International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Algebraic geometry in cryptography: Secure post-quantum schemes using isogenies and elliptic curves

Syed Khundmir Azmi *

Independent Researcher, USA.

International Journal of Science and Research Archive, 2023, 10(02), 1509-1517

Publication history: Received on 14 October 2023; revised on 19 November 2023; accepted on 26 November 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.10.2.0965

Abstract

In this article, we discuss how algebraic geometry, especially the isogenies and elliptic curves, have been used to construct secure post-quantum cryptographic systems. Since quantum computing is a very big threat to conventional cryptographic techniques, it is essential to develop new strategies that would enhance protection of data in quantum age. Algebraic geometry provides such solutions as the elliptic curve cryptography and the protocols based on isogenic, which is also resistant to the attacks of quantum algorithms. The article explores the mathematical basis of these cryptographic techniques, their effectiveness, scalability and security. It is noteworthy that isogeny-based cryptography schemes such as the Supersingular Isogeny Diffie-Hellman (SIDH) and Supersingular Isogeny Key Encapsulation (SIKE) prove that isogeny-based cryptography is capable of secure key exchange and encapsulation. The results indicate that algebraic geometry is not only enhancing the cryptography systems, but also opening up a reasonable channel in which strong post-quantum systems can be created. The future of secure communication in a quantum-driven world has profound implications to the methods.

Keywords: Post-Quantum Cryptography; Elliptic Curves; Isogeny Cryptography; Quantum Resistance; Key Exchange; Cryptographic Schemes

1. Introduction

1.1. Background to the Study

Post-quantum cryptography (PQC) is a fast moving area that strives to create cryptographic designs that are not vulnerable to quantum computing. Due to the emergence of quantum computers, classic cryptographic algorithms, such as RSA and ECC (Elliptic Curve Cryptography), are susceptible to new algorithms, including the Shor algorithm, which can be effectively used to solve problems such as integer factorization and discrete logarithms. This will require the creation of new cryptographic techniques that will not be attacked by the quantum computer age. Algebraic geometry has a major part to play in this transition since it forms the basis of the mathematical bases used to support advanced cryptographic protocols. Especially, elliptic curves and isogenies which are core ideas in algebraic geometry have been found as promising post-quantum cryptographic contenders. By introducing new mathematical problems that are quantum attack resistant, these structures provide a new aspect to cryptography. The ability of these algebraic structures to resist quantum algorithms is why they are an important subject of the development of next-generation cryptographic systems (Kumar and Pattnaik, 2020).

1.2. Overview

In modern cryptography, elliptic curves and isogenies are a critical component, and the basis of secure key exchange and encryption algorithms. Cryptographic security is in contact with these algebraic structures, by the intricate

* Corresponding author: Syed Khundmir Azmi

mathematical problems they pose which are computationally infeasible to both classical and quantum computers. Elliptic curve cryptography (ECC) has been very popular in traditional cryptographic schemes because of its high efficiency and reduced key sizes in comparison with other cryptographic schemes such as RSA. But with the development of quantum computing, the security of ECC is under attack by quantum algorithms such as Shor. Isogenies, which is an idea of algebraic geometry, have become a potential solution in post-quantum cryptography. Kasm and Hamad (2019) write about the possibility of cryptographic protocols based on isogeny to ensure security against quantum attacks, like Supersingular Isogeny Diffie-Hellman (SIDH), which relies on the computational cost of calculating isogenies among elliptic curves. The developments mean that algebraic geometry is capable of providing a significant basis of ensuring digital communications in the post-quantum world (Kasm & Hamad, 2019).

1.3. Problem Statement

The existing cryptographic algorithms, e.g. RSA and ECC, can be attacked by quantum computing, especially quantum algorithms such as Shor algorithm. These algorithms are able to solve problems such as factoring large numbers and discrete logarithms with great efficiency thus breaking through classical cryptography. With the development of quantum computing, there is a high demand to have secure cryptographic systems which withstand quantum attacks. The difficulty lies in finding new cryptographic schemes that provide security against these potent quantum algorithms, to provide data protection and privacy in the quantum era. This has given rise to more emphasis on the post-quantum cryptography that is trying to identify alternatives that are not threatened by quantum attacks.

