Engineering and Technology Journal e-ISSN: 2456-3358
Volume 09 Issue 10 October-2024, Page No.- 5456-5462
DOI: 10.47191/etj/v9i10.31, I.F. – 8.227
© 2024, ETJ

Improving the CSIDH Protocol for Multi-party Cryptography: Rigorous Mathematical Analysis, Efficiency, and Security Comparison

Mohammed El Baraka, Siham Ezzouak
Sidi Mohamed Ben Abdellah University, Fez, Morocco

ABSTRACT

This paper introduces a novel Distributed Key Generation (DKG) protocol based on the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) framework for secure multi-party cryptography. Our proposed protocol is designed to address scalability and security concerns, particularly in post-quantum cryptographic systems. The main contributions include the introduction of Piecewise Verifiable Proofs (PVPs) for non-interactive zero-knowledge verification of secret shares, and the provision of rigorous security analysis, including resistance to quantum adversaries via Shor's and Grover's algorithms. We analyze the protocol's efficiency, ensuring low computational overhead even in large-scale systems, and compare it with other distributed cryptographic protocols such as RSA-based and lattice-based schemes. Through mathematical proofs and complexity analysis, we demonstrate that our protocol offers enhanced security, efficiency, and scalability in a post-quantum environment. The results presented in this paper provide a strong foundation for implementing secure multi-party computations in quantum-resistant systems.

Keywords: CSIDH, post-quantum cryptography, distributed key generation, isogenies, zero-knowledge proofs, Shor's algorithm, Grover's algorithm, multi-party cryptography.

1 Introduction

With the increasing threat posed by quantum computers, traditional cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC) are becoming vulnerable to quantum attacks. As a result, post-quantum cryptographic schemes are of growing importance. One promising candidate is the **Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)** protocol, which offers security based on the hardness of the Supersingular Isogeny Problem (SIP) and is resistant to quantum attacks.

However, while CSIDH has been well-researched in the context of two-party key exchanges, its extension to multi-party cryptography presents unique challenges, particularly in terms of security, scalability, and computational efficiency. To address these challenges, we propose a novel **Distributed Key Generation (DKG)** protocol based on CSIDH, aimed at securely generating a shared secret among multiple parties.

1.1 Contributions of This Paper:

1. Novel DKG Protocol: We propose a CSIDH-based DKG protocol, optimized for secure multi-party cryptography.

2. Piecewise Verifiable Proofs (PVPs): Non-interactive zero-knowledge proofs that ensure the correctness of each participant's share without revealing secret information.

3. Security Analysis: We provide a rigorous security analysis, proving the protocol's resistance to classical and quantum attacks, including detailed analysis against Shor's and Grover's algorithms.

4. Efficiency and Scalability: We analyze the time complexity and computational costs of our protocol, demonstrating its scalability in large-scale cryptographic systems.

5. Comparison with Existing Protocols**: We compare our protocol's security and efficiency with other distributed cryptographic systems, including RSA-based and lattice-based schemes.

1.2 Structure of This Paper:

- Section 2: Preliminaries provides the mathematical foundation, including definitions of elliptic curves, isogenies, and Shamir's Secret Sharing scheme, as well as explanations of key quantum algorithms (Shor's and Grover's).

- Section 3: The Distributed Key Generation (DKG) Protocol** introduces our novel protocol, including its components, mathematical formulation, and use of Piecewise Verifiable Proofs (PVPs).

- Section 4: Efficiency Analysis presents a detailed analysis of the computational efficiency of our protocol, calculating the time complexity of key operations.

- Section 5: Security Analysis rigorously examines the classical and quantum security of the protocol, including proofs of correctness, privacy, and resistance to quantum attacks.

- Section 6: Comparison with Existing Protocols compares our protocol's performance against other DKG systems, including RSA-based and lattice-based schemes.

- Section 7: Conclusion summarizes the main contributions and highlights the implications for post-quantum cryptography.

1.3 Related Works

The development of post-quantum cryptographic systems has gained significant traction in recent years. Isogeny-based cryptography, particularly the CSIDH protocol, has emerged as a strong candidate for quantum-resistant public key cryptosystems. **Jao and De Feo** first introduced the use of supersingular isogenies for constructing post-quantum cryptosystems in their work on supersingular isogeny-based key exchange [2]. **Castryck et al.** later improved on this with the introduction of the CSIDH protocol, which leverages commutative group actions on elliptic curves to achieve quantum resistance [3].

