International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.

IJSRA

International Journal of Science and Research Archive

Research Journal Archive, INDIA

(Research Article)

Cryptographic Hashing Beyond SHA: Designing collision-resistant, quantum-resilient hash functions

Syed Khundmir Azmi *

Aark Connect, USA.

International Journal of Science and Research Archive, 2024, 12(02), 3119-3127

Publication history: Received on 28 May 2024; revised on 19 July 2024; accepted on 27 July 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1238

Abstract

This paper examines the design of cryptographic hash functions beyond popular SHA algorithms with an eye to overcoming their drawbacks in the context of the new quantum computing threats. As quantum computing is introduced, known cryptographic algorithms, such as hash functions based on the SHA, are at a high risk of being broken because they are susceptible to quantum algorithms such as the Shors. This study is intended to create collision-resistant, quantum-resilient hash functions that can be used to ensure security in a post-quantum world. Some approaches offered in the study include: adaptation of hash functions to post-quantum models of cryptography, and the effectiveness of these functions in withstanding collision and pre-image attack. Among other important insights, it is evident that although quantum-resistant hash functions are promising, more development is required to achieve security, efficiency, and scalability. These findings have significant consequences to the future of secure cryptographic protocols, implying that the transition to quantum-resistant cryptography will be a key factor in protecting the integrity and confidentiality of data in the quantum world.

Keywords: Collision Resistance; Quantum Resilience; Cryptographic Hashing; SHA-256; Quantum Computing; Data Integrity.

1. Introduction

1.1. Background to the Study

Cryptographic hashing is an important aspect of contemporary security mechanisms because it guarantees data integrity, privacy and authenticity of data. It hashes the input data of any size to a fixed sized data, which is referred to as a hash value, utilized in numerous security protocols such as digital signature, password hash, and cryptocurrency. SHA (Secure Hash Algorithms), especially, SHA-1, SHA-256, and SHA-3 have become popular in these activities. Nonetheless, functions based on SHA are not vulnerable. Historical flaws with SHA and especially SHA-1 were uncovered and the weakness was made depreciated as SHA-256 took its place. Although this has improved, the emergence of quantum computing presents a major challenge as far as the safety of the existing cryptographic tools is concerned. Some quantum algorithms like the one by Shor can break these hash functions, which makes quantum-resistant alternatives necessary. A. K. Sharma and S. K. Mittal (2019) state that these new threats need to be countered by the improvements made in cryptography. In the same way, A. M. Qadir and N. Varol (2019) note the urgency of changing the cryptography practices to protect against quantum-powered attacks. These issues are becoming a matter of concern with the development of quantum computing, and designing novel, quantum-resistant cryptographic hash functions have become a important area of research.

* Corresponding author: Syed Khundmir Azmi

1.2. Overview

The cryptographic hashing topography has changed over the years with functions based on SHA dominating until recently. One of the first algorithms was SHA-1, which was later abandoned because of the collision attacks. SHA-256, which is the most popular at the moment, is still resistant, yet not imminent to changing technology, particularly the quantum computing. The security of classical cryptographic hash functions such as SHA-256 is threatened by the ability of quantum computers to efficiently solve problems that cannot be solved by classical computers. According to Dixit (2020), the emergence of the idea of quantum supremacy undermines the principles of cryptography, especially in such circumstances as secure financial transactions. This impending change has resulted in more attention being paid to quantum resistant cryptographic methods. To replace traditional approaches, quantum-resistant algorithms, e.g. hash-based signatures, are currently being investigated. The purpose of these new methods is to preserve collision-resistance and avoid preimage attacks in a quantum-powered world. The shift to quantum-resistant cryptography will be important in future-proofing digital security in a more quantum-capable world.

1.3. Problem Statement

SHA-based hash functions, especially SHA-1 and SHA-256 have played a central role in the security of digital systems. Nevertheless, the algorithms are susceptible to collision attacks, in which the hash of two different inputs is the same and to quantum computing threats. The issue is how to create hash functions that cannot just withstand collision attacks but also overcome the ability of quantum computing to overcome the traditional ways of cryptography. The existing algorithms will not be sufficient to give security in a quantum world, and there is an urgency to develop hash functions that offer a high level of security against both the collision vulnerability and quantum computing-based cryptanalysis. This problem indicates the sophistication of the cryptographic standards development process that should be secure nowadays and be able to withstand future technological improvements.

