Review of SHA-3 for Post-Quantum Cryptographic Applications

[1]Dr. Rajeev Kumar Thakur, [2]Rajnish Sharma
[1]Associate Professor, [2]Research Scholar,
Department of Electronics and Communication Engineering,
NRI Institute of Information Science and Technology, Bhopal, India

Abstract— **This review presents a comprehensive analysis of the Secure Hash Algorithm-3 (SHA-3) and its suitability for post-quantum cryptographic applications. As quantum computing poses significant threats to classical public-key cryptosystems, cryptographic hash functions such as SHA-3 are gaining renewed importance due to their inherent resistance to quantum attacks like Grover's algorithm. The paper examines the design principles of SHA-3 based on the Keccak sponge construction, highlighting its structural advantages, security strength, and flexibility compared to earlier hash standards. Key performance metrics, including collision resistance, preimage resistance, and implementation efficiency in hardware and software environments, are critically reviewed. Furthermore, the role of SHA-3 in post-quantum security frameworks, digital signatures, authentication protocols, and blockchain systems is discussed. The review concludes that SHA-3 remains a robust and future-ready cryptographic primitive, making it a vital component in building secure post-quantum cryptographic solutions.**

Keywords*— *SHA-3, Post-Quantum Cryptography, Keccak, Hash Function, Quantum Resistance, Cryptographic Security.

I. INTRODUCTION

The The rapid advancement of quantum computing has introduced a paradigm shift in the field of information security, raising serious concerns about the long-term reliability of conventional cryptographic algorithms. Classical cryptographic systems, which currently secure digital communication, financial transactions, cloud storage, and critical infrastructure, are largely built on mathematical problems such as integer factorization and discrete logarithms[1]. Algorithms like RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC) derive their security from the computational difficulty of these problems for classical computers. However, with the advent of large-scale quantum computers, these assumptions are no longer guaranteed[2]. Quantum algorithms such as Shor's algorithm can efficiently break RSA and ECC, while Grover's algorithm can significantly reduce the effective security of symmetric cryptographic primitives. This emerging threat has led to the development of Post-Quantum Cryptography (PQC), which focuses on designing cryptographic algorithms that remain secure against both classical and quantum adversaries[3].

Within the post-quantum landscape, symmetric cryptographic algorithms and cryptographic hash functions play a crucial role. Unlike public-key cryptosystems, symmetric algorithms are not completely broken by quantum attacks; instead, their security is weakened by a quadratic speed-up provided by Grover's algorithm[4]. As a result, increasing key sizes and output lengths can effectively restore security margins. Advanced Encryption Standard (AES), for instance, is still considered quantum-resistant when used with larger key sizes such as AES-256[5]. Similarly, cryptographic hash functions retain their structural security properties under quantum threats, making them fundamental building blocks for post-quantum secure systems. Hash functions are extensively used in digital signatures, message authentication codes, password protection, key derivation functions, and blockchain technologies, all of which must remain secure in a quantum-enabled future[6].

Secure Hash Algorithms (SHA) form one of the most important families of cryptographic hash functions standardized for global use. Earlier members of the SHA family, including SHA-1 and SHA-2, have been widely deployed in security protocols such as

SSL/TLS, IPsec, and secure email systems[7]. However, vulnerabilities discovered in SHA-1 and the theoretical concerns surrounding the Merkle–Damgård construction motivated the development of SHA-3. SHA-3, based on the Keccak sponge construction, represents a fundamentally different design philosophy, offering improved security assurance, flexibility in output length, and resistance to a wide range of cryptanalytic attacks[8]. These characteristics make SHA-3 particularly relevant in post-quantum cryptographic applications, where robustness, adaptability, and long-term security are critical.

The integration of SHA-3 and other quantum-resistant security algorithms is becoming increasingly important in modern cryptographic protocols and emerging technologies. In blockchain systems, hash functions provide immutability, integrity, and consensus security, while in Internet of Things (IoT) and embedded systems, lightweight yet secure primitives are required to operate under strict resource constraints. Post-quantum secure architectures must therefore balance security strength, computational efficiency, energy consumption, and implementation feasibility. SHA-3's sponge-based architecture supports such requirements by enabling parallelism, domain separation, and customizable security parameters[9].

