3^{e_B} are asymptotically equal, i.e. $4^{e_A} \approx 3^{e_B}$. Whereas the traditional SIDH makes use of primes as described above, eSIDH uses primes of the form $p = 4^{e_A}\ell_B^{e_B}\ell_C^{e_C}f - 1$, where ℓ_B and ℓ_C are small prime numbers; f a cofactor; and e_A, e_B and e_C are positive such that $4^{e_A} \approx \ell_B^{e_B}\ell_C^{e_C}$. Therefore, there is a reasonable speed gain due to parallelism from the replacement of 3^{e_B} in the traditional SIDH with $\ell_B^{e_B}\ell_C^{e_C}$. To harness the parallelism opportunity, the paper carried out a multicore implementation of SIKE and SIDH by presenting a design for an eSIDH instantiation that enable parallel computation of its scalar multiplication operations. The paper recommended an expanded search for more efficient eSIDH primes that will satisfy all the security levels as stated in [18]. The knowledge of the endomorphism ring of a supersingular elliptic curve gives impetus to the attack on SIDH. Based on this, to find a solution to the SIDH vulnerability, [12] analyzed the practicability of a protocol for generating a supersingular elliptic curve with unknown endomorphism ring and provided a statistical proof of zero knowledge of the isogeny. The work achieved zero isogeny knowledge by generating a chain of secret random walks on the supersingular ℓ-isogeny graph such that given two curves E_1 and E_2, either party in communication can prove that they know an isogeny with revealing it.

In designing a key exchange scheme, it is important to determine the desired expectations of the design of the security protocol use in insecure wireless networks. To do this, a distinction between the sufficiency of secure security mechanisms is needed, not forgetting device limitations and what is known to be necessary for a key exchange scheme [19]. An important requirement for a key exchange scheme is a secure one-way hash function such that given a set of input it is easy to obtain a corresponding output but computationally impossible to obtain the original in-put given the output. A key exchange system should be secure against man-in-the-middle (MitM) attack, no eavesdropper must be able to intercept the public key [20]. As a countermeasure against this attack, it is necessary that a key exchange scheme provide a way whereby the two parties mutually authenticate each other satisfying the requirement that the parties in the communication must be distinguishable, from their individual perspectives [21]. This means that the parties in the communication should be able to verify each other's identity creating room for no impersonation of any of the parties in the communication by an adversary [22]. Such a scheme is called Authenticated Key Exchange (AKE), which serves to protect against MitM attack. Another vital requirement of a key ex-change scheme is that the session keys must have perfect forward secrecy (PFS), which stipulates that session keys be changed frequently and automatically such that even if the private key is compromised, the encrypted session data cannot be decrypted.

2.1 Overview of Isogeny-based Cryptography

In the recent past not much attention was given to using the hardness of finding isogenies of elliptic curves in the design of cryptographic systems. Presently, the focus of cryptographic research has been shifted to study and adoption of harder mathematical problems such as isogenies due to the realization of the quantum computer with huge computational capabilities. Isogeny based cryptography promises to resist the huge cryptanalytic powers of the much dreaded futuristic (quantum) computer. The supposed security of the existing cryptographic standards such as RSA, Elgamal, ECDH, ECDSA, etc. is broken by Shor's algorithm [23] solution to the factorization and the discrete logarithm problems in polynomial time and Grover's algorithm cryptanalytic power over AES.

Isogenies: Let $\mathbb{E}_1$ and $\mathbb{E}_2$ be elliptic curves having equal cardinality, viz: #E1 = #E2, and let the curves also have identity elements $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively. Then we describe an isogeny, ϕ as a surjectively mapping $\mathbb{E}_1 \longmapsto \mathbb{E}_1$ if and only if $\phi(\mathcal{O}_1) = \mathcal{O}_2$. The mapping ϕ: $\mathbb{E}_1 \longmapsto \mathbb{E}_1$ also a group homomorphism, i.e. $\forall$P, Q $\in \mathbb{E}_1$: $\phi(P + \mathrm{Q}) = \phi(P) + \phi(\mathrm{Q})$. Two elliptic curves are isogenic if there is an isogeny between them. The isogeny kernel is the set of points on the domain curve which is mapped to the identity element: ker(ϕ) = {P $\in \mathbb{E}_1$ | ϕ(P) $\longmapsto \mathcal{O}_2$}. There is a one-to-one relation between isogenies and their kernels and each isogeny can be calculated from their respective kernels. It is common to a kernel to an isogeny as a data structure in SIDH. Given $\mathbb{E}_1$ as an elliptic curve, for any subgroup H $\subseteq \mathbb{E}_1$ there is a unique (up to isomorphism) elliptic curve $\mathbb{E}_2$ with an associated isogeny ϕ: $\mathbb{E}_1 \longmapsto \mathbb{E}_1$ with ker(ϕ) = H, which is a natural map having an isomorphic image to the quotient of the kernel in the domain, i.e. $\mathbb{E}_2 \cong \mathbb{E}_1/\ker(\phi)$. Parts of the protocol deal with the computation of an isogeny of a certain degree. For the purpose of this paper, the degree of an isogeny is the cardinality of its kernel.

2.2 Quantum-Safe Candidates for Key Exchange

All existing cryptographic systems potentially suffer the risk of extinction due to quantum related attacks. NIST, in response to this quantum instigated threat, rolled out calls for proposals in search of harder mathematical problems whose solution (complexity) would lie on the exponential side, the first standardization move for quantum cryptography [24]. Based on this, many proposals have been submitted the aim of which is to find quantum-resistant versions to existing DH and ECDH key establishment protocols. Two interesting quantum-based scheme in this category are Supersingular Isogeny Deffie Hellman (SIDH) and Supersingular Isogeny Key Encapsulation (SIKE). SIDH is based on the hard problem of computing isogenies between two supersingular elliptic curves.

2.3. The Concept Central to SIDH: Isogeny simply means "equal origin". It is a characteristic of a supersingular elliptic curve. Couveignes first suggested the use of isogenies in cryptography in 1997 and in 2011, [9] made the biggest contribution in the area of using Isogeny in a key encapsulation, which they tagged Supersingular Isogeny Key Encapsulation (SIKE) scheme submitted to NIST PQC Standardization 2017. This property permits mapping a point from one curve to a point on another curve in this family shown in Figure 1. Given two supersingular elliptic curves E_1 and E_2 defined over extension field: $E_1/\mathbb{F}_{p^2}$ and $E_2/\mathbb{F}_{p^2}$, where p is a large prime, there is an isogeny ϕ: $E_1 \longrightarrow E_2$, with a smooth degree ℓ that maps E_1 to E_2. Now, we formulate the Supersingular Isogeny

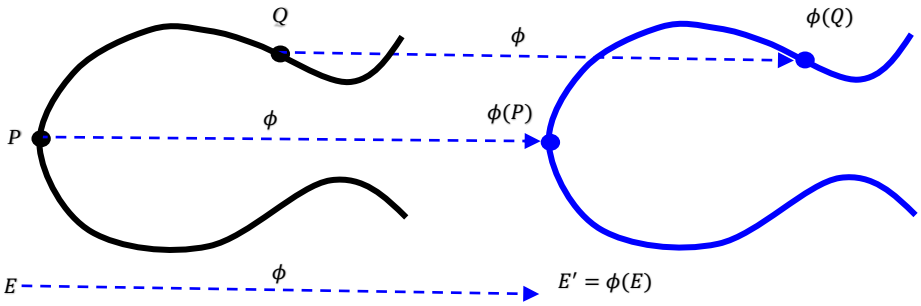

Figure 1: Post Quantum Isogeny-based Cryptography

problem as follows: given $P, \mathrm{Q} \in E_1$ and $\phi(P), \phi(Q) \in E_2$, find the secret isogeny map ϕ. The main attraction to supersingular elliptic curve isogeny-based scheme like SIDH is its small public/private key size.

Further understanding of this is by considering isogenies walks illustrated in Figure 2. Alice and Bob start with the same point on the curve *E*, and randomly walk away from the starting point of

the curves resulting in the creation of curve E_A (Alice's curve) with 4-degree isogeny and E_B (Bob's curve) with 3-degree isogeny. The two parties exchange their curves. Alice repeats the random walk again from E_B. Bob repeats his random walk from E_A, and the two eventually meet at a new secret curve, ES, where $A_{10} = B_8$ as indicated in red. If we regard isomorphic groups as being the same, then Alice's and Bob's walk is commutative. This gives rise to a curve known only to both Alice and Bob, and which represents the new key, because no third party knows this curve, except information about Alice's and Bob's random walk is known. Worthy of note is that isomorphic curves have equivalent j-invariant, i.e. in a closed algebraic field, if the j-invariants, $j(E_1) = j(E_2)$, then the curves E_1 and E_2 are said to be isomorphic.