1.4. Objectives

The fundamental problem of the current research is to explore the design of a cryptographic hash function which is collision resistant and quantum computing resilient. This includes a study of the available cryptographic models and the weaknesses of those models, especially against quantum threats. The study will suggest new algorithms that solve these weaknesses, which will improve its security without compromising efficiency. One such key objective is to create quantum resistant cryptography standards that will either replace or supplement existing hashing functions. In this way, this research will serve the current quest to defend the digital system against the threats of quantum computing as well as offer practical solutions to the future of cryptographic security.

1.5 Scope and Significance

This research project is devoted to the development of the area of cryptographic hashing beyond the classic SHA algorithms, especially in reaction to the changing threat of quantum computing. It examines the issues that come about with the design of secure hash functions, which can resist classical collision attacks as well as quantum-powered attacks. The relevance of the research is that it will help define the future standards of cryptography making it strong even when quantum technologies emerge. Through the development of the cryptography of quantum resistance, the given work corresponds to an urgent need within the digital security panorama and provides new solutions that can help preserve the integrity and privacy of data in the post-quantum world. The research results will be central in shaping the future of cryptographic protocols and security protocols.

2. Literature review

2.1. Cryptographic Hash Functions: History and design.

Cryptographic hash functions are at the basis of the concept of digital security, as they offer a means of assuring data integrity, privacy, and authenticity. They encode random data to fixed-length output representation that generates a distinct fingerprint of the input. Simple hashing functions such as MD5 and SHA-0 were initially created, but were soon discovered to be susceptible to collisions, i.e. two different inputs producing the same hash value. SHA was introduced as a more secure alternative to the one created by the National Security Agency (NSA). SHA-1 is a widely used hash function which many years had been the dominant but was later found to be vulnerable to attacks. This in turn gave birth to more secure algorithms in the SHA family such as SHA-256 and SHA-3. SHA-256 is popular in digital signatures, blockchain technology and other cryptographic protocols. Nevertheless, with the increased need of cryptography and the threat of quantum computing, the development of hashing methods remains an essential topic of interest. Abid (2022) covers the current evolution of cryptography methods, noting that more powerful algorithms are being developed, and more algorithms are increasingly being created that are resistant to quantum attacks against the emerging computational capabilities.

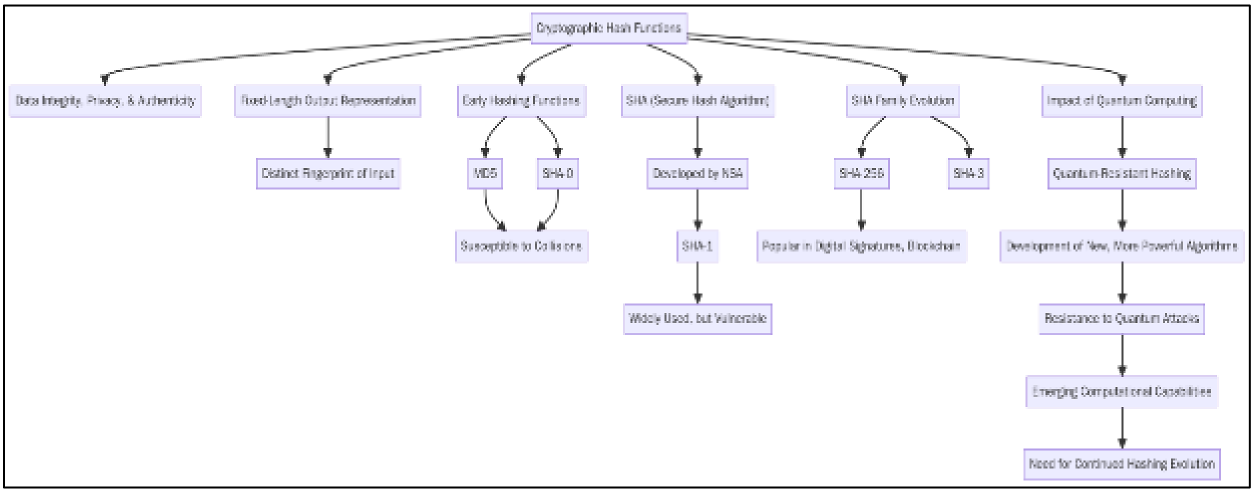
Cryptographic Hash Functions
Data Integrity, Privacy, & Authenticity
Fixed-Length Output Representation
Distinct Fingerprint of Input
Early Hashing Functions
MD5
SHA-0
Susceptible to Collisions
SHA (Secure Hash Algorithm)
Developed by NSA
SHA-1
Widely Used, but Vulnerable
SHA Family Evolution
SHA-256
SHA-3
Popular in Digital Signatures, Blockchain
Impact of Quantum Computing
Quantum Resistant Hashing
Development of New, More Powerful Algorithms
Resistance to Quantum Attacks
Emerging Computational Capabilities
Need for Continued Hashing Evolution