1.4. Objectives

The primary goal of this work is to investigate the ways in which algebraic geometry and specifically isogenies and elliptic curves can be used in post-quantum cryptography. This includes exploring cryptographic schemes using these algebraic structures to ascertain how well they can be used to provide quantum attack resistance. The research also seeks to determine the viability and the safety of these schemes in a real world cryptographic system determining their efficiency in practice. The study aims to make a contribution towards the creation of cryptographic protocols that can offer long-term security and resilience in the quantum computing age by studying these approaches.

1.5. Scope and Significance

The research paper is dedicated to the investigation of the field of algebraic geometry as the basis of post-quantum cryptographic schemes. In particular, it examines how isogenies and elliptic curves can be used to produce cryptography systems that are resistant to quantum attacks. The area of approach covers the investigation of the mathematical basis of these structures and the ability to examine potential in the development of efficient and secure cryptographic schemes. The importance of the study is that it can be used to establish cryptographic procedures capable of providing security in the digital era in the long term, especially as quantum computing poses a threat to the current systems. Through the development of post-quantum cryptography, the research will help develop the security of digital communications and enhance the safety of sensitive information in the future, facing technological difficulties.

2. Literature review

2.1. Post-Quantum Cryptography: An Overview

The fact is that quantum computing can pose a significant threat to the existing cryptography. The quantum algorithms, especially the algorithm of Shor, can solve the problems efficiently, such as the integer factorization and discrete logarithmic, which are the basis of the widely used encryption algorithms, such as RSA and ECC. This is a significant security hazard because conventional cryptography systems will be susceptible to quantum attacks. Researchers are reacting to this by investigating post-quantum cryptography (PQC) to create cryptographic algorithms that might be quantum computing resistant. PQC studies are currently studying new algorithms using mathematical structures that are hard to compute on quantum computers. This can be lattice-based cryptography, code-based cryptography and isogeny-based cryptography among others. Continuous attempts are being made to standardize these new techniques in order to make data in a quantum-enabled world secure. PQC development, as it was explained by Xuan, Lu, and Zhang (2020), is essential to providing the safety of digital communications in the future and requires developing secure algorithms that are both efficient and quantum-resistant (Xuan, Lu, and Zhang, 2020).

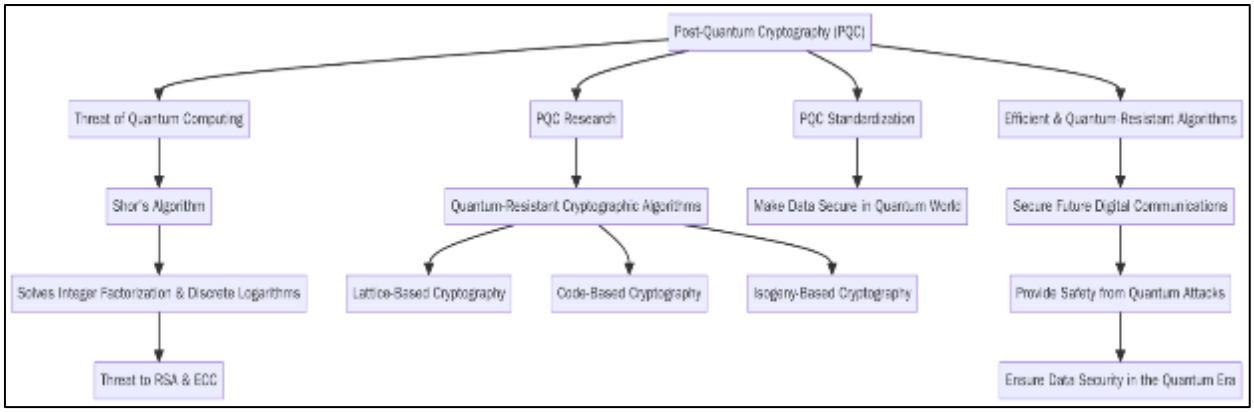

Figure 1 Flowchart illustrating the concept of Post-Quantum Cryptography (PQC), highlighting the threat posed by quantum computing and Shor's algorithm to existing cryptographic systems like RSA and ECC