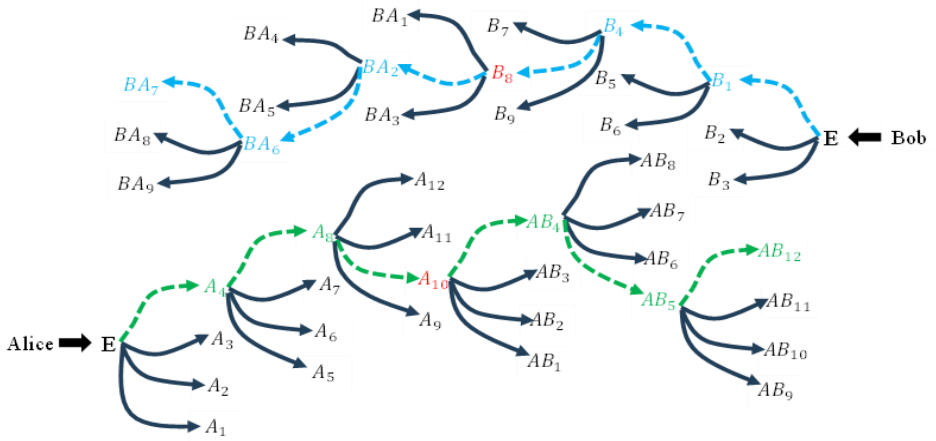

Figure 2: Isogeny Walks from Different Degree Isogenies

2.4 The SIDH Protocol Analysis

Alice and Bob wish to communicate with each other but they first need to exchange keys for a secure communication. One of the post Quantum approaches to ensuring secure key exchange is using a Supersingular Isogeny Diffie Hellman (SIDH). The basic setup for SIDH is as follows: Alice and Bob agree on a common supersingular elliptic curve E of Abelian variety. Alice then chooses a secret subgroup A ⊆ E, quotients out the image of A bordered by B and sends the resulting group, E/A to Bob. Bob chooses a secret subgroup B ⊆ E, quotients out the image of B bordered by A and sends the resulting group, E/B to Alice. Both Alice and Bob can now individually compute the common secret $(E/B)/A \cong E/(A+B) \cong (E/A)/B$ as shown in Figure 3. Now, the idea is that both of them have the same group maybe with the origin of group E. However, believing that A and B chosen by Alice and Bob are both subgroups of E is mathematically ambiguous.

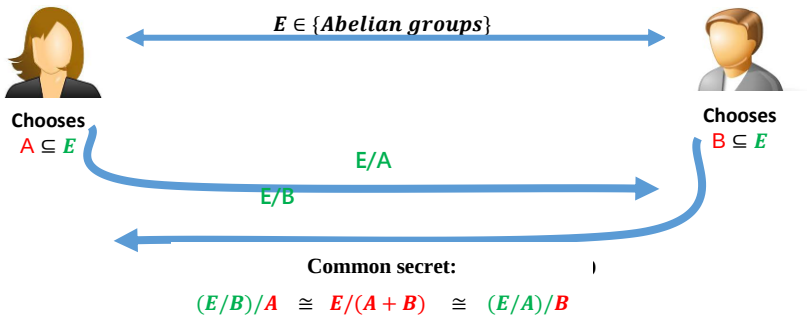

Figure 3: SIDH

Therefore, to make $(E/B)/A \cong (E/A)/B$ precise, we have to say how A should be used as a

subgroup of E by providing a quotient map φ_A from A to E/A and φ_B from B to E/B such that Figure 3 now becomes as shown in figure 4. The quotient maps show how E is map to the images of the subgroups chosen by Alice and Bob.

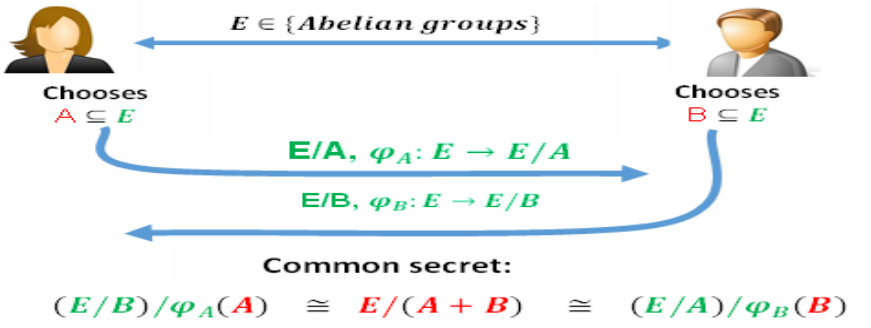

Figure 4: An Improve SIDH Setup with Quotient Maps to specify the mapping of E to the Images of the Subgroups

The specification of $\varphi_A: E \to E/A$ and $\varphi_B: E \to E/B$ turns around to constitute a problem as it reveals the kernels, Ker φ_A and Ker φ_B of A and B respectively. This is, in part, because E is a supersingular elliptic curve with a known endomorphism ring. A trick to get around this is the source of introducing auxiliary points. Figure 5 shows the protocol with the quotient maps of auxiliary points exchanged.

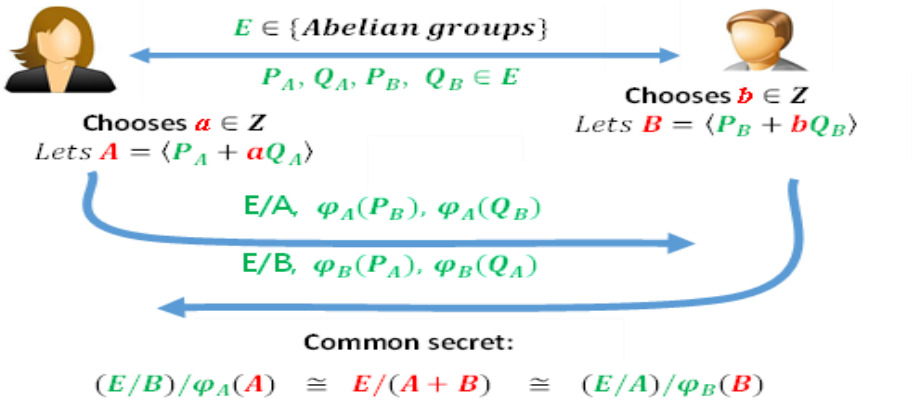

Figure 5: SIDH with the quotient maps of auxiliary points exchanged

Alice chooses two auxiliary points $\boldsymbol{P_A}$ and $\boldsymbol{Q_A}$ from the subgroup A generated from E and Bob does the same by choosing $\boldsymbol{P_B}$ and $\boldsymbol{Q_B}$ from the subgroup B generated from E such that $\boldsymbol{P_A, Q_A, P_B, Q_B} \in \boldsymbol{E}$. Alice chooses a secret a $\in \mathbf{Z}$ computes A using her auxiliary points to get $\boldsymbol{A = \langle P_A + aQ_A \rangle}$. Likewise, Bob chooses a secret b $\in \mathbf{Z}$ computes B using his auxiliary points to get $\boldsymbol{B = \langle P_B + bQ_B \rangle}$. Now, instead of giving the image of her quotient map of A, $\boldsymbol{\varphi_A: E \to E/A}$ Alice only sends the images of the quotient maps $\boldsymbol{\varphi_A(P_B)}$ and $\boldsymbol{\varphi_A(Q_B)}$ of Bob's auxiliary points $\boldsymbol{P_B}$ and $\boldsymbol{Q_B}$ to Bob. Bob does the same by sending the images of the quotient maps $\boldsymbol{\varphi_B(P_A)}$ and $\boldsymbol{\varphi_B(Q_A)}$ of Alice's auxiliary points $\boldsymbol{P_A}$ and $\boldsymbol{Q_A}$ to Alice. This setup enables Alice's map A and Bob's map B generated from E to be secret. Now, since having possession of the quotient maps of each other's auxiliary points, using Bob's quotient map $\boldsymbol{\varphi_B}$, Alice can compute $\boldsymbol{\varphi_B(A)} = \boldsymbol{\varphi_B(\langle P_A + aQ_A \rangle)}$ resulting in $\boldsymbol{\langle \varphi_B(P_A) + a\varphi_B(Q_A) \rangle}$ and Bob can use Alice's quotient map $\boldsymbol{\varphi_A}$ to compute $\boldsymbol{\varphi_A(B)} = \boldsymbol{\varphi_A(\langle P_B + bQ_B \rangle)}$ resulting in $\boldsymbol{\langle \varphi_B(P_A) + b\varphi_B(Q_A) \rangle}$. To make things complete, we take a look at a simplified version of SIDH as concretely proposed by [9]. Let E: $\boldsymbol{y^2 = x^3 + x}$ be an element of supersingular curves over the finite field $\mathbb{F}_{p^2}$. Let $\boldsymbol{E[2^e]}$ torsion points encountered along the way