The problem of distributed key generation has been extensively studied in the context of classical cryptography. **Boneh and Franklin** developed efficient RSA-based DKG protocols, but these are vulnerable to quantum attacks due to Shor's algorithm [9]. More recently, **Peikert** and others have focused on lattice-based DKG protocols, which are resistant to quantum attacks but suffer from higher computational overheads [10, 11]. While lattice-based schemes show promise, their scalability remains a challenge for large-scale cryptographic systems.

In the realm of zero-knowledge proofs, **Goldwasser et al.** introduced the concept of zero-knowledge interactive proofs, which form the foundation for Piecewise Verifiable Proofs (PVPs) in our protocol [14]. These PVPs ensure that participants can verify the validity of each share without compromising security, an essential feature for secure multi-party cryptography.

This work builds upon these existing foundations, extending the CSIDH protocol to multi-party cryptography, and introducing optimizations for efficiency and security that make it suitable for post-quantum systems.

2 Preliminaries

In this section, we provide the necessary mathematical background for the CSIDH protocol and the DKG extension. We also define key quantum algorithms that are relevant to the security analysis.

2.1 Elliptic Curves

Definition 1. *An **elliptic curve** E over a finite field $\mathbb{F}_p$ is given by the Weierstrass equation:*

$$E : y^2 = x^3 + ax + b \quad \textit{where} \quad a, b \in \mathbb{F}_p$$

The set of points on the curve, denoted $E(\mathbb{F}_p)$, forms an abelian group under point addition, with the point at infinity serving as the identity element. The group operation is well-defined using a geometric construction involving the intersection of lines with the curve [1].

Theorem 1. *The **number of points** on an elliptic curve over a finite field $\mathbb{F}_p$ is bounded by Hasse's theorem:*

$$|E(\mathbb{F}_p)| = p + 1 - t \quad \textit{where} \quad |t| \leq 2\sqrt{p}$$

This result provides an upper and lower bound for the number of points and is fundamental in cryptographic applications, where the cardinality of $E(\mathbb{F}_p)$ determines the strength of the discrete logarithm problem (DLP) on elliptic curves [1].

2.2 Isogenies and Isogeny Graphs

Definition 2. *An **isogeny** $\varphi : E_1 \to E_2$ is a surjective homomorphism between two elliptic curves that preserves the group structure:*

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

The degree of an isogeny $\deg(\varphi)$ is the size of its kernel, and isogenies of the same degree can be composed to form more complex isogenies [2].

Theorem 2. *The **kernel of an isogeny** is a finite subgroup of the elliptic curve, and the number of points in the kernel is equal to the degree of the isogeny:*

$$|\ker(\varphi)| = \deg(\varphi)$$

Proposition 1. *For any elliptic curve E over a finite field, the set of all isogenies between curves can be represented as a directed graph, known as an **isogeny graph**, where vertices correspond to elliptic curves and edges correspond to isogenies of a fixed degree [4].*

2.3 The Supersingular Isogeny Problem (SIP)

Definition 3. *The* ***Supersingular Isogeny Problem (SIP)*** *is defined as follows: Given two supersingular elliptic curves E_1 and E_2 over a finite field, find an isogeny $\varphi : E_1 \to E_2$ [2].*

Theorem 3. *The SIP is believed to be quantum-resistant due to the difficulty of finding an isogeny between two supersingular elliptic curves. This problem is computationally infeasible both classically and quantumly, and no polynomial-time algorithm (including Shor's algorithm) is known to solve it [2,* **?***].*

2.4 Group Action in CSIDH

Definition 4. *In the CSIDH protocol, the ideal class group $\mathcal{C}$ acts on the set of isomorphism classes of supersingular elliptic curves. Given an elliptic curve E_1 and an ideal $I \in \mathcal{C}$, the group action results in a new elliptic curve E_2:*

$$E_2 = I * E_1$$

Theorem 4. *The* ***Group Action Inverse Problem (GAIP)*** *is defined as follows: Given two elliptic curves E_1 and E_2, find the ideal $I \in \mathcal{C}$ such that $E_2 = I * E_1$. The GAIP is assumed to be hard, even for quantum computers, and serves as the security foundation of the CSIDH protocol [***?***].*

2.5 Shamir's Secret Sharing

Definition 5. *Shamir's Secret Sharing is a method for distributing a secret S among n participants. The secret is encoded in a polynomial $f(x)$ of degree $t-1$, where t is the threshold required to reconstruct the secret:*

$$f(x) = S + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}$$

Each participant P_i receives a share $s_i = f(i)$. The secret can be reconstructed using ***Lagrange interpolation*** *if at least t shares are available [5].*