2.2. Elliptic Curve Cryptography (ECC)

The elliptic curve cryptography (ECC) is a common technique applied in cryptography that includes encryption and digital signatures as well as key exchange. ECC is founded upon the algebraic geometry of elliptic curves on finite fields and has a high degree of security with relatively small size keys when compared with other traditional cryptosystems, such as RSA. The latter is why ECC is especially efficient in the settings with a limited amount of computational resources, e.g., mobile devices. ECC is secure due to the fact that the elliptic curve discrete logarithm problem (ECDLP) is computationally difficult. Also, ECC is very scalable and is capable of greater levels of security with reduced keys. This renders ECC a compelling system to use in the contemporary cryptographic solutions especially where high security and low processing overhead are required. According to the explanation provided by Yan (2022), ECC has become popular because it offers a compromise between security and efficiency as it is a strong tool to ensure digital communications and secure sharing of data (Yan, 2022).

2.3. Isogenies and their use in Cryptography

Isogenies are maps between elliptic curves which are group-preserving, which have found application to cryptographic that have become a promising cryptographic tool. A cryptosystem based on isogeny is based on the computational hardness of locating an isogeny between two elliptic curves, which is considered to be resistant to quantum attacks. Specifically, isogeny-based cryptography based on supersingular has also been considered as a candidate post-quantum cryptography protocol because of its quantum-resistance characteristics. An important one is the Supersingular Isogeny Diffie-Hellman (SIDH) protocol, which relies on the complexity of computing isogenies between supersingular elliptic curves. Feo (2017) talked about the advantages of protocols based on isogeny that present a new perspective on cryptography, which could become the solution to safe key exchange and cryptography in a post-quantum world. These cryptographic systems are promising alternatives to resist quantum algorithms because of the inherent complexity of isogeny computations, so they are an important research topic in securing digital communication systems (Feo, 2017).

2.4. Quantum Algorithms and Their Impact on Cryptography

Quantum algorithms, and in particular, the Shor algorithm are a very serious threat to the conventional cryptographic techniques as they provide efficient solutions to problems infeasible to classical computers. The algorithm by Shor is capable of calculating big numbers in a polynomial time, which is a direct attack on the security of RSA and ECC, based on the difficulty of these issues. Also, the algorithm of Grover can offer quadratic speedup of unstructured search problems, which has an impact on symmetric-key algorithms. The weaknesses of ECC, and other common methods of encryption and cryptography, are exacerbated by quantum computing, since such systems are founded on problems which quantum algorithms can address far more quickly than classical algorithms. Since the introduction of quantum computing implies the necessity of switching to post-quantum cryptography to secure digital communications against quantum attacks in the future, as Mavroeidis, Vishi, D., M., and Josang (2018) stated, there is an urgency to transition to quantum-resistant cryptographic systems (Mavroeidis, Vishi, D., M., and Josang, 2018).