in E be $\langle P_A, Q_A \rangle$, 3^f torsion points encountered along the way in E be $\langle P_B, Q_B \rangle$ and let $p = 2^e 3^f - 1$ be the chosen prime (just a technical assumption). The auxiliary points of Alice form the 2^e torsion and the auxiliary points of Bob forms the 3^f torsion. This ensures that torsion is defined over $\mathbb{F}_{p^2}$. Alice chooses a $\in Z$ and builds a secret subgroup A = $\langle P_A + aQ_A \rangle \subseteq E[2^e]$. She then quotients out the subgroup A by computing $\varphi_A: E \to E/A$ as a composition of 2-isogenies and sends E/A and the quotient maps of Bob's auxiliary points $\varphi_A(P_B)$ and $\varphi_A(Q_B)$ to Bob. On the other side, Bob chooses b $\in Z$ and builds a secret subgroup B = $\langle P_B + bQ_B \rangle \subseteq E[3^f]$. Bob quotients out the subgroup B by computing $\varphi_B: E \to E/B$ as a composition of 3-isogenies and sends E/B and the quotient maps of Alice's auxiliary points $\varphi_B(P_A)$ and $\varphi_B(Q_A)$ to Alice as shown in figure 6.

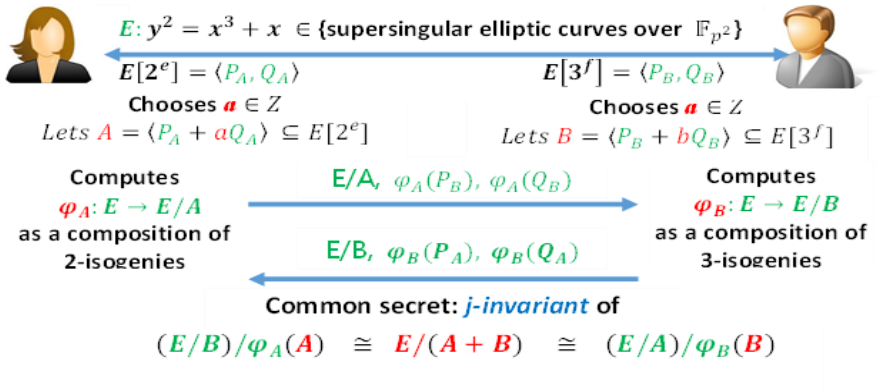

Figure 6: SIDH Concrete Proposal with prime, $p = 2^e 3^f - 1$, [9][22]

2.4 SIDH and Ordinary Diffie Hellman Protocol

If Alice and Bob wish to exchange keys (shared secret) in a channel eavesdropped by an attacker, the key exchange protocol makes use of a cyclic group G, with a generator, g ∈ G as a public parameter. Alice chooses a secret, a and Bob chooses a secret, b where a, b ∈ G and each of them determines ga and gb respectively. the computed values are exchanged over the insecure channel. On receipt of gb from Bob, Alice computes $(g^b)^a$. Likewise, Bob also computes $(g^a)^b$. This is depicted in figure 7.

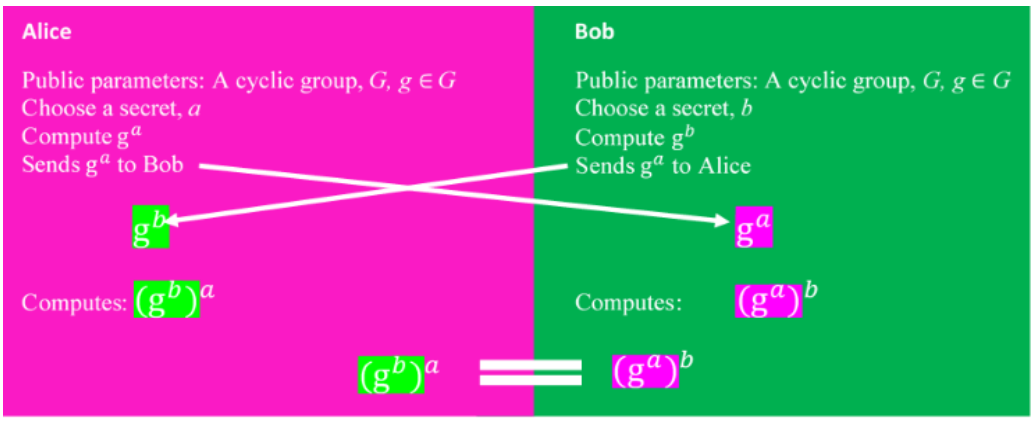

Figure 7: A Schematic of the Traditional Diffie Hellman Protocol

A replacement for this version of DH protocol is overdue to maintain security of cryptosystems based on it. To achieve this, we need a structure, which can pose a more complex problem that a quantum computer cannot find solution in polynomial time. A supersingular isogeny-based approach offers this level of security as it is based on the problem of finding isogenies between elliptic curves, which beats both classical and quantum-based cryptanalysis. Using a supersingular

isogeny to build a DH-like protocol is realized in SIDH, a scheme that uses a supersingular isogeny class as shown in figure 8.

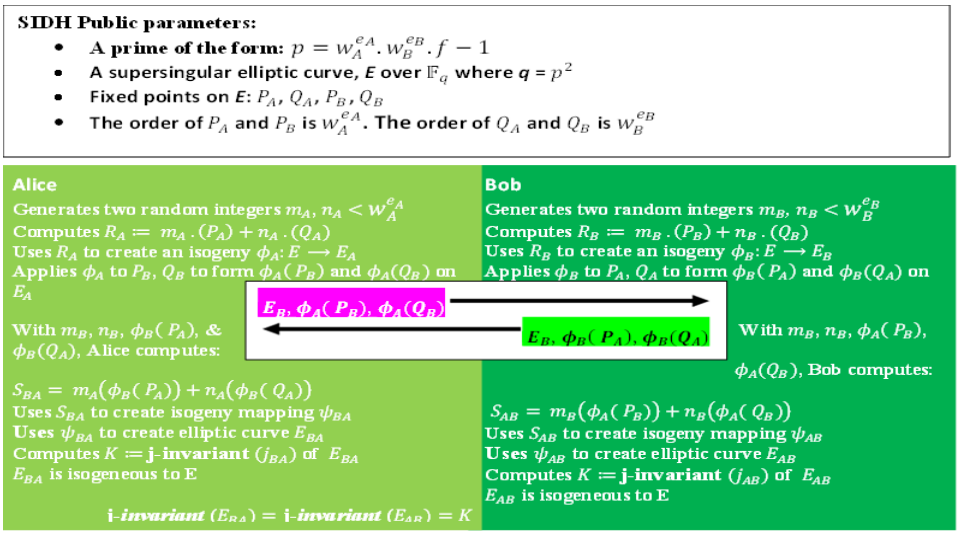

Figure 8: SIDH key exchange protocol between parties Alice and Bob

In the protocol, Alice and Bob create respective isogenies using the same elliptic curve, *E* by creating random points that represent the kernel of their isogeny. This random point R_A (or R_B) a random linear combination of the points (P_A, Q_A) and (P_B, Q_B). Using R (or R_B), Alice and Bob can use Velu's formulas to compute the isogenies $\boldsymbol{\phi}_A$ and $\boldsymbol{\phi}_B$ respectively. To ensure that the isogenies created are different and non-commutative, parties A and B select different pairs of points. Parties A and B then use Velu's formulas for creating isogenies $\boldsymbol{\phi}_A$ and $\boldsymbol{\phi}_B$ respectively using the random points in the kernel. Next, the image of (P_A, Q_A) or (P_B,Q_B) are calculated using the $\boldsymbol{\phi}_B$ and $\boldsymbol{\phi}_A$ isogenies respectively resulting in A and B having two pairs of points $\boldsymbol{\phi}_B(P_A)$, $\boldsymbol{\phi}_B(Q_A)$, and $\boldsymbol{\phi}_A(P_B)$, $\boldsymbol{\phi}_A(Q_B)$ respectively. A and B now exchange these pairs of points over a communications channel. The pair of points received by each party forms the basis for the kernel of a new isogeny together with the same linear coefficients used before. They each compute points S_{BA} and S_{AB} and use Velu's formulas to construct new isogenies.