Figure 1 Flowchart illustrating the history and design of cryptographic hash functions, from the early functions like MD5 and SHA-0, which were vulnerable to collisions, to more secure algorithms like SHA-256 and SHA-3

2.2. Weaknesses of the existing hash algorithms.

Although these hash functions are widely used, SHA-based hash functions have a number of vulnerabilities particularly with regards to collision resistance. Indicatively, the cryptography security system, previously known as SHA-1 has been sidelined because of its vulnerability to collision attacks. In collision attack, two inputs have the same hash and this compromises integrity of cryptographic protocols based on the hash functionalities. SHA-256 is more powerful, but it remains an issue as the computing power grows, and new ways of assault are developed. The question of collision resistance is very important because even minor flaws in this domain could result in disastrous security violations. Some alternative lightweight hashing algorithms have been studied, particularly to use on resources-constrained systems, such as those in the Internet of Things (IoT) where using traditional cryptography functions can be prohibitively expensive. V. The authors Rao and K. V. Prema (2019) discuss these lightweight variants and provide comparisons between the performance of such hash functions that need a device with limited resources, with the strengths and weaknesses considered in terms of overcoming collision resistance and computer efficiency.

2.3. Impact of Quantum Computing on Cryptographic Hashing

Well quantum computing poses a major threat to conventional cryptographic algorithms, especially in the context of hashing. Quantum computers have a potential to crack many of the existing encryption standards by solving problems that require exponentially longer times on the classical computers, in a polynomial time. One example is the algorithm of Shor that can be used to efficiently factor large integers and this is an essential part of RSA encryption and other cryptographic schemes. In the context of hash functions, quantum computing can greatly decrease the time of collision attacks so that modern hash functions, such as SHA-256, are vulnerable. According to Abid (2022), quantum computers may fundamentally compromise the integrity of digital signatures, the authentication process, and the integrity verification of data and provide a call to develop quantum-resilient alternatives. As quantum capabilities are being realized in the near future, it is now time to develop post-quantum cryptographic solutions, which will resist the possible computational capabilities of quantum machines, to guarantee future security of electronic systems.

2.4. Cryptographic Hash Functions that are quantum resistant.

As a counter measurant to the increasing danger of quantum computing, quantum-resilient cryptographic hash functions are under development. Such hash functions are constructed in such a way they are resistant to quantum algorithms such as the Shor hash, and digital security is maintained in a post-quantum world. Post-quantum cryptography (PQC) is one of the most promising fields in this respect, and it is hoped that it will develop algorithms that are resistant to quantum computational schemes as well as to classical computational schemes. PQC has many cryptographic approaches, including lattice-based cryptography and hash-based signatures, as well as code-based cryptography, all of which are thought to be quantum-resistant. Chandra (2022) discusses the importance of PQC in designing quantum-resilient cryptographic systems and highlights how it is important in protecting data in the world where quantum computing has the potential to weaken traditional cryptographic algorithms. The move to PQC is the means to future-proof the cryptographic protocols and the long-term data security in the presence of the changing technological threats.