Theorem 5. *Shamir's Secret Sharing scheme is* ***information-theoretically secure****, meaning that any coalition of fewer than t participants cannot reconstruct the secret. The security of the scheme relies on the fact that the polynomial $f(x)$ is completely determined by t points, and fewer than t points provide no information about the secret S [5].*

2.6 Quantum Algorithms: Shor's and Grover's

Definition 6. ***Shor's algorithm*** *is a quantum algorithm that efficiently solves the integer factorization problem and the discrete logarithm problem in polynomial time. It can break classical RSA and ECC cryptosystems, but it does not apply directly to isogeny-based cryptographic systems [6].*

Definition 7. ***Grover's algorithm*** *provides a quadratic speedup for unstructured search problems, reducing the time complexity of brute-force search from $O(N)$ to $O(\sqrt{N})$. In cryptographic terms, this means that Grover's algorithm can reduce the effective security level of a system by approximately half [7].*

Theorem 6. *Isogeny-based cryptographic systems, such as CSIDH, are believed to be secure against attacks using Shor's algorithm. The hardness of the Supersingular Isogeny Problem (SIP) underpins this security, as there are no known quantum algorithms capable of solving SIP in polynomial time [2, 8].*

Proposition 2. *Grover's algorithm can be applied to speed up brute-force key searches in cryptographic protocols. In the case of CSIDH, increasing the field size or parameter sizes can mitigate the impact of Grover's algorithm by maintaining the desired security level [8].*

3 The Distributed Key Generation (DKG) Protocol

We now describe our DKG protocol for CSIDH, which allows multiple participants to securely generate a shared secret.

- **Isogeny Computation**: Each participant computes φ_i, the isogeny from E to E_i, based on their secret share. The hardness of finding the isogeny between supersingular elliptic curves underpins the security of this step.
- **Piecewise Verifiable Proofs (PVPs)**: PVPs are zero-knowledge proofs that ensure the commitment C_i is valid without revealing the secret share s_i. They are sound (only valid commitments will be accepted) and complete (valid commitments will always pass the verification).
- **Secret Reconstruction:** Lagrange interpolation ensures that the shared secret can only be reconstructed with the collaboration of at least t participants.

4 Efficiency Analysis

The efficiency of the DKG protocol is essential for its feasibility in large-scale cryptographic applications. Here, we analyze the computational costs associated with each step of the protocol, providing justifications for the time complexities and the number of operations involved in the key steps.

4.1 Isogeny Computation

For each participant, computing the isogeny φ_i from the base elliptic curve E to E_i is the most computationally intensive step. This computation relies on the CSIDH protocol, where the class group action on supersingular elliptic curves is equivalent to solving a set of isogeny problems. Each isogeny computation requires:

- Time complexity: $O(\log p)$, where p is the size of the prime field $\mathbb{F}_p$. The logarithmic complexity reflects the fact that the length of the isogeny path is proportional to the logarithm of the field size [3, 12].
- Number of operations: For n participants, each computing an isogeny, the total number of isogeny operations is proportional to $n \log p$. Therefore, the total number of operations for all participants is $O(n \log p)$.

4.2 Piecewise Verifiable Proof (PVP) Generation and Verification

After computing their isogeny, each participant generates a PVP, which is a non-interactive zero-knowledge proof of the correctness of the share. The PVP involves creating and verifying small cryptographic proofs.
- Time complexity: $O(1)$ per participant, as generating and verifying the PVP is independent of the field size and depends only on the structure of the cryptographic proof [14].
- Number of operations: For n participants, generating and verifying PVPs requires $O(n)$ operations.

4.3 Secret Reconstruction

The final step in the DKG protocol is the reconstruction of the shared secret using Lagrange interpolation. This step involves computing polynomial interpolation, which depends on the number of participants and the degree of the polynomial used in Shamir's Secret Sharing [5].
- Time complexity: $O(t^2)$, where t is the threshold for the minimum number of participants required to reconstruct the secret. This quadratic complexity arises from the interpolation algorithm, which involves computing products and sums of shares.
- Number of operations: For t participants, the number of operations needed for secret reconstruction is $O(t^2)$. In a typical case where t is small compared to n, this step is relatively efficient.