3.0 Methodology

The proposed scheme first determines whether a given elliptic curve E is supersingular by verifying that the cardinality of E over finite field $\mathbb{F}_q$ is such that $\#\boldsymbol{E}(\mathbb{F}_q) \equiv \mathbf{1}\ (\boldsymbol{mod\ p})$ using the Schoof–Elkies–Atkin (SEA) algorithm where $\boldsymbol{q = p^2}$. This identification process is necessary to avoid the use of elliptic curves that are non-supersingular, as determining non-supersingular elliptic curves isogenies is nontrivial. We are not perturbed by the algorithm's polynomial-time complexity nature. Our scheme, QRSI-AKE is based on eSIDH with characteristic security against MitM attack and side channel attack. Additionally, our (eSIDH)-based key exchange scheme employs the hard computational assumption behind the Supersingular Isogeny Diffie-Hellman (SIDH) to establish a shared secret key between two parties. eSIDH works over a class of particular pairs of elliptic curves called Montgomery curves. The security of eSIDH relies on the hardness of finding the isogeny between two Montgomery curves in polynomial time. eSIDH is a promising alternative to SIDH as it offers faster key computation, reduced key sizes, and resistance to quantum attacks**.**

3.1 Proposed Protocol Description

The proposed protocol is based on the eSIDH protocol hence it operates on supersingular elliptic curves defined over finite field, $\mathbb{F}_{p^2}$ where $\boldsymbol{p}$ is a prime of the form $\boldsymbol{p = 4^{e_A}\ell_B^{e_B}\ell_C^{e_C}f - 1}$. The protocol consists of two phases: the key generation and the key agreement phases. We choose the exponents $\boldsymbol{e_A}$, $\boldsymbol{e_B}$, and $\boldsymbol{e_C}$ such that $\boldsymbol{4^{e_A} \approx \ell_B^{e_B}\ell_C^{e_C}}$. Alice is responsible to compute degree-$\boldsymbol{4^{e_A}}$ isogenies and Bob is responsible to compute degree-$\boldsymbol{\ell_B^{e_B}\ell_C^{e_C}}$ isogenies. Leveraging on eSIDH's inherent parallelism, Bob calculates two secret points $\boldsymbol{r_B = \ell_B^{e_B}}$ and $\boldsymbol{r_C = \ell_C^{e_C}}$ in parallel using two pairs of point $\langle \boldsymbol{P_B, Q_B} \rangle$ representing $\boldsymbol{r_B}$ and $\langle \boldsymbol{P_C, Q_C} \rangle$ representing $\boldsymbol{r_C}$ given as

$$R_B = P_B + [m_B]Q_B \text{ and } R_C = P_C + [m_C]Q_C \quad (1)$$

where $\boldsymbol{R_B}$ and $\boldsymbol{R_C}$ are Bob's secret points, $\langle \boldsymbol{P_B, Q_B} \rangle$ and $\langle \boldsymbol{P_C, Q_C} \rangle$ are points on the supersingular elliptic curve and $\boldsymbol{m_B} \in [\boldsymbol{1, r_B - 1}]$ and $\boldsymbol{m_C} \in [\boldsymbol{1, r_C - 1}]$ are integers randomly chosen by Bob.

Assumptions: The security of our model is established under the isogeny adaptations of the decisional Diffie–Hellman (SI DDH) assumption and gap Diffie–Hellman assumptions [15]. This work considers two types of Supersingular Isogeny Gap Diffie–Hellman (SI GDH) problems namely degree-sensitive SI-GDH (ds-GDH) and degree-insensitive SI-GDH (di-GDH).

Definition 1: Supersingular Isogeny Decisional Diffie–Hellman (SI DDH) Assumption Let $\aleph$ be a quantum computer adversary. For $\mathrm{pk}^{\mathrm{sidh}} = \big(\mathfrak{g} = (E;\ P_A, Q_A, P_B, Q_B), \mathfrak{e} = (\ell_A, \ell_B, e_B, e_B)\big) \leftarrow_R Gen^{sidh}(1^\lambda)$ and $\mathfrak{a}, \mathfrak{r} \in_R SK_A, \mathfrak{b}, \mathfrak{s} \in_R SK_B$, $\aleph$ receives χ_b for $b \in_R \{0,1\}$, that is defined by $\chi_0 = \big(\mathrm{pk}^{\mathrm{sidh}}, \mathfrak{g}^{\mathfrak{a}}, \mathfrak{g}^{\mathfrak{b}}, (\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}}\big)$ and $\chi_1 = \big(\mathrm{pk}^{\mathrm{sidh}}, \mathfrak{g}^{\mathfrak{a}}, \mathfrak{g}^{\mathfrak{b}}, (\mathfrak{g}^{\mathfrak{r}})^{\mathfrak{s}}\big)$ $\aleph$ outputs a guess bit b'. If $b = b'$, $\aleph$ wins. The advantage of $\aleph$ for the SI DDH problem is thus defined as $\mathbf{Adv}_{\mathfrak{g},\mathfrak{e}}^{\mathrm{SI-DDH}}(\aleph) = \Pr[\aleph \text{ wins}] - 1/2$. The SI-DDH assumption is: For any polynomial-time quantum machine adversary, $\aleph$, the advantage of $\aleph$ for the SI-DDH problem is negligible in parameter λ.

Definition 2: ds- and di-Supersingular Isogeny Gap Decisional Diffie–Hellman Assumptions Let $\aleph$ be a quantum computer adversary. For $\mathrm{pk}^{\mathrm{sidh}} = \big(\mathfrak{g} = (E;\ P_A, Q_A, P_B, Q_B), \mathfrak{e} = (\ell_A, \ell_B, e_B, e_B)\big) \leftarrow_R Gen^{sidh}(1^\lambda)$ and $\mathfrak{a} \in_R SK_A, \mathfrak{b} \in_R SK_B$, $\aleph$ receives and $\aleph$ access SI-DDH oracle for any input $\chi = \mathrm{pk}^{\mathrm{sidh}}, (E'_A;\ P'_{AB}, Q'_{AB}), (E'_B;\ P'_{BA}, Q'_{BA}, \mathfrak{h}')$ where P'_{AB}, Q'_{AB} and P'_{BA}, Q'_{BA} are points in $E'_A(\mathbb{F}_{p^2})$ and $E'_B(\mathbb{F}_{p^2})$ respectively and $\mathfrak{h}' \in \mathbb{F}_{p^2}$, and the outputs $\mathfrak{h} \in \mathbb{F}_{p^2}$. If $\mathfrak{h} = (\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}} (= (\mathfrak{g}^{\mathfrak{b}})^{\mathfrak{a}})$, $\aleph$ wins. Two types of SI-GDH problems are defined here based on the conduct of the SI-DDH oracle.

- degree sensitive SI-GDH (ds-SI-GDH) problem: The ds-SI-DDH oracle answers true if there exist a supersingular elliptic curve E'_{AB} and isogenies $\phi'_A, \phi'_B, \phi'_{AB}, \phi'_{BA}$ among $E, E'_A, E'_B, E,\ E'_{AB}$ which form a commutative diagram as in figure 9 such that
  - (i) degree d'_A of ϕ'_A (and ϕ'_{BA}) is equal to $\ell_A^{e_A}$ and degree d'_B of ϕ'_B (and ϕ'_{AB}) is equal to $\ell_B^{e_B}$ and
  - (ii) $P'_{AB} = \phi'_A(P_B),\ Q'_{AB} = \phi'_A(Q_B)$ and $P'_{BA} = \phi'_B(P_A),\ Q'_{BA} = \phi'_B(Q_A)$ where points (P_A, Q_A, P_B, Q_B) are given in public key $\mathrm{pk}^{\mathrm{sidh}}$, and $\mathfrak{h}' = j(E'_{AB})$ and false otherwise.
- degree insensitive SI-GDH (di-SI-GDH) problem: The di-SI-DDH oracle outputs true if a supersingular elliptic curve E'_{AB} and isogenies $\phi'_A, \phi'_B, \phi'_{AB}, \phi'_{BA}$ exist among $E, E'_A, E'_B, E,\ E'_{AB}$ forming a commutative structure as in figure 9 such that
  - (i) degree d'_A of ϕ'_A (and ϕ'_{BA}) is a power of ℓ_A and degree d'_B of ϕ'_B (and ϕ'_{AB}) is a power of ℓ_B and
  - (ii) $P'_{AB} = \phi'_A(P_B),\ Q'_{AB} = \phi'_A(Q_B)$ and $P'_{BA} = \phi'_B(P_A),\ Q'_{BA} = \phi'_B(Q_A)$ where points (P_A, Q_A, P_B, Q_B) are given in public key $\mathrm{pk}^{\mathrm{sidh}}$, and $\mathfrak{h}' = j(E'_{AB})$ and false otherwise.