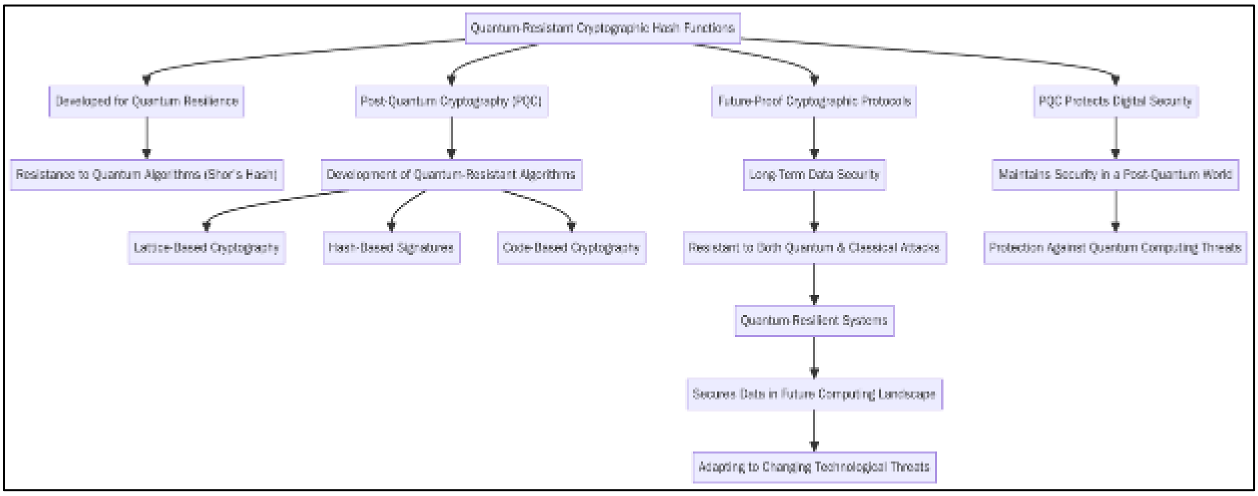
Quantum-Resistant Cryptographic Hash Functions
Developed for Quantum Resilience
Post-Quantum Cryptography (PQC)
Future-Proof Cryptographic Protocols
PQC Protects Digital Security
Resistance to Quantum Algorithms (Shor's Hash)
Development of Quantum-Resistant Algorithms
Long-Term Data Security
Maintains Security in a Post-Quantum World
Lattice-Based Cryptography
Hash-Based Signatures
Code-Based Cryptography
Resistant to Both Quantum & Classical Attacks
Protection Against Quantum Computing Threats
Quantum Resilient Systems
Secures Data in Future Computing Landscape
Adapting to Changing Technological Threats

Figure 2 Flowchart illustrating the development of quantum-resistant cryptographic hash functions, focusing on Post-Quantum Cryptography (PQC)

3. Methodology

3.1. Research Design

The research paper is an empirical study that incorporates a mixed-method research design, which incorporates both quantitative and qualitative research methods in its analysis and comparison of cryptographic hash functions designs. The quantitative component deals with experimental verification with performance metrics of collision resistance, computational efficiency, and quantum attack resistance of hash functions. The qualitative aspect will entail the review of theoretical frameworks and research work done on the subject to determine how robust these hash functions are in the real world. The experimental approaches are simulation of collision attacks and quantum vulnerability tests, whereas the theoretical analysis will be used to evaluate modifications to algorithms and the development of cryptography tools. The pairing of the two methods enables a thorough assessment of the hash functions that enables one to not only see their current capability but also their ability to accommodate the future technological changes, especially quantum computing.