4.4 Justification of Results:

- The logarithmic time complexity of the isogeny computation reflects the reliance on the CSIDH structure, which benefits from sublinear performance due to the relatively small group size in comparison to classical elliptic curve cryptography [3, 13].
- The constant time complexity for PVP generation and verification ensures that the overhead from zero-knowledge proofs does not significantly impact performance. This is crucial for scalability, as it allows the protocol to accommodate a large number of participants without increasing computational costs exponentially [14].
- The quadratic complexity of the secret reconstruction process, while more expensive than the other steps, is justified by the use of Lagrange interpolation. Given that the threshold t is typically much smaller than n, this step does not dominate the overall time complexity and remains efficient in practice.

We summarize the overall time complexity in the following table.

This analysis shows that our CSIDH-based DKG protocol is computationally efficient, with most steps scaling logarithmically or linearly with the number of participants. The only quadratic term arises from the secret reconstruction phase, which is manageable given the typical sizes for t in real-world applications.

5 Security Analysis: Mathematical Justification

In this section, we provide a detailed security analysis of the DKG protocol for CSIDH. The analysis is divided into two parts:
1. Classical Security: Ensuring that the protocol is secure against classical adversaries.
2. Quantum Security: Analyzing the resistance of the protocol to quantum attacks, particularly Shor's and Grover's algorithms.

5.1 Security Requirements

For the DKG protocol to be secure, it must satisfy the following:

1. Correctness: The protocol must ensure that if all participants follow the protocol, the correct shared secret will be generated [5].

2. Privacy: No participant (or set of participants less than the threshold t) should be able to learn the secret or the shares of others [5].

3. Resistance to Quantum Attacks: The protocol must be resistant to attacks that exploit quantum algorithms such as Shor's and Grover's [6, 7].

5.2 Mathematical Proofs of Security

We first address the security guarantees of the DKG protocol by providing mathematical proofs for correctness, privacy, and quantum security.

Theorem 7 (Correctness of the DKG Protocol)**.** *The DKG protocol ensures that the correct shared secret S will be generated as long as the number of participants $n \geq t$, where t is the threshold.*

Proof. The correctness of the protocol is based on the use of Shamir's Secret Sharing scheme. Each participant P_i contributes a secret share s_i encoded in a polynomial $f(x)$ of degree $t-1$. The secret is reconstructed using Lagrange interpolation:

$$S = \sum_{i=1}^{t} s_i \prod_{\substack{1 \leq j \leq t \\ j \neq i}} \frac{0-j}{i-j}$$

Since the protocol ensures that at least t participants are required to reconstruct the secret, and the interpolation guarantees unique reconstruction when t valid shares are combined, the correctness of the secret reconstruction is assured [5]. □

Theorem 8 (Privacy of the DKG Protocol)**.** *The DKG protocol preserves the privacy of the participants. Specifically, no coalition of fewer than t participants can reconstruct the shared secret or learn the individual shares of other participants.*

Proof. The privacy guarantee follows directly from the properties of Shamir's Secret Sharing. The polynomial $f(x)$ is of degree $t-1$, which means that knowledge of fewer than t shares reveals no information about the constant term S, which represents the secret.

The commitment $C_i = \varphi_i * E$ published by each participant contains no information about the actual share s_i, as it only reveals the result of the isogeny φ_i, which is computationally infeasible to reverse (due to the hardness of the Supersingular Isogeny Problem, SIP) [2]. Therefore, even with access to the commitments, fewer than t participants cannot learn any information about the secret [13]. □

5.3 Quantum Security: Resistance to Shor's and Grover's Algorithms

Quantum security is a major concern for post-quantum cryptographic protocols. In this section, we rigorously analyze the security of the DKG protocol under quantum adversaries, focusing on the two most powerful quantum algorithms known: Shor's and Grover's.

Theorem 9 (Resistance to Shor's Algorithm)**.** *The DKG protocol is secure against attacks using Shor's algorithm. Specifically, the security of the protocol relies on the hardness of the Supersingular Isogeny Problem (SIP), for which no polynomial-time quantum algorithm (including Shor's algorithm) exists [2].*

Proof. Shor's algorithm provides an efficient means of solving the discrete logarithm problem and factoring large integers in polynomial time. However, the security of the DKG protocol does not rely on these problems. Instead, it relies on the hardness of finding an isogeny between two supersingular elliptic curves, i.e., solving the SIP.