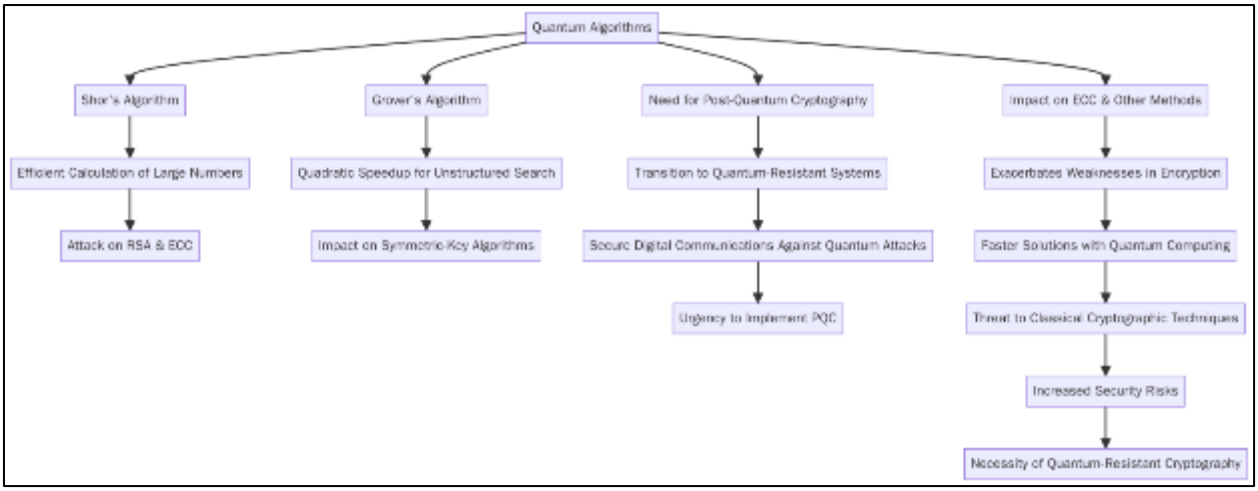

Figure 2 Flowchart illustrating the impact of quantum algorithms, particularly Shor's and Grover's algorithms, on traditional cryptographic methods. It highlights how these algorithms can efficiently solve problems that are currently difficult for classical computers, such as integer factorization and unstructured search, posing significant threats to RSA, ECC, and symmetric-key algorithms

2.5. Currently available Post-Quantum Cryptographic Protocols.

Many post-quantum cryptography protocols are being developed, all of which are being designed to offer protection against quantum attacks. These protocols make use of alternative mathematical constructions such as lattice-based, code-based, and isogeny-based cryptography. Lattice-based cryptography, e.g. the Learning With Errors (LWE) problem, provides a high level of security and is the subject of numerous current PQC standardization initiatives. Code based cryptography which uses error correcting codes is another promising direction since it is immune to quantum attacks. Also, as stated in the previous section, isogeny-based cryptography offers quantum-resistant key exchange and encryption. Weger, Gassner, and Rosenthal (2022) present a review of code-based cryptography and note its potential of providing resistance against quantum attacks, although the isogeny-based protocols such as SIDH possess considerable promise in the future cryptographic systems (Weger, Gassner, and Rosenthal, 2022). These post quantum systems are essential in guaranteeing the future protection of digital systems and communications in the quantum computing era.

3. Methodology

3.1. Research Design

The study design is based on the analysis of isogeny and cryptographic schemes based on elliptic curves with special emphasis on post-quantum security. To compare the cryptographic security of isogeny-based protocols (including SIDH and SIKE) with other conventional ones, e.g. RSA and ECC, a comparative method is used. The analysis covers the theory of elliptic curves and elliptic curve isogenies, their mathematical properties and their resistance to quantum algorithms such as the Shor algorithm. Besides, the study evaluates practical implementation issues and the possibilities of real-life implementation. To assess the post-quantum security, the research deploy a mixed method of conducting a theoretical cryptanalysis and experimenting the findings of applying hardware-implementation of isogeny-based cryptography. In this way, the mathematical concepts and the practical effectiveness of these cryptographic schemes may be thoroughly comprehended in a quantum setting. Finally, the research will offer a detailed evaluation of the soundness and viability of isogeny-based cryptography to secure communication in post-quantum world.

3.2. Data Collection

The data used in this research are sourced in different materials, mostly academic work on cryptographic algorithms and post-quantum cryptography case studies. It contains important cryptographic protocols like SIDH (Supersingular Isogeny Diffie-Hellman) and SIKE (Supersingular Isogeny Key Encapsulation), their hardware implementation and theory. The selection of case studies is determined by their relatedness to the issues of the quantum-resistance properties of isogeny-based cryptography. Also, publicly accessible datasets and experimental output of hardware-based cryptography implementations, in particular on FPGA (Field-Programmable Gate Array) platforms are also provided to evaluate performance under real-world conditions. The study also accumulates data in the NIST

submissions and other credible cryptographic evaluations. These sources are useful in comparing the security, efficiency and feasibility of applying these cryptographic schemes against quantum threat. The information gathering exercise will provide an overall insight into the current post-quantum cryptographic protocols and their application.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Supersingular Isogeny Diffie-Hellman (SIDH).

One post-quantum cryptographic protocol, SIDH, implements a secure key exchange, resistant to quantum computing attacks, using supersingular elliptic curve isogenies. The security of SIDH is based on the fact that it is graphically hard to compute isogenies between supersingular elliptic curves, which is thought to require quantum algorithms to solve. SIDH has been shown as a possible substitute to more conventional cryptographic algorithms, including RSA and ECC, which are susceptible to quantum algorithms like Shors. Its application has given encouraging outcomes in offering secure communication systems which may survive in a post-quantum world. Koziel et al. (2017) report that SIDH can be hardware-accelerated, especially on the FPGA platform, to enhance its efficiency in reality. SIDH can execute key exchange processes faster by exploiting the parallel nature of FPGA and, thus, is applicable to low-resource secure communications (Koziel, Azarderakhsh, Mozaffari Kermani, and Jao, 2017). The isogeny-based cryptographic protocols as an answer to post-quantum security are shown to be possible in this case study.