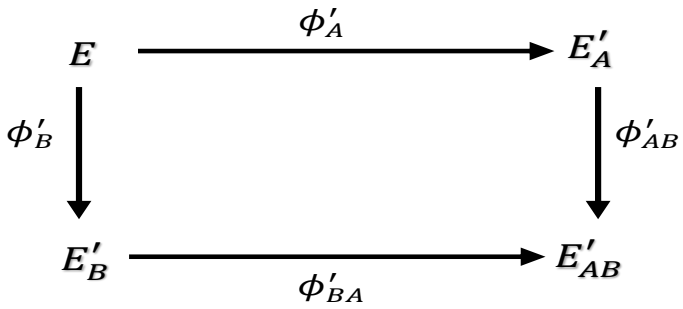

Figure 9: Commutative Diagram with instances of SI-Decisional DH Oracles

In the above, $\boldsymbol{d'_A = \deg(\phi'_A) = \deg(\phi'_{BA})}$ and $\boldsymbol{d'_B = \deg(\phi'_B) = \deg(\phi'_{AB})}$. The advantage of adversary $\aleph$ are defined as $\mathbf{Adv}^{\mathbf{ds-SI-GDH}}_{\mathfrak{g},\mathfrak{e}}(\aleph) = \mathbf{Pr}[\aleph \mathbf{wins}]$ and $\mathbf{Adv}^{\mathbf{di-SI-GDH}}_{\mathfrak{g},\mathfrak{e}}(\aleph) = \mathbf{Pr}[\aleph \mathbf{wins}]$ respectively. The ds-SI-GDH (and di-SI-GDH) assumption is: For any polynomial-time quantum machine adversary, $\aleph$, the advantage of $\aleph$ for the ds-SI-GDH (and di-SI-GDH) problem is negligible in security parameter $\boldsymbol{\lambda}$. The protocol run is as in figure 10.

3.2 Choice of Parameters for Implementation

Since the protocol in this paper is based on eSIDH, we carefully choose the parameters for the prime, $\boldsymbol{p = 4^{e_A}\ell_B^{e_B}\ell_C^{e_C}f - 1}$ used in the proposed protocol. These parameters include $\boldsymbol{e_A, e_B, e_C, \ell_B}$, and $\boldsymbol{\ell_C}$. We adopted the eSIDH primes because they are more flexible and easily accessible than their SIKE counterparts. If the values of $\boldsymbol{\lambda}$ and the small primes $\boldsymbol{\ell_B}$ and $\boldsymbol{\ell_C}$ are fixed where $\boldsymbol{\lambda}$ is given as $\lceil \log_2 p \rceil$, representing the minimum number of words used as an eSIDH prime. By intentionally changing $\boldsymbol{e_B, e_C}$ and f, we are able to search $\frac{N}{2}-$ Montgomery friendly primes helping us to achieve Montgomery reduction as compared to SIKE primes. For computations on Bob's side, we leverage the tradeoff between the sizes of the base primes, $\boldsymbol{\ell_B}$ and $\boldsymbol{\ell_C}$ and the exponents $\boldsymbol{e_B}$ and $\boldsymbol{e_C}$. In isogeny evaluations, the magnitude of the step to be performed is defined by the base primes while the exponents define number of steps that must be performed. Hence, we opted to keep the to keep the base primes large while the exponents are reduced. Based on this consideration, we choose the parameters for the prime, $\boldsymbol{p = 4^{e_A}\ell_B^{e_B}\ell_C^{e_C}f - 1}$ such that $\boldsymbol{2e_A \approx \log_2(\ell_B^{e_B}\ell_C^{e_C})}$. We choose $\boldsymbol{e_A}$ in such a way that the security level offered by SIKE is achieved. The co-factor, f is also selected to ensure that $\boldsymbol{p}$ is a $\frac{N}{2}-$ Montgomery friendly prime.

Therefore, the following prime and values were chosen for our implementation.

Prime chosen: $\boldsymbol{p_{434} = 4^{109}3^{70}5^{45} - 1}$

$\boldsymbol{e_A} = 109$, $\boldsymbol{e_B} = 70$, $\boldsymbol{e_C} = 45$, $\boldsymbol{\ell_B} = 3$, $\boldsymbol{\ell_C} = 5$ and $\boldsymbol{f} = 1$.

3.3 Exploiting eSIDH's Inherent Parallelism

We assume that $\boldsymbol{\lambda = \lceil log_2(p) \rceil}$, referred to in section 3.2, is bit length of the eSIDH prime $\boldsymbol{p = 4^{e_A}\ell_B^{e_B}\ell_C^{e_C}f - 1}$ and for convenience Bob set $\boldsymbol{r_B = \ell_B^{e_B}}$ and $\boldsymbol{r_C = \ell_C^{e_C}}$. Bob has to calculate two secret points by choosing two pairs of points defined as two separate secret points $\langle \boldsymbol{P_B, Q_B} \rangle$ and $\langle \boldsymbol{P_C, Q_C} \rangle$ as stated earlier. Bob sets $\boldsymbol{E[r_B] = \langle P_B, Q_B \rangle}$ and $\boldsymbol{E[r_C] = \langle P_C, Q_C \rangle}$ and randomly chooses two integers $\boldsymbol{m_B \in [1, r_B - 1]}$ and $\boldsymbol{m_C \in [1, r_C - 1]}$ and uses them to compute $\boldsymbol{R_B}$ and $\boldsymbol{R_c}$ according to equation 1. Now, if $\boldsymbol{\ell_B, \ell_C, e_B}$, and $\boldsymbol{e_C}$ are chosen such that $\boldsymbol{\log_2(\ell_B)e_B \approx \log_2(\ell_C)e_C}$ then the cost of calculating $\boldsymbol{R_B}$ is about $\frac{\boldsymbol{2\lambda}}{\boldsymbol{4}}$ xDBL. It should be noted that this cost is almost the same cost needed to calculate $\boldsymbol{R_C}$ and which the combined cost of $\boldsymbol{R_B}$ and $\boldsymbol{R_C}$ is less than the cost of calculating Alice's $\boldsymbol{R_A}$ using the optimal strategy [17]. This signifies a performance gain due to the parallel computation implicit in eSIDH because computations of $\boldsymbol{R_B}$ and $\boldsymbol{R_C}$ are mutually exclusive.

Based on this, Bob's secret points $\boldsymbol{R_B}$ and $\boldsymbol{R_C}$ can be computed in parallel using a multicore processor. Furthermore, we can calculate the isogeny $\boldsymbol{\phi_{BC}}$ as $\boldsymbol{\phi_B}\,^{\circ}\boldsymbol{\phi_C}$ without the need for multiplication by $\boldsymbol{r_C}$ as shown in step 4 of Bob's protocol run. This gain in the reduction in computation complexity of the isogeny, $\boldsymbol{\phi_{BC}}$ comes from the fact that $\mathbf{gcd}(\boldsymbol{r_B}, \boldsymbol{r_C}) = \mathbf{1}$ with the order of the points $\boldsymbol{R_B}$, $\boldsymbol{R_C}$ being $\boldsymbol{r_B}$ and $\boldsymbol{r_C}$ respectively. Based on this, $\boldsymbol{R_B}$ and $\boldsymbol{\phi_B}(\boldsymbol{R_C})$ respectively are used to generate the kernels of $\boldsymbol{\phi_B}$ and $\boldsymbol{\phi_C}$. This saving in computation cost is also significant in the key agreement phase where Alice equally have to generate kernels of $\boldsymbol{\phi'_B}$ and $\boldsymbol{\phi'_C}$ using $\boldsymbol{R'_B}$ and $\boldsymbol{\phi'_B}(\boldsymbol{R'_C})$ respectively.