Currently, no polynomial-time algorithm (classical or quantum) exists to solve the SIP, and Shor's algorithm is ineffective against isogeny-based cryptographic problems [4]. The complexity of finding an isogeny between two random supersingular elliptic curves over $\mathbb{F}_p$ remains computationally infeasible even for quantum computers, thus ensuring that the DKG protocol remains secure against attacks using Shor's algorithm. □

Theorem 10 (Resistance to Grover's Algorithm)**.** *The DKG protocol is secure against attacks using Grover's algorithm. Grover's algorithm can be applied to brute-force search problems, but it only offers a quadratic speedup, which can be mitigated by increasing key sizes [7].*

Proof. Grover's algorithm provides a quadratic speedup for unstructured search problems, reducing the time complexity of brute-force key search from $O(2^n)$ to $O(2^{n/2})$. However, this speedup does not render the DKG protocol vulnerable, as the primary security of the protocol is based on the SIP.

To counter the effect of Grover's algorithm, the size of the parameters (e.g., the size of the field p) can be doubled to maintain the same level of security as in a classical setting. Specifically, increasing the size of the key ensures that Grover's algorithm does not lead to a practical attack on the DKG protocol [8]. □

5.4 Security Against Collusion Attacks

The DKG protocol must also ensure that no coalition of participants (fewer than the threshold t) can combine their shares to reconstruct the secret or learn information about the shares of others.

Theorem 11 (Security Against Collusion Attacks)**.** *The DKG protocol is secure against collusion attacks. No coalition of fewer than t participants can learn the shared secret or other participants' shares [5].*

Proof. The security against collusion follows from the privacy properties of Shamir's Secret Sharing. Since the polynomial $f(x)$ is of degree $t-1$, knowledge of fewer than t shares does not provide sufficient information to reconstruct the polynomial or determine the secret S.

Moreover, the commitments $C_i = \varphi_i * E$ reveal no information about the actual share s_i, as reversing the isogeny is computationally infeasible (due to the hardness of SIP). Therefore, even if fewer than t participants combine their shares, they cannot learn the secret or any other participant's share [2]. □

5.5 Security Against Forging or Invalid Shares

The use of **Piecewise Verifiable Proofs (PVPs)** ensures that any attempt by a malicious participant to submit an invalid share will be detected.

Theorem 12 (Security Against Invalid Shares)**.** *The DKG protocol detects and prevents the use of invalid or forged shares through the use of Piecewise Verifiable Proofs (PVPs). A malicious participant cannot successfully submit an invalid share without detection [14].*

Proof. Each participant generates a Piecewise Verifiable Proof (PVP) π_i, which is a non-interactive zero-knowledge proof that the commitment C_i corresponds to a valid isogeny and secret share. The PVP is sound and complete, meaning:
1. Soundness: If the share is invalid, the PVP will fail, and the commitment will be rejected.
2. Completeness: If the share is valid, the PVP will succeed, and the commitment will be accepted.

This ensures that no participant can submit a forged or invalid share without being detected by other participants, maintaining the integrity of the DKG protocol [14]. □

5.6 Conclusion of Security Analysis

The DKG protocol for CSIDH is mathematically proven to be secure under both classical and quantum settings. It resists attacks from Shor's and Grover's algorithms by relying on the hardness of the Supersingular Isogeny Problem (SIP), which remains computationally infeasible even in a quantum setting. Additionally, the protocol is secure against collusion and forgery due to the use of Shamir's Secret Sharing and Piecewise Verifiable Proofs (PVPs). Therefore, the DKG protocol meets the necessary security requirements for a robust multi-party cryptographic system.

6 Comparison with Existing Protocols

In this section, we present the existing distributed key generation protocols and compare them with our CSIDH-based DKG protocol.

6.1 Classical RSA-based Distributed Key Generation

Classical RSA-based DKG protocols are among the oldest approaches to distributed key generation. These protocols involve using RSA encryption to enable multiple parties to collaborate in generating a shared RSA private key. However, with the advent of quantum computing, RSA-based cryptography is no longer considered secure, as Shor's algorithm can break the RSA problem in polynomial time [6]. Classical RSA-based DKG protocols are thus vulnerable to quantum attacks, and their efficiency is limited by the large computational overhead involved in RSA key generation [9].