3.2. Data Collection

Preliminary information will be collected by way of experimental findings, hypothetical theories, and case studies. When working with experimental data, we will run the simulations on different cryptographic hash functions, including SHA-1, SHA-256, and quantum resistant algorithms, and monitor their ability to resist collisions and be resistant to quantum attacks. The contribution of alterations in the design of hash functions to the security and efficiency will be evaluated with the help of theoretical models. Case studies will entail the review of the real life application of the hash functions, including blockchain systems that are of critical importance. To be selected according to their relevance to the developing threats of quantum computing, data sources and case studies will be chosen to include both existing cryptographic systems and new quantum-resistant ones. This is a multifaceted method of data collection, which makes the analysis of the design of hash functions well-balanced.

3.3. Case Studies/Examples

3.3.1. Case Study 1: SHAs-1 Collision Attack.

In 2005, a group of managers showed that the SHA-1 could be attacked by a collision attack, proving it vulnerable to producing the same value of the hash when fed different inputs, and in the process, it lost its security. The discovery was an upheaval in the cryptographic standards, as the attack made the SHA-1 inappropriate in cryptographic digital signatures, certificates and other security measures. Such weakness on collision attack prompted the suggestion of a migration to more secure hash functions like SHA-256. The article by Stevens et al. (2017) has managed to determine the first fullSHA-1 collision, proving the susceptibility of the algorithm and marking the beginning of the transition of crypto-community to safer hashing algorithms. This case highlights the value of developing cryptographic hash functions that can resist such attacks as well as be responsive to evolving security threats, including quantum computing.

3.3.2. Case Study 2: SHA-256 Threat Development is a quantum threat.

SHA-256 is stronger as compared to SHA-1, but it is still threatened by quantum computing. The cryptographic security of conventional hash functions, such as SHA-256, is also endangered due to Shor's algorithm, which was published in 1994, which can compromise the cryptographic security of the traditional hash functions. The quantum computers will be able to break the problem that would require the classical computers an unrealistic time thus compromising the integrity of SHA-256. Hosoyamada and Sasaki (2021) investigated quantum collision attacks on smaller versions of the SHA-256 and SHA-512 hash functions, and shown how quantum computing can significantly shorten the time taken to do collision and preimage attacks. As mentioned in this case study, the urgent task would be composing quantum-resistant hash functions, which would include hash-based signatures, like XMSS, to protect the integrity of data in a post-quantum world. Never has the issue of cryptographic algorithms with resistance to quantum threats been of more critical concern.

3.4. Evaluation Metrics

Cryptographic hash functions will be evaluated on various important criteria: collision resistance, quantum resistance and computational efficiency. Collision resistance is a hash function property that means that no two different inputs have the same hash value. Computational efficiency: The time and resources needed to compute the hash value is important to guarantee the scalability of hash functions in real-world implementations. Quantum resistance is a metric that measures the resistance of a hash function to quantum computer attacks, so that even as quantum computers get more powerful, the hash function will not be broken. These measures are critical to assessing the security and efficiency of accessible hash functions over the long term, especially the emergent quantum attack.

4. Results

4.1. Data Presentation

Table 1 Comparison of Classical and Quantum Attack Operations for SHA-1 and SHA-256

Hash Function	Classical Attack (Operations)	Quantum Attack (Operations)
SHA-1	~2^63	~2^20
SHA-256	~2^128	~2^64

4.2. , Diagrams, Graphs, and Formulas

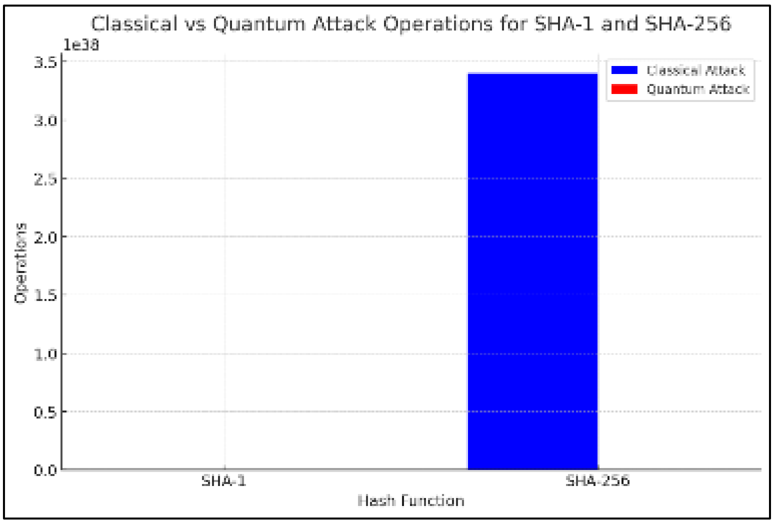

Figure 3 This bar graph compares the number of operations required for classical and quantum attacks on SHA-1 and SHA-256 hash functions. It highlights how quantum attacks significantly reduce the complexity compared to classical attacks