For instance, given the eSIDH prime, $\boldsymbol{p_{434}} = \mathbf{4}^{109}\mathbf{3}^{70}\mathbf{5}^{45} - \mathbf{1}$, Alice must compute $\mathbf{4}^{109}$ while Bob can compute $\mathbf{3}^{70}$ and $\mathbf{5}^{45}$ in parallel on two separate CPU cores. Comparing this to an equivalent prime used in SIKE, $\boldsymbol{p_{434}} = \mathbf{2}^{216}\mathbf{3}^{137} - \mathbf{1}$, one can observe that the base primes are small than in the case of eSIDH prime but the exponents are tremendously larger. Secondly, Bob must compute $\mathbf{3}^{137}$ on a single core and hence does not offer opportunity for leveraging the inherent parallelism in modern CPU technology. The impact of the choice of eSIDH prime over the SIKE prime cannot be overemphasized as there is a significant timing speedup compared to SIKE primes. The noticeable gain performance can be attributable to $\boldsymbol{p_{434}}$ being a Montgomery friendly prime with a faster modular reduction property.

Performance achieved by using multi-core processor is higher than that of a single core at any point in time. We arrived at this piece of knowledge when our scheme implemented with eSIDH- $\boldsymbol{p_{434}} = \mathbf{4}^{109}\mathbf{3}^{70}\mathbf{5}^{45} - \mathbf{1}$ on Intel i5 with quad (4) cores exhibited far better performance than using the SIKE prime, $\boldsymbol{p_{434}} = \mathbf{2}^{216}\mathbf{3}^{137} - \mathbf{1}$ on the same CPU architecture. Interestingly, we notice a performance degradation when a single-core CPU architecture was used. The implementation with the SIKE prime performed better.

In this work, the only practical consideration and potential limitation in exploiting parallelism with respect to implementing the enhanced prime can be explained using Amdahl's Law [25]. Only a fraction of a program, d is parallelizable while the other portion, $(1 - d)$ must be executed completely sequentially. What this means is that no matter the number of processors, the sequential portion of a program will spend same time as it would on a single core system.

3.4 Isogeny Computation on Montgomery Curves

Montgomery curve is the main building block for implementing the eSIDH based key exchange protocol called QRSI-AKE developed in this paper. Assuming K, is a field having characteristic not equal to 2 or 3, we can denote the Montgomery curve or *K* by

$$\boldsymbol{M_{a,b}}: \boldsymbol{by^2} = \boldsymbol{x^3} + \boldsymbol{ax^2} + \boldsymbol{x} \tag{2}$$

with the condition that $\boldsymbol{b}(\boldsymbol{a^2} - \mathbf{4}) \neq \mathbf{0}$. In this paper, we refer to $\boldsymbol{M_{a,b}}$ as $\boldsymbol{M_a}$ when b = 1. For carrying out arithmetic computation on the elliptic curve, we use differential addition and doubling formula and for isogeny computation, we use odd degree isogenies.

In the key generation phase

The public parameters of eSIDH are given by: a supersingular base curve E with basis points $P_A, Q_A, P_B, Q_B, P_C, Q_C \in E_0$ such that $E[r_A] = \langle P_A, Q_A \rangle$, $E[r_B] = \langle P_B, Q_B \rangle$ and $E[r_C] = \langle P_C, Q_C \rangle$

Alice	Bob
1. Generates two random integers m_A , $n_A < (4^{e_A})$	1. Generates two random integers m_B, $m_C < (4^{e_A})$
2. Chooses a point $\langle P_A, Q_A \rangle$ on the curve and computes $R_A = m_A.P_A + n_A.Q_A$	2. Chooses two pairs of points $\langle P_B, Q_B \rangle$ and $\langle P_C, Q_C \rangle$ on the curve and computes $R_B = P_B + m_B.Q_B$ and $R_C = P_C + m_C.Q_C$
3. Uses R_A to create an isogeny mapping $\phi_A: E \to E_A$	3. Uses R_B and R_C to create ϕ_B and ϕ_C isogenies $\phi_B: E \to E_B$ and $\phi_C: E_B \to E_{BC}$ respectively.
4. Chooses another point $\langle P_B, Q_B \rangle$ on the curve and applies ϕ_A to $\langle P_B, Q_B \rangle$ to form E_A: $\phi_A(P_B)$ and $\phi_A(Q_B)$	4. Combines the ϕ_B and ϕ_C isogenies using the CRT: $\phi_{BC} = \phi_B \circ \phi_C$ where the kernel of ϕ_B is generated by R_B and the kernel of ϕ_C is generated by $\phi_B(R_C)$
5. Sends $\boldsymbol{\phi_A(P_B), \phi_A(Q_B)}$ to Bob	5. Redefines his public points as $S = P_B + P_C$ and $T = Q_B + Q_C$
	6. Sends $\boldsymbol{\phi_{BC}}$, S, T, $\boldsymbol{m_B, m_C, r_B, r_C}$ to Alice

In the key Agreement phase

Alice	Bob
6. Uses m_A, n_A, $\boldsymbol{\phi_{BC}}$, S, T, $\boldsymbol{m_B, m_C, r_B, r_C}$ to compute $R_B^{'} = r_C(\boldsymbol{\phi_A(S)}) + m_B(\boldsymbol{\phi_A(T)})$ $R_C^{'} = r_B(\boldsymbol{\phi_A(S)}) + m_C(\boldsymbol{\phi_A(T)})$	7. Uses m_B, m_C, $\boldsymbol{\phi_A(P_B), \phi_A(Q_B)}$ to compute $R_A^{'} = m_B(\boldsymbol{\phi_{BC}(P_A)}) + m_C(\boldsymbol{\phi_{BC}(Q_A)})$
7. Uses $R_B^{'}$ and $R_C^{'}$ to create isogeny mappings $\boldsymbol{\phi}_B^{'}: E_A \to E_{AB}$ and $\boldsymbol{\phi}_C^{'}: E_{AB} \to E_{ABC}$ respectively	8. Uses $R_A^{'}$ to create isogeny mapping $\boldsymbol{\phi}_A^{'}: E_{BC} \to E_{BCA}$
8. Combines the $\boldsymbol{\phi}_B^{'}$ and $\boldsymbol{\phi}_C^{'}$ isogenies to $\boldsymbol{\phi}_{BC}^{'}$ using the CRT	7. Uses $\boldsymbol{\phi}_A^{'}$ to create an elliptic curve E_{BCA} isogenous to E
9. Uses $\boldsymbol{\phi}_{BC}^{'}$ to create an elliptic curve E_{ABC} isogenous to E	10. Computes $K =$ j-invariant (j_{BCA}) of the curve E_{BCA}
10. Computes $K =$ j-invariant (j_{ABC}) of the curve E_{ABC}	

j-invariant (j_{ABC}) of the curve E_{ABC} is equal to j-invariant (j_{BCA}) of the curve E_{BCA}
Hence Alice and Bob have established a common secret session key, K

Figure 10: QRSI-AKE Protocol Run

3.5. Computations on the Montgomery Elliptic Curve

Point Addition and Point Doubling: Assuming $\boldsymbol{P}$ and $\boldsymbol{Q}$ are points on the Montgomery curve, $\boldsymbol{M_a}$ with coordinates $(\boldsymbol{x_P}, \boldsymbol{y_P})$ and $(\boldsymbol{x_Q}, \boldsymbol{y_Q})$ where $\boldsymbol{x_P \neq x_Q}$ and $\boldsymbol{P - Q}$ is given as $\boldsymbol{x_{P-Q}}, \boldsymbol{y_{P-Q}}$, then we compute the $\boldsymbol{x}$ coordinates of the sum of the two points, $\boldsymbol{P + Q}$ and the doubling of $\boldsymbol{P}$, $\boldsymbol{x_{[2]P}}$ as follows:

$$x_{P+Q} = \frac{\left(x_P x_Q - 1\right)^2}{\left(x_{P-Q}\left(x_P - x_Q\right)^2\right)} \tag{3}$$

$$x_{[2]P} = \frac{(x_P^2 - 1)^2}{\left(4x_P(x_P^2 + ax_P + 1)\right)} \tag{4}$$

Computing the odd degree isogenies on Montgomery curves:

Assuming $\boldsymbol{P} = (\boldsymbol{x_1}, \boldsymbol{y_1})$ is a point on the Montgomery curve, $\boldsymbol{M_a}$ having order $\boldsymbol{\ell} = \boldsymbol{2d} + \boldsymbol{1}$ and $(\boldsymbol{x_1}, \boldsymbol{y_1}) = [\boldsymbol{i}]\boldsymbol{P}$, then we can compute $\boldsymbol{\ell}$-isogeny, $\boldsymbol{\phi}$ from $\boldsymbol{M_a}$ to $\boldsymbol{M_{a'}}$ =$\boldsymbol{M_a}/\langle \boldsymbol{P} \rangle$ as follows:

$$\boldsymbol{\phi}: (\boldsymbol{x}, \boldsymbol{y}) \rightarrow (\boldsymbol{f}(\boldsymbol{x}), \boldsymbol{y} \cdot \boldsymbol{f}'(\boldsymbol{x})) \tag{5}$$

where**,**

$$\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{x} \cdot \prod_{\boldsymbol{i}=\boldsymbol{1}}^{\boldsymbol{d}} \left(\frac{\boldsymbol{x}\boldsymbol{x_i} - \boldsymbol{1}}{\boldsymbol{x} - \boldsymbol{x_i}} \right)^{\boldsymbol{2}}$$

4.0 Security Analysis

The key exchange scheme based on eSIDH appears to be a promising alternative to traditional key exchange algorithms such as Diffie-Hellman (DH) and elliptic curve cryptography (ECC) in the face of the impending quantum computer technology in the next couple of years. The security of eSIDH relies on the intractability of the supersingular isogeny problem, which provides a potentially stronger level of security. However, it is important to continue rigorous analysis of the scheme and monitor developments in cryptanalysis. Additionally, the relatively higher computational overhead of eSIDH compared to DH and ECC should be considered when selecting a key exchange algorithm.