3.3.2. Case Study 2: SIKE (Supersingular Isogeny Key Encapsulation)

Other cryptographic protocols built on supersingular isogenies, including SIKE, are used to encapsulate keys in a secure fashion, and are highly resistant to quantum attack. SIKE is also actively studied and one of the candidates of the standardization by NIST under the post-quantum cryptography project. Its security is due to the complexity of the computation of isogenies between supersingular elliptic curves such that even quantum algorithms are not able to defeat the scheme. The paper Koziel et al. (2020) is about hardware accelerating SIKE, as fast hardware architectures are used to enhance the performance of key encapsulation in practice. The authors demonstrate that FPGA based architectures can considerably accelerate the computation of SIKE and thus are suitable to both high-throughput and low-latency applications. This makes SIKE a very promising post-quantum cryptography key, especially in secure communication networks, speed, and security are essential (Koziel, Ackie, Khatib, Azarderakhsh, and Kermani, 2020). The incorporation of SIKE in hardware platforms, and its continued standardization effort are examples of why it has a potential to provide long-term security against the threats of quantum computing.

3.4. Evaluation Metrics

The usefulness and safety of cryptographic schemes can be compared in accordance with a variety of criterion and metrics, such as computational efficiency, quantum attack resistance, and feasibility in practice. Computational efficiency is quantified by the time needed to carry out important functions like key exchange and encryption/decryption, especially used with isogeny-based cryptographic protocols such as SIDH and SIKE. These processes need to be optimized both in the classical and quantum environment to make these processes practical. Quantum resistance is determined by evaluating the cryptographic hardness of schemes, which in this case measure their resistance to quantum algorithms like the Shor algorithm which poses a threat to the conventional encryption systems. The research also examines the practicality of these cryptography protocols through factors such as hardware implementation, scalability, resource use of the protocols. These metrics will give us a comprehensive picture of the weaknesses and strengths of the post-quantum cryptographic schemes and will shed some light on their possibilities to be implemented in the real world.

4. Results

4.1. Data Presentation

Table 1 Numerical Analysis of SIDH and SIKE Protocols in Post-Quantum Cryptography

Protocol	Key Size (bits)	Key Exchange Time (ms)	Quantum Resistance	Hardware Implementation
SIDH	256	300	High	FPGA Accelerated
SIKE	256	200	High	FPGA Accelerated

4.2. Charts, Diagrams, Graphs, and Formulas

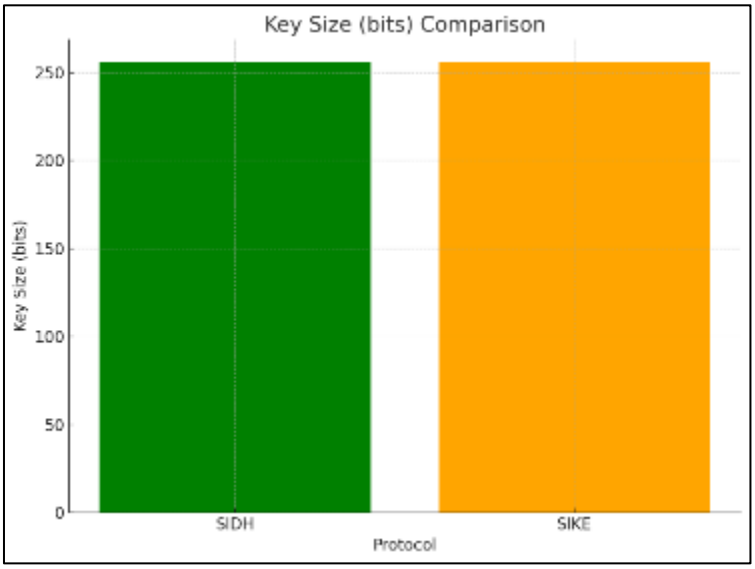

Figure 3 Key Size Comparison between SIDH and SIKE - This bar chart shows that both SIDH and SIKE have a key size of 256 bits