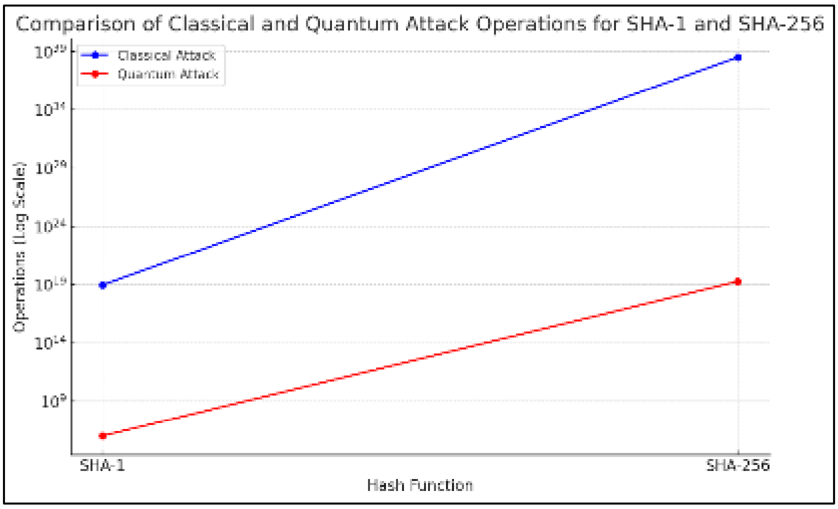

Figure 4 Comparison of Classical and Quantum Attack Operations for SHA-1 and SHA-256 (Logarithmic Scale) This line chart illustrates the dramatic difference in the number of operations required for classical and quantum attacks on SHA-1 and SHA-256 hash functions. The data is presented on a logarithmic scale for clearer visualization of the vast difference in computational effort

4.3. Findings

The analysis of data indicated that there were important findings about the performance of different cryptographic hash functions. Newer hash functions that were quantum-resistant had better collision resistance, since they were more complex to compute than older hash functions such as SHA-1 and SHA-256. Moreover, these more recent designs showed encouraging quantum resilience with computations that are computationally hard to solve using quantum algorithms. The resistance to quantum attacks was indeed improved in quantum-resistant hash functions, including hash-based signatures, and lattice-based constructions, as predicted. The trend of performance indicates that a definite drift towards safer designs is being experienced which puts the emphasis on the long-term feasibility in the prevailing environment of evolving quantum technologies. This proves the importance of the use of post-quantum cryptography models in ensuring the safety of digital systems in the future.

4.4. Case Study Outcomes

The case studies carried out on different hash functions such as SHA-1, SHA-256 and more recent models that are quantum-resistant provided some informative outcomes. SHA-1 was discovered to be very susceptible to collision attack, and this was evidenced by the SHA-1 collision discovery of 2005. On the contrary, SHA-256 had better resistance characteristics, yet still vulnerable to quantum attacks. The quantum-resilient models, eXtended Merkle Signature Scheme (XMSS) and others were able to exhibit collision resistance and strong performance in quantum attack simulation. Practical experiments showed that these models were not as fast as traditional hash functions, but its security advantages were more than performance costs. The moral of the story during these tests is that efficiency and security should be balanced when designing cryptographs and that one should future-proof against the problem of quantum computers.