The transition to post-quantum cryptographic applications necessitates a comprehensive re-evaluation of existing security algorithms and the adoption of quantum-resilient alternatives. Secure Hash Algorithms, particularly SHA-3, along with symmetric encryption schemes and emerging post-quantum primitives, form the backbone of future-proof security systems. Understanding their design principles, security guarantees, and practical deployment challenges is essential for developing cryptographic infrastructures capable of withstanding the threats posed by quantum computing while ensuring confidentiality, integrity, and authenticity in next-generation digital environments[10].

II. LITERATURE SURVEY

Imran et al., [1] presented a high-speed hardware-oriented design approach for post-quantum cryptographic systems with a focus on optimized hashing and multiplication units. The work emphasized reducing latency while maintaining strong security guarantees against quantum-enabled adversaries. By integrating efficient arithmetic units with optimized hash computation, the proposed architecture achieved significant throughput improvements. The authors demonstrated that careful circuit-level optimizations can greatly enhance performance for PQC workloads. Experimental results showed reduced critical path delay and improved energy efficiency. The study is highly relevant for real-time post-quantum secure systems. It highlights the importance of SHA-based hashing in next-generation cryptographic hardware.

Guitouni et al., [2] presented an innovative hardware implementation of SHA-3 using three-dimensional cellular automata. The design aimed to enhance diffusion and non-linearity properties while improving computational efficiency. The proposed architecture reduced hardware complexity and improved parallelism compared to conventional SHA-3 implementations. Simulation results confirmed better performance in terms of speed and area utilization. The authors also discussed cryptographic robustness against known attacks. This approach is suitable for secure embedded and post-quantum systems. The work demonstrates the adaptability of SHA-3 to novel hardware paradigms.

Baird et al., [3] evaluated the energy consumption of SHA-256 and SHA-3 when deployed in resource-constrained IoT devices. The study provided a comparative analysis focusing on power, execution time, and memory usage. Results showed that SHA-3 can offer competitive energy efficiency when properly optimized. The authors highlighted the trade-offs between security strength and energy cost. The work is significant for post-quantum IoT environments where long-term security is essential. It supports the feasibility of SHA-3 in low-power applications. The findings guide designers in selecting suitable hash functions for constrained devices.

Huynh, [4] a system-level SHA-3 accelerator specifically designed for IoT authentication applications. The architecture focused on balancing performance, area, and power consumption. By employing pipelining and parallel processing, the accelerator achieved high throughput. The study demonstrated improved authentication latency compared to software-based implementations. Security analysis confirmed compliance with SHA-3 standards. The proposed solution is suitable for scalable IoT ecosystems. This work reinforces SHA-3 as a strong candidate for post-quantum authentication mechanisms.

Dolmeta et al., [5] conducted a comparative study of Keccak-based SHA-3 implementations on FPGA and ASIC platforms. The authors analyzed performance metrics such as throughput, area, and power consumption. Results indicated that ASIC implementations offer superior energy efficiency, while FPGA solutions provide flexibility. The study highlighted design trade-offs for different deployment scenarios. The work is valuable for selecting platforms in post-quantum secure hardware. It also provides practical insights into SHA-3 implementation challenges. The findings aid designers in optimizing cryptographic accelerators.

Annapurna et al., [6] introduced a true random number generator integrated with SHA-3 for secure hardware systems. The proposed TRNG enhanced entropy generation and resistance to prediction attacks. SHA-3 was used to strengthen randomness post-processing. Experimental validation confirmed high-quality random outputs suitable for cryptographic use. The design supports secure key generation in post-quantum environments. The work emphasizes the role of SHA-3 beyond hashing. It contributes to building trust in hardware security primitives.

Torres-Alvarado et al., [7] presented a fault-tolerant SHA-3 hardware architecture using modular redundancy. The design aimed to protect IoT devices against hardware failures and fault injection attacks. Redundant modules ensured correct hash computation even under fault conditions. The authors demonstrated improved reliability with minimal overhead. Security evaluation showed enhanced resilience for critical applications. The architecture is suitable for safety-critical and post-quantum systems. This work highlights reliability as a key aspect of cryptographic hardware design.

Lee et al., [8] presented a low-power VLSI implementation of Keccak-based SHA-3 for password authentication in IoT devices. The design focused on minimizing power consumption while maintaining security strength. Circuit-level optimizations reduced switching activity and leakage power. Performance evaluation showed efficient operation in constrained environments. The implementation supports secure user authentication. The study confirms the practicality of SHA-3 in low-energy systems. It aligns well with post-quantum security requirements for IoT.