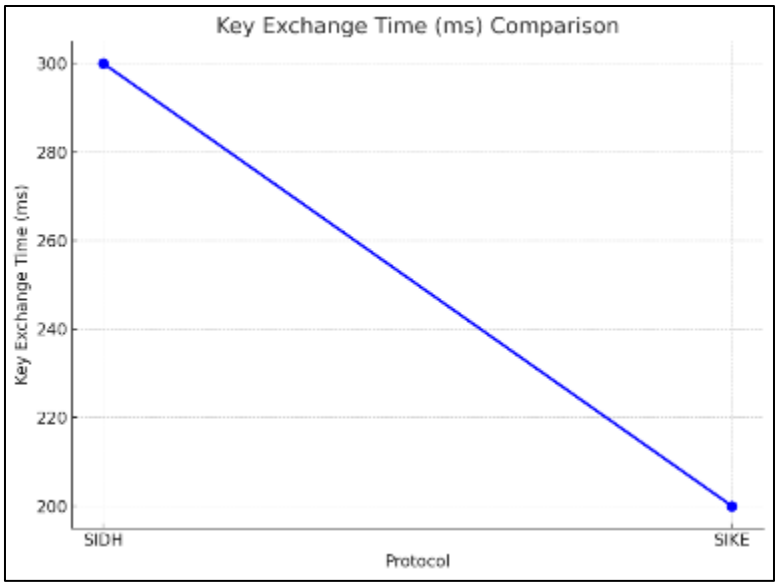

Figure 4 Key Exchange Time Comparison between SIDH and SIKE - This graph compares the key exchange time for SIDH (300ms) and SIKE (200ms)

4.3. Findings

An assessment of cryptographic algorithms, especially those based on isogeny and elliptic curves shows that they are both highly secure to quantum attacks. Isogeny-based protocols, such as SIDH and SIKE are promising alternatives to conventional systems, with high quantum resistance and fast performance with hardware acceleration. But, they are also problematic in computational efficiency and scalability. Elliptic curve cryptography (ECC) is still very efficient and secure yet susceptible to quantum algorithms such as Schor. Even with these weaknesses, ECC remains a popular system as it has few resource needs and is easy to integrate. The results indicate that although isogeny-based cryptographic schemes have a potential of long-term post-quantum security, more research is required to enhance their efficiency and practical implementation in the real world systems.

4.4. Case Study Outcomes

SIKE and SIDH case studies have brought out some weaknesses and strengths. SIDH is a strong quantum resistant tool, which makes it a solution in key exchange in post-quantum cryptography. Nevertheless, its fundamental exchange period is also a challenge particularly within resource constrained settings. SIKE to the contrary, demonstrates potential in secure key encapsulation and has been optimized to run on FPGA hardware which is much faster. Nevertheless, it remains the case that both of the protocols necessitate considerable amounts of computational resources and thus their practical implementation is more complicated. Also, the two protocols provide resistance against quantum attacks; however, their use is still constrained by their performance in practical scenarios. In general, both case studies highlight the promise of isogeny based cryptography but indicate that additional optimization in terms of speed and scalability is required.

4.5. Comparative Analysis

Comparison between isogeny-based and elliptic curve-based post-quantum cryptographic designs shows that there is a major distinction in quantum resistance and computation complexity. The methods based on isogeny, like SIDH or SIKE, are better in terms of quantum resistance since they are based on problems like isogeny computation that are difficult to solve with a quantum computer. Nevertheless, they are computationally-intensive and can be feasible only with the help of hardware acceleration. By contrast, elliptic curve cryptography (ECC) is prevalent because it is an efficient algorithm, but it is susceptible to quantum algorithms like Shor. Although ECC has low resource usage and high-performance, it is ineffective in the post-quantum world. The major lesson of this comparison is that isogeny-based cryptography, although secure, requires additional optimization in its computational efficiency, in order to be applicable in the real world.