4.1 The Extended Canetti-Krawczyk Security Model

The security analysis of the key exchange scheme based on eSIDH considers the eCK. The choice of eCK model is based on the fact that security requirements such as key compromise impersonation (KCI), weak perfect forward secrecy (wPFS) and maximal exposure attacks (MEX) are brought into the eCK model. This security model considers the use of a quantum computer that can solve the ECDLP problem. The scheme developed in this paper is shown to be secure, with the eCK model providing a stronger level of security. These results demonstrate the effectiveness of the use of eSIDH as a secure key exchange protocol even in the presence of quantum computing capabilities. Our motivation is that for an adversary to recover the session key in the eCK model, both the long-term and ephemeral secret keys must be compromise. In this section, we describe the components of the eCK security model.

We assume that there are a set of $\boldsymbol{n}$ parties given by $\mathbf{P} = \{\boldsymbol{P_1}, \ldots, \boldsymbol{P_n}\}$ where $\boldsymbol{i}$ in each party $\boldsymbol{P_i}$ is an element of the set of integers [1,…,n] and each $\boldsymbol{P_i}$ posses a pair of long-term (public and secret) keys denoted as $(\boldsymbol{pk_{P_i}}, \boldsymbol{sk_{P_i}})$. $\boldsymbol{P_i}$ can initiate up to $\boldsymbol{s} \leq \boldsymbol{n}$ concurrent or sequential sessions. We refer to the initiator of a protocol session as owner represented as **P** and the other party as the responder represented as $\boldsymbol{Q}$. The owner sends the first protocol message and any party that responds to the protocol message becomes the responder. A session, $\prod_{\boldsymbol{P,Q}}^{\boldsymbol{s}}$ enters an accepted state when the session key is successfully computed. $\prod_{\boldsymbol{P,Q}}^{\boldsymbol{s}}$ may terminate without assuming the accept state. Let the protocol sessions $\prod_{\boldsymbol{P,Q}}^{\boldsymbol{s}}$ and $\prod_{\boldsymbol{P',Q'}}^{\boldsymbol{s'}}$ be initiated by owner, **P** and the other party earlier called the Responder, $\boldsymbol{Q}$. A legitimate protocol run results from proper setup of **P**'s and $\boldsymbol{Q}$'s sessions. This means that **P** and $\boldsymbol{Q}$ set up their individual sessions represented as $\prod_{\boldsymbol{P,Q}}^{\boldsymbol{s}}$ and $\prod_{\boldsymbol{P',Q'}}^{\boldsymbol{s'}}$ respectively. The two sessions must pass the following requirement to be partners:

(i) They both have computed session keys and the session keys are identical

(ii) All Messages sent from $\prod_{P,Q}^{s}$ and received by $\prod_{P',Q'}^{s'}$ and vice versa must be identical

(iii)The owner is the initiator and the other party is the responder

(iv)When P initiates a protocol run, Q is the responder and vice versa.

4.2 Adversarial Model

Our protocol also assumes certain adversarial capabilities. Let the adversary א be a probabilistic-time polynomial system. א have control of the entire network and is capable of interacting with any initiated protocol sessions in the accepted state. The following specifies the powers ascribed to א.

(i) א can initiate new sessions and either modify or delay messages or capable of both. It can do this by sending query with (P , Q, s, m) as parameters to the session $\prod_{P,Q}^{s}$.

(ii) א can run a query to reveal the session key with (P , Q, s) as parameters in the known session key attack. א obtains the session key of $\prod_{P,Q}^{s}$ the later has accepted and is in possession of a session key.

(iii) א is capable of running a query to reveal all the ephemeral keys as far as the randomness of the session, $\prod_{P,Q}^{s}$.

(iv) א can obtain all the long-term secrets of the initiator or owner P by run the Corrupt query with P as the parameter and use it to setup long-term secrets as P at anytime hence corrupting P. However, this does not reveal any session keys to א.

(v) א can try to determine whether there is a difference between a random key and the session key accepted and held by a session. To do this, it can run the Test query with (P , s) as parameters. Here, the session, $\prod_{P,Q}^{s}$ selects a random bit $b \in \{0,1\}$. If b = 1, the correct session key is delivered to א else a random session key is chosen and sent to א.

4.3 eCK Security Game

Stage 0: Using the security parameter k, the challenger, $\mathcal{C}$ generates keys. stage 1: The adversary, א is executed with the following capabilities Send query, SessionKeyReveal query, EphemeralKeyReveal query, Corrupt queries to any session at will and Test query.

Stage 2: The adversary א chooses a fresh session executes the Test query.

Stage 3: א keeps running Send query, SessionKeyReveal query, EphemeralKeyReveal query, and Corrupt queries with the only constraint that the test session cannot be violated.

Stage 4: At a certain instance, א produces the bit, $b' \in \{0,1\}$ as output by guessing b during test session. If $b = b'$, א wins the security game.

Our protocol is said to be secure in the eCK model if no probabilistic polynomial time (PPT) adversary wins the eCK security game with an advantage given by

$$Adv_{QRSEI-AKE}^{eCK}(\aleph) = |\Pr[b' = b] - 1/2|$$

where $\Pr[b' = b]$ is the probability that the adversary א wins the eCK security game.

4.4 QRSI-AKE Protocol's Resilience Against Attacks

Though SIDH was the first version of a Deffie Hellman-like key exchange scheme based on supersingular isogeny, in this paper we took cognizance of the weakness of SIDH. The protocol developed in this paper is based on eSIDH. We, alongside this, intentionally employ the Montgomery and Edward elliptic curves to provide security against timing attacks. This is because scalar multiplication based on the Montgomery form do not depend on the bit-pattern of the secret key unlike the Weierstrass-form dependent scalar multiplication. We also propose to use Edwards curve since every Edwards curve is birationally equivalent to elliptic curve in Montgomery form. The QRSI-AKE Protocol is also strong against key recovery attack as we leverage the responsibility of one party in the communication, say Alice, to compute degree-$\boldsymbol{4^{e_A}}$ isogenies and the other party, say Bob, to compute degree-$\boldsymbol{\ell_B^{e_B}\ell_C^{e_C}}$ isogenies. based on this, Bob computes two values $\boldsymbol{\ell_B^{e_B}}$ and $\boldsymbol{\ell_C^{e_C}}$ as against one value 3^{e_B} in the large prime, $p = 4^{e_A}3^{e_B}$ as obtainable in the SIDH protocol which is vulnerable to key recovery attack. In addition, the public keys generated indistinguishable from random bitstrings. Notice that Alice's public key sent to Bob is of the form $\boldsymbol{\phi_A(P_B), \phi_A(Q_B)}$ while Bob's public key sent to Alice is of the form $\boldsymbol{\phi_{BC}, S, T, m_B, m_C r_B r_C}$ in figure 10 lines 5 and 6

respectively. This indistinguishability offers the scheme in this paper resilience against offline dictionary attack.