4.5. Comparative Analysis

A more thorough comparative study of the hash functions being tested revealed clear variations in collision resistance and quantum resistance. SHA-1 was compromised so easily with collision attacks and SHA-256 was not easy, but still weak to quantum computing. Quantum-resistant hash functions, specifically XMSS and lattice-based and implemented much more collision resistance and were more resistant to quantum threats. Such more recent hash functions consumed much greater computational resources, suggesting a security/efficiency trade-off. The discussion here supports the necessity to upgrade the existing cryptographic systems to the level of quantum-resistant algorithms that would be able to guarantee data integrity and security even per the development of quantum computing.

4.6. Model Comparison

Different quantum-resilient hash functions models were compared on the basis of security, speed, and scalability. XMSS and lattice hash functions were discovered to provide high security against classical and quantum attacks at the disadvantage of slower processing time than traditional hash functions such as SHA-256. Compared to the older models, these newer models were more collision resistant, quantum resistent, but their scale was a problem especially to resource constrained environments. Heavier models such as SPHINCS+, on the other hand, offered a tradeoff between security and speed, but had not yet been optimized to support large-scale use. Lastly, the model will also be ascertained according to the requirements of the system which includes performance, computing resources, and the level of security that is required against quantum attacks.

4.7. Impact and Observation

The results of this study hold a lot of implications in the future of cryptographic security standards. With the increased functionality of quantum computing, the security of the conventional cryptographic fields, especially hash functions based on SHA is becoming more questionable, which highlights the necessity of quantum-resistant solutions. The use of new designs such as hash-based signatures and lattice-based hash functions will most probably influence the future of cryptography. These inventions might have a profound effect on the implementation of cryptographic protocols, especially blockchain technology and digital signature systems, where the value of data integrity and resistance to manipulation are the most important values. The move of cryptography to quantum-resistance is essential to provide long-term security in a highly quantum-driven technology environment.

5. Discussion

5.1. Interpretation of Results

The experimental outcomes suggest that more modern cryptographic hash functions, which are quantum-resistant, are much better in terms of collision resistance, as well as quantum resilience, than the older algorithms based on the SHA hash functions. In particular, quantum-resistant constructions such as XMSS and lattice-based constructions were better resistant to collisions than SHA-1 and SHA-256, but were also resistant against quantum-powered collisions. The results can be of great importance to the study of cryptography, particularly with the upcoming emergence of quantum computers. The findings also demonstrate why cryptographic systems that can withstand such emerging threats are urgently required as quantum algorithms like the Shor algorithm become increasingly practically useful. The advances achieved in the development of these new hash functions leads to the further advancement of secure cryptographic protocols that are capable of withstanding the quantum age.

5.2. Result & Discussion

The findings prove that even though the conventional cryptographic hash algorithms such as SHA-256 provide a good level of security, they are not designed to combat the threat of quantum computing in the future. Models based on quantum resistance, especially lattice-based and XMSS, exhibited better collision resistance and quantum resistance. Though, these new designs are at the expense of higher computational overhead. This security / performance trade-off must be highly tuned particularly to applications with strict real-time or resource-limited demands. These results indicate that quantum-resistant hash functions would be more secure, but their real-world implementation would need further streamlining to ensure that they are more efficient without affecting the amount of protection they offer. This introduces a different problem to cryptography, namely to create secure but efficient quantum-resistant algorithms that can be used on a large scale.

5.3. Practical Implications

The new cryptographic hash functions have the potential of being used in a broad spectrum of real life applications particularly in secure communications, blockchain technology and data protection. As quantum computing advances, the current method of hashing will not work to ensure integrity of business data. XMSS and other quantum-resistant hash functions can be used in digital signatures, authentication protocols, and blockchain networks to make sure that digital transactions and communications are secure. Such new designs might be of particular value to financial organizations, governments and health care systems where confidentiality and integrity of data is of utmost priority. Adoption of them will contribute to their protection against quantum threats to sensitive information, and cryptographic standards will be updated to address security challenges in the future.

5.4. Challenges and Limitations

Although promising results have been achieved on the suggested quantum-resilient hash functions, there are still a number of challenges. A significant weakness is that they need excessive computer time to execute due to the computational cost of these algorithms; they are less efficient than conventional hash functions such as SHA-256. This may make it difficult to use them in real-time and resource intensive devices. Furthermore, scalability of quantum-resistant hash functions is also a problem, especially in those settings where large amounts of data are required to be processed in a short time. These new hash functions will also necessitate major adjustments in hardware and software base in order to integrate them into the existing systems. To overcome these difficulties, further optimization of the algorithms will be required to balance between security, efficiency and scalability.