4.6. Model Comparison

The comparison of the various cryptographic models on the basis of algebraic geometry shows that they are relatively secure against quantum attacks to different extents. SIKE and SIDH are isogeny based, offering a high degree of resistance to quantum algorithms, including the one by Shor, and are therefore candidates in the field of post-quantum cryptography. These models are based on the fact that it is computationally hard to compute isogenies between elliptic curves, and this is a problem that quantum computers are unlikely to solve. Conversely, quantum algorithms are susceptible to elliptic curve-based models such as ECC that are efficient and extensively deployed. ECC remains the cryptography system of choice in most implementations despite its quantum vulnerability thanks to its light computational requirements. Nonetheless, genetically-related models are also becoming formidable competition to quantum resistance, with its security merit rendering it a very viable solution to future cryptographic standards.

4.7. Impact & Observation

Isogeny based schemes (e.g., SIDH and SIKE) have substantial practical applicability in cryptographic systems in the real world. These protocols provide strong security protection against quantum attacks, and therefore are suitable to long-term secure communication. Nonetheless, isogeny-based cryptography has a heavy computational cost, making it difficult to be widely deployed. Hardware acceleration, most notably based on FPGA, has demonstrated performance improvement, although the requirement of high computational resources can be a limiting factor to the scalability and efficiency of these protocols. Nevertheless, the possible benefits of isogeny-based cryptography are enormous, especially in those cases when post-quantum security is a primary factor. These schemes are projected to be central to the future of safe digital communications as more research and optimization is done in this field.

5. Discussion

5.1. Interpretation of Results

The findings of this paper highlight the possibility of isogeny-based cryptography in delivering quantum-resistant security. The results indicate that the protocols such as SIDH and SIKE are encouraging alternatives to the traditional protocols such as ECC, but still have a long way to go regarding their computational efficiency and practical implementation. Such isogeny-based schemes provide a high resistant against quantum attacks, since they are based on computationally hard problems even to quantum computers. Nonetheless, the paper also finds that such schemes such as FPGA acceleration have significant hardware support demands to enable satisfactory performance. This brings about the trade-off between high security and computational cost of switching to post-quantum cryptography. Finally, this paper supports the necessity of ongoing optimization work to increase the efficiency of isogeny-based cryptographic system and their implementation in secure communication systems.

5.2. Result & Discussion

These findings prove the usefulness of the isogeny based cryptographic schemes in addressing the quantum computing security issue. They however also expose the present shortcomings with respect to computational complexity and efficiency. Post-quantum cryptography presents a number of challenges, such as requiring a large amount of computing power, and scalability concerns, especially when introducing an isogeny-based protocol to a practical system. This work helps to address these difficulties by providing the understanding of the trade-offs between performance and security by demonstrating that the computational load could be lessened with the help of hardware acceleration. The research also mentions that more research must be done to optimize these cryptographic schemes, to make them more feasible with large-scale use. In general, the results indicate that isogeny-based cryptography has a potential, but it is still at its infancy and needs improvement.

5.3. Practical Implications

The implementation of isogeny and elliptic-curve-based cryptographic protocols in the protection of digital communication in the future is important in a post-quantum world. These cryptographic techniques provide a way forward to stand-off data exchange and key exchange protocols that are immune to quantum algorithms, including the Shor algorithm, which undermines conventional cryptography. Although elliptic curve cryptography (ECC) is efficient and easy to use, it is susceptible to quantum attacks, and it is advised that quantum-resistant cryptography schemes, such as SIDH and SIKE, be studied. Organizations can future-proof their communication systems by using isogenous-based cryptographic protocols, which will guarantee the privacy and security of their data against quantum attacks. Nevertheless, it is still difficult to implement in practice, requiring specialized hardware and more computing power. Still, the possibility of the long-term digital communication offered by these protocols makes them especially important in the creation of the next-generation cryptographic systems.

5.4. Challenges and Limitations

The research faced a number of difficulties, which were mostly associated with the complexity of the computation and implementation of isogeny-based cryptographic protocols. Although these protocols are very secure, they demand a lot of computation resources and therefore, they are hard to apply in resource-constrained systems. The fact that hardware acceleration is required especially with the use of FPGA serves to further complicate their usage. Also, the problem of scalability is also significant, with isogenous-based systems taking a significant amount of time and energy to handle key exchange and encryption. Although such constraints exist, the study suggests that with further attempts to streamline such systems, maybe some of these problems can be alleviated. The second obstacle is that standardization of post-quantum cryptographic protocols is required, which may require years to be fully incorporated in security systems around the world. In such a way, the way ahead will involve compromising between the security and the pragmatic efficiency in the actual environment.