4.5. Discussion

While our intention in this section is not to give a description of a secure cryptosystem based on the traditional DH protocol, it is worthy of note to state that its security depends on the choice of a model for the cyclic group. To the best of our knowledge, the family of groups that can offer a DH based cryptosystem secure against classical attacks is the elliptic curves over finite field $\mathbb{F}$. It is a common knowledge that existing cryptosystem primitives including DH based cryptos will be broken with the arrival of quantum computers. This is because the traditional (ordinary) DH protocol depends on the DLP or the ECDLP for its security, which the quantum computer is capable of solving in polynomial time. Therefore, this paper engaged in finding a quantum safe mathematical problem that can withstand quantum-based cryptanalysis. We explored the various hard mathematical problems resistant to exploitation against a quantum computer including lattices, hashes, codes, isogenies, high entropy-based symmetric key resistance, and multivariate quadratic problems. All these hard problems are capable of surpassing the impending cryptographic nightmare posed by quantum computing although still at the theoretical level. We found that of these quantum resistant primitives, the supersingular elliptic curve isogeny is suitable for purposes of key exchange and key establishment protocol definitions. The traditional Deffie Helman based key exchange protocol will no longer be secured in the face of quantum computers hence a supersingular isogeny-based version of DH protocol for key exchange, SIDH. We explored eSIDH, an extended version of SIDH, which enables the use of primes that are Montgomery friendly. These primes allow for exploiting the parallelism associated with one of the parties' computational requirements and also offer faster field arithmetic due to the parallelism.

6.0 Conclusion

There are many real-world security problems, which cryptographers have provided solutions. These problems all bother on how to protect the desirable properties that make information valuable including confidentiality, integrity, availability and nonrepudiation. The existing solutions to these problems have helped to ensure secure communication over insecure and untrusted channels giving the illusion of a more trusted world. One requirement of secure communication is secure key exchange, which classically is provided by schemes such as ECDH key exchange. With the promising computational power of quantum computers, all key exchange based on schemes with DLP, integer factorization problem, and ECDLP problem will fail cryptanalysis test with quantum computers hence the rush to migrate to more robust methods soon. SIDH based key exchange is the quantum analogue of the classical ECDH. Using an extended version of SIDH called eSIDH, we proposed an authenticated key exchange protocol resistant against quantum cryptanalysis, timing attacks, offline dictionary attack and MitM attack which security is based on the hard problem of finding isogenies of supersingular elliptic curve. We also considered the security of our protocol under the eCK because of the additional security requirements captured in the model.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Steven, D. G. and Vercauteren F. "Computational problems in supersingular elliptic curve isogenies", *Cryptology*, ePrint Archive, Paper 2017/774, doi: 10.1007/s11128-018-2023-6, https://eprint.iacr.org/2017/774.

[2] Cohen, A. D'Oliveira, R. G. L Salamatian S. & Medard, M. "Network Coding-Based Post-Quantum Cryptography". *IEEE Journal on Selected Areas in Information Theory*. https://doi.org/10.1109/jsait.2021.3054598, 2021.

[3] Cayrel, PL. Yousfi, El. Alaoui, S.M. Hoffmann, G Meziani, M. Niebuhr, R. "Recent Progress in Code-Based Cryptography". *In: Kim, Th., Adeli, H., Robles, R.J. Balitanas, M. (eds) Information Security and Assurance. ISA. Communications in Computer and Information Science*, vol 200. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23141-4_3, 2011.

[4] Balamurugan, C. Singh, K. Ganesan, G. & Rajarajan, M. "Post-Quantum and Code-Based Cryptography—Some Prospective Research Directions", 2021. Cryptography, 5(4),38.

[5] Li, L. Lu, X. & Wang, K. "Hash-based signature revisited". *Cybersecurity* 5, 13. https://doi.org/10.1186/s42400-022-00117-w, 2022.

[6] Suhail, S. Hussain, R. Khan, A. & Hong, C.S. "On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions". *IEEE Internet of Things Journal*, 8, 1-17, 2020.

[7] Thanalakshmi, P. Anitha, R. Anbazhagan, N. Cho, W. Joshi, G. P. & Yang, E. "A Hash-Based Quantum-Resistant Chameleon Signature Scheme". *Sensors* (Basel, Switzerland), 21(24), 8417. https://doi.org/10.3390/s21248417, 2021.

[8] Wunderer, T. "A detailed analysis of the hybrid lattice-reduction and meet-in-the-middle attack". *Journal of Mathematical Cryptology*, 13(1), 1-26. https://doi.org/10.1515/jmc-2016-0044, 2019.

[9] Jao, D. Feo, L.D. "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies". *In: Yang, B. (ed.) Post-Quantum Cryptography-4th International Workshop, PQCrypto*, Taipei, Taiwan. Vol. 7071 of Lecture Notes in Computer Science, pp. 19–34. Springer (2011). https://doi.org/10.1007/978-3-642-25405-5, 2011.

[10] Alawatugoda, J. "Authenticated Key Exchange Protocol in the Standard Model under Weaker Assumptions", *Cryptography* 7(1):1. https://doi.org/10.3390/cryptography, 2023.

[11] Alamati, N De Feo, L. Montgomery, H. Patranabis, S. "Cryptographic Group Actions and Applications". *In: Moriai, S., Wang, H. (eds) Advances in Cryptology* – ASIACRYPT 2020. ASIACRYPT 2020. Lecture Notes in Computer Science, vol 12492. Springer, Cham. https://doi.org/10.1007/978-3-030-64834-3_14, 2020.

[12] Basso, A. "A post-quantum round-optimal oblivious PRF from isogenies". *Cryptology* ePrint Archive, Paper 2023/225 (2023). https://eprint.iacr.org/2023/225, 2023.

[13] Yalamuri, G. Honnavalli, P. Eswaran, S. "A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats", *Procedia Computer Science*, Volume 215, Pages 834-845, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.086, 2022.

[14] Tom, J. J. Anebo, N. P. Onyekwelu, B. A. Wilfred, A. & Eyo, R.E. "Quantum Computers and Algorithms: A Threat to Classical Cryptographic Systems". *In International Journal of Engineering and Advanced Technology* (Vol. 12, Issue 5, pp. 25–38), Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP. https://doi.org/10.35940/ijeat.e4153.0612523, 2023.

[15] Fujioka, A., Takashima, K., Terada, S., Yoneyama, K. "Supersingular Isogeny Diffie–Hellman Authenticated Key Exchange". *In: Lee, K. (eds) Information Security and Cryptology – ICISC 2018. ICISC 2018. Lecture Notes in Computer Science*, vol 11396. *Springer*, Cham. https://doi.org/10.1007/978-3-030-12146-4_12, 2019.

[16] Xu, X. Xue, H. Wang, K. Au, M.H. Tian, S. "Strongly Secure Authenticated Key Exchange from Supersingular Isogenies". *In: Galbraith, S., Moriai, S. (eds) Advances in Cryptology – ASIACRYPT 2019. ASIACRYPT 2019*. Lecture Notes in Computer Science, vol 11921. Springer, Cham. https://doi.org/10.1007/978-3-030-34578-5_11, 2019.

[17] Cervantes-Vázquez, D., Ochoa-Jiménez, E., & Rodríguez-Henríquez, F. "Extended supersingular isogeny Diffie–Hellman key exchange protocol: Revenge of the SIDH". *IET Information Security*, 15(5), 364-374, 2021.

[18] Azarderakhsh, R. et al. "Supersingular Isogeny Key Encapsulation". *Second Round Candidate of the NIST's Post-Quantum Cryptography Standardisation Process* (2017). https://sike.org/.Accessed 23 April 2021.

[19] Tom, J.J. Alese, B.K. Thompson, A.F. & Anebo, N.P. "Performance and Security of Group Signature in Wireless Networks". *International Journal of Computer* (IJC) ISSN 2307-4523 (2018) Volume 29, No 1, pp 82-98, 2018. Global Society of Scientific Research and Researchers.

[20] Yang, X. Yi, X. Khalil, I. Fengling, H. & Tari, Z. "Securing Body Sensor Network with ECG". 298-306, 2016. 10.1145/3007120.3007121, 2016.

[21] Soukharev, V. & Hess, B. "PQDH: A Quantum-Safe Replacement for Diffie-Hellman based on SIDH". *IACR Cryptol*. ePrint Arch., 2019, 730, 2019.

[22] Zhang J., Zhang, Z Ding, J. Snook, M. Dagdelen, Ö. "Authenticated Key Exchange from Ideal Lattices". *In: Oswald, E., Fischlin, M. (eds) Advances in Cryptology - EUROCRYPT 2015*. Lecture Notes in Computer Science, vol 9057. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-46803-6_24, 2015.

[23] Shor, P. W. "Algorithms for quantum computation: Discrete logarithms and factoring". *In Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124–134. IEEE, 1994.

[24] National Institute of Standards and Technology “Post-Quantum Cryptography Standardization Process”. https://csrc.nist.gov/Projects/ Post-Quantum-Cryptography, 2017.
[25] Amdahl, G.M. “Validity of the Single-Processor Approach to Achieving Large-Scale Computing Capabilities,” Proc. Am. Federation of Information Processing Societies Conf., AFIPS Press, pp. 483-485, 1967.