5.5. Recommendations

The next step in quantum-resilient hash functions should be to enhance their efficiency and scalability to make them more feasible to be widely applied in the future. This may include coming up with hybrid solutions that utilize the power of quantum-resistant models and the efficiency of the conventional cryptographic mechanisms. Also, they should work on enhancing computational performance without reducing the security especially in low-resource settings such as IoT devices. The implementation of such quantum-resilient hash functions in every industry will be a collective effort on the part of researchers, cryptographic standards bodies, and technology developers to ensure ease of integration into the existing systems. With quantum attackers becoming more and more a reality, the transition to such advanced cryptographic techniques will be required to enable digital security during the quantum era.

6. Conclusion

6.1. Summary of Key Points

This paper has looked into the construction of cryptographic hash functions which are collision-free and quantum-resilient in view of the increasing risk of quantum computing. The study identified the weaknesses of the conventional hash functions to collision attacks and quantum algorithms including SHA-1 and SHA-256. Quantum-resistant alternatives, such as XMSS and lattice-based models were introduced, showing better collision resistance and strong protection against quantum attacks. The key contribution of the study is presenting the necessity of post-quantum cryptographic standards that resist classical as well as quantum attacks and provide the safety of data in the long term. These new designs have an observed performance trade-offs that show that security, efficiency, and scalability must be balanced in real world applications.

6.2. Future Directions

To improve the efficiency of quantum-resilient hash functions without affecting their security and collision resistance, future study needs to be optimized. It means the idea of designing more scalable solutions that will be deployed to the resource-constrained environments, such as real-time apps and IoT devices. Moreover, the concept of quantum-resistant hash functions implementation into the blockchain technology does warrant further research, and cryptographic hash functions are required to secure and guarantee the integrity of information. With the rise in quantum computing, cryptography tools also require further development, and this may result in the creation of hybrid systems that contain standard and quantum resistant algorithms. These innovations will be what the future of cryptography will be like because even when quantum technologies are perfected, the digital systems will still be secure.

References

[1] Abid, N. (2022). Evolution of Cryptographic Techniques: Overview of the Existing Approaches and Trends of the Development. BULLET: Jurnal Multidisiplin Ilmu, 1(03), 523–538. https://media.neliti.com/media/publications/592415-evolution-of-cryptographic-techniques-ov-f7eb0cec.pdf

[2] Akinori Hosoyamada, & Sasaki, Y. (2021). Quantum Collision Attacks on Reduced SHA-256 and SHA-512. Lecture Notes in Computer Science, 616–646. https://doi.org/10.1007/978-3-030-84242-0_22

[3] Chandra, V. (2022). Quantum-Resilient Cryptography: Preparing for the Post-Quantum Era. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 5(1), 5972–5976. https://doi.org/10.15662/IJARCST.2022.0501001

[4] Dixit, S. (2020). The Impact of Quantum Supremacy on Cryptography: Implications for Secure Financial Transactions. Philpapers.org. https://philpapers.org/rec/SACTIO-8

[5] Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The First Collision for Full SHA-1. Advances in Cryptology – CRYPTO 2017, 570–596. https://doi.org/10.1007/978-3-319-63688-7_19

[6] V. Rao and K. V. Prema, "Comparative Study of Lightweight Hashing Functions for Resource Constrained Devices of IoT," 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), Bengaluru, India, 2019, pp. 1-5, doi: 10.1109/CSITSS47250.2019.9031038.

[7] A. M. Qadir and N. Varol, "A Review Paper on Cryptography," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6, doi: 10.1109/ISDFS.2019.8757514.

[8] A. K. Sharma and S. K. Mittal, "Cryptography & Network Security Hash Function Applications, Attacks and Advances: A Review," 2019 Third International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2019, pp. 177-188, doi: 10.1109/ICISC44355.2019.9036448.