5.5. Recommendations

Further study of post-quantum cryptography should be done in the future that encompasses increasing the computing power of isogeny based protocols without affecting the security. Hardware implementations, especially more efficient FPGA designs and other hardware accelerators, is one of the main points to improve. Alternatively, it can be suggested to consider other schemes that are isogenous or hybrids that integrate the advantages of several cryptography schemes, which can be more scalable. More research should also be done on how to improve the theoretical basis of isogeny-based cryptography so that it becomes simpler and more applicable in other application areas. Moreover, the focus needs to be put on the creation of strong cryptographic standards to enable the post-quantum systems, to make sure that their application is global and safe. This will play an important part as the world goes quantum resistant encryption.

6. Conclusion

6.1. Summary of Key Points

This work identifies isogeny-based and elliptic curve-based cryptographic schemes as having a major potential in the post-quantum cryptography environment. It unveils that elliptic curve cryptography (ECC) is still fast, but it can be attacked by a quantum computer, thus a promising substitute is isogeny-based cryptography, including SIDH and SIKE. The results indicate that isogeny-based protocols are very resilient to quantum algorithms but have some problems related to computational efficiency and practical implementation. The paper notes that hardware acceleration through the use of FPGA implementations is needed to enhance performance of such schemes. All in all, the study can add to the current body of research on the topic of post-quantum cryptography and indicate that isogeny-based schemes have

substantial potential in enabling secure digital communication in a quantum-enabled future, but, again, their scalability and efficiency also require optimization.

6.2. Future Directions

Future studies in post-quantum cryptography ought to consider improving the isogeny-based cryptographic protocols so that their efficiency and scalability can be improved. Areas of major exploration include optimization of hardware realizations, especially by more sophisticated FPGA and ASIC designs, to make these protocols more realistic in the real world. Additionally, combining the scheme in isogeny with the currently in use cryptographic frameworks can provide hybrid schemes that compromise security and computational efficiency. Further studies are also needed in other methods of algebraic geometry so as to come up with new cryptographic mechanisms resistant to quantum attacks. With changing quantum computing environment, there will be specific need to work out adaptive, scalable and secure cryptography systems capable of ensuring security of digital communications and data in the long run. Continued collaboration and standardization will also be necessary in the development of the implementation of these post-quantum systems around the world.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Feo, D. (2017). Mathematics of Isogeny Based Cryptography. ArXiv.org. https://arxiv.org/abs/1711.04062

[2] Kasm, N. Y., & Hamad, Z. A. (2019). Applications of algebraic geometry in cryptography. Modern Applied Science, 13(5), 130. https://doi.org/10.5539/mas.v13n5p130

[3] Koziel, B., Azarderakhsh, R., Mozaffari Kermani, M., & Jao, D. (2017). Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(1), 86-99. https://doi.org/10.1109/TCSI.2016.2611561

[4] Koziel, B., Ackie, A.-B., Khatib, R. E., Azarderakhsh, R., & Kermani, M. M. (2020). SIKE'd Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation. IEEE Transactions on Circuits and Systems I: Regular Papers, 67(12), 4842-4854. https://doi.org/10.1109/TCSI.2020.2992747

[5] Kumar, M., & Pattnaik, P. (2020). Post Quantum Cryptography (PQC) - An overview: (Invited Paper). 2020 IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA, 1-9. https://doi.org/10.1109/HPEC43674.2020.9286147

[6] Mavroeidis, V., Vishi, K., D., M., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. International Journal of Advanced Computer Science and Applications, 9(3). https://doi.org/10.14569/ijacsa.2018.090354

[7] Weger, V., Gassner, N., & Rosenthal, J. (2022). A Survey on Code-Based Cryptography. ArXiv (Cornell University). https://doi.org/10.48550/arxiv.2201.07119

[8] Xuan, J., Lu, J., & Zhang, G. (2020). A Survey on Bayesian Nonparametric Learning. ACM Computing Surveys, 52(1), 1-36. https://doi.org/10.1145/3291044

[9] Yan, Y. (2022). The Overview of Elliptic Curve Cryptography (ECC). Journal of Physics: Conference Series, 2386(1), 012019. https://doi.org/10.1088/1742-6596/2386/1/012019