6.2 Lattice-based Distributed Key Generation

Lattice-based cryptographic schemes have gained prominence in post-quantum cryptography due to their conjectured resistance to quantum attacks. Lattice-based DKG protocols, which are typically based on the Learning With Errors (LWE) problem, enable secure multi-party key generation. However, these protocols often require significantly larger key sizes to maintain the same level of security as classical schemes [10]. While lattice-based DKG protocols are resistant to quantum attacks, their efficiency is constrained by the high computational and memory overhead associated with lattice-based cryptography [11].

6.3 CSIDH-based Distributed Key Generation (Our Protocol)

Our CSIDH-based DKG protocol leverages the hardness of the Supersingular Isogeny Problem (SIP) to ensure quantum security. The use of isogenies between supersingular elliptic curves provides a quantum-resistant foundation for the protocol. Additionally, Piecewise Verifiable Proofs (PVPs) allow for efficient non-interactive verification of each participant's secret share. This makes our protocol more efficient and scalable for large-scale multi-party cryptographic systems [3, 2].

We now compare the efficiency and security of our protocol with the aforementioned classical and lattice-based protocols.

7 Conclusion

In this paper, we presented a novel Distributed Key Generation (DKG) protocol based on the Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) framework, with significant improvements in security, efficiency, and scalability, particularly in post-quantum cryptographic systems. Our protocol introduces Piecewise Verifiable Proofs (PVPs), allowing for non-interactive verification of secret shares in a zero-knowledge setting, which enhances the robustness of multi-party cryptography without sacrificing computational efficiency.

We provided a rigorous security analysis, proving that the protocol is resistant to both classical and quantum adversaries, particularly those using Shor's and Grover's algorithms. The security of our scheme is grounded in the hardness of the Supersingular Isogeny Problem (SIP), which remains a computationally infeasible problem for both classical and quantum computers. Additionally, we showed that the protocol maintains privacy and correctness even in the presence of adversarial participants, providing strong guarantees for real-world multi-party applications.

The efficiency analysis demonstrated that our protocol scales well for large numbers of participants, with time complexities that outperform classical RSA-based DKG protocols and are competitive with lattice-based schemes, making it a practical choice for large-scale cryptographic systems in a post-quantum world. The comparative analysis further highlighted the advantages of our approach in terms of both security and computational cost.

Overall, this work contributes to the growing body of research in post-quantum cryptography by extending the applicability of CSIDH to secure multi-party computations. The presented DKG protocol addresses critical challenges in secure distributed cryptography, providing a solid foundation for future work in scalable, quantum-resistant systems. Future research directions may include exploring additional optimizations for further reducing computational overhead, as well as adapting the protocol for specific applications such as blockchain, secure voting systems, and cloud-based cryptographic services.

The contributions made in this work highlight the potential of isogeny-based cryptography as a key tool in the development of secure, scalable, and efficient post-quantum cryptographic protocols. We anticipate that the techniques and methods introduced here will inspire further advancements in the field of distributed cryptography, contributing to the ongoing efforts to secure digital systems against the looming threat of quantum computing.

References

[1] J. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.

[2] D. Jao and L. De Feo, ”Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies,” in *Post-Quantum Cryptography*, 2011, pp. 19–34.

[3] D. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, ”CSIDH: An efficient post-quantum commutative group action,” in *Advances in Cryptology – ASIACRYPT 2018*, pp. 395–427.

[4] L. De Feo and D. Jao, ”Towards quantum-resistant cryptosystems: Supersingular isogeny graphs,” in *Post-Quantum Cryptography*, 2011.

[5] A. Shamir, ”How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[6] P. Shor, ”Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.

[7] L. Grover, ”A fast quantum mechanical algorithm for database search,” in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, 1996.

[8] D. Unruh, ”Post-quantum security of Fiat-Shamir,” in *Advances in Cryptology - ASIACRYPT 2017*, pp. 65–95.

[9] D. Boneh and M. Franklin, ”Efficient generation of shared RSA keys,” in *Proceedings of Advances in Cryptology - CRYPTO ’97*, pp. 425–439.

[10] C. Peikert, ”A decade of lattice cryptography,” *Foundations and Trends in Theoretical Computer Science*, vol. 10, no. 4, pp. 283–424, 2016.

[11] V. Vaikuntanathan, ”Lattice cryptography,” in *Advances in Cryptology – CRYPTO 2017*, pp. 48–76.

[12] C. Costello, ”A brief introduction to isogeny-based cryptography,” in *Proceedings of Real World Crypto 2019*.

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

[14] S. Goldwasser, S. Micali, and C. Rackoff, ”The knowledge complexity of interactive proof systems,” *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, 1989.