Tran et al., [9] a high-performance SHA-256 accelerator targeting Society 5.0 applications. The architecture employed multi-memory and pipeline techniques to enhance throughput. Although focused on SHA-256, the work provides insights applicable to SHA-3 designs. The accelerator achieved superior performance compared to existing implementations. Energy efficiency was also improved through architectural optimization. The study highlights the continued relevance of hash acceleration. It offers design lessons for post-quantum cryptographic hardware.

Zhang et al., [10] introduced a full-pipeline message scheduling design for SHA-2 implementations. The proposed approach significantly improved processing speed and resource utilization. The authors addressed bottlenecks in traditional pipeline structures. Experimental results showed higher throughput with reduced latency. Although SHA-2 based, the methodology is extendable to SHA-3 architectures. The work contributes to efficient hash function hardware design. It supports scalable cryptographic systems in future security frameworks.

Bhattacharjee et al., [11] explored in-memory computing techniques for SHA-2 using ReRAM technology. The proposed design reduced data movement and improved energy efficiency. The authors demonstrated faster hash computation compared to conventional architectures. The approach is promising for edge and embedded security applications. While focused on SHA-2, the concept can be adapted for SHA-3. The work highlights emerging memory-centric security designs. It is relevant for post-quantum hardware acceleration.

Kundi et al., [12] presented a shared cryptographic coprocessor supporting AES encryption/decryption and SHA-3 hashing. The design aimed to reduce hardware cost through resource sharing. Performance evaluation showed efficient operation with minimal overhead. The coprocessor is suitable for secure embedded and IoT devices. The integration of SHA-3 enhances quantum resistance. The work demonstrates practical multi-algorithm security architectures. It supports the deployment of post-quantum-ready cryptographic systems.

Table 1: Summary of literature review

Sr. No.	First Author (Year)	Work (Title)	Outcome
1	Imran (2024)	High-Speed Design of Post Quantum Cryptography With Optimized Hashing and Multiplication	Achieved high-throughput and low-latency PQC hardware using optimized hashing and arithmetic units.
2	Guitouni (2025)	Efficient Hardware Implementation of SHA-3 Using 3D Cellular Automata	Improved SHA-3 performance and parallelism with reduced hardware complexity.
3	Baird (2025)	Energy Costs of SHA-256 and SHA-3 in Resource-Constrained IoT Devices	Demonstrated SHA-3 as energy-efficient and feasible for low-power IoT systems.
4	Huynh (2023)	System-Level SHA-3 Accelerator for IoT Authentication	Delivered high-speed authentication with balanced power and area efficiency.
5	Dolmeta (2023)	Comparative Study of Keccak SHA-3 on FPGA and ASIC Platforms	Identified trade-offs between FPGA flexibility and ASIC energy efficiency.
6	Annapurna (2022)	TRNG with SHA-3 for Secure Hardware Systems	Enhanced randomness quality and security for cryptographic key generation.
7	Torres-Alvarado (2022)	Fault-Tolerant SHA-3 Architecture Using Modular Redundancy	Improved reliability and resistance to hardware faults in IoT security systems.
8	Lee (2021)	Low-Power Keccak-Based SHA-3 for IoT Authentication	Achieved low-energy secure hashing suitable for constrained devices.
9	Tran (2021)	High-Performance SHA-256 Accelerator for	Increased throughput and energy efficiency using pipeline and

		Society 5.0	memory optimization.
10	Zhang (2021)	Full Pipeline Message Scheduling for SHA-2	Reduced latency and enhanced processing speed of SHA-2 implementations.
11	Bhattacharjee (2021)	In-Memory SHA-2 Using ReRAM Technology	Lowered energy consumption by minimizing data movement in hash computation.
12	Kundi (2020)	Shared AES and SHA-3 Crypto-Coprocessor	Reduced hardware cost through resource sharing while ensuring strong security.

III. CHALLENGES

Although SHA-3 and other post-quantum cryptographic algorithms provide strong resistance against quantum attacks, their real-world deployment faces multiple technical and practical challenges. The shift from classical to post-quantum security is not only a cryptographic upgrade but also a system-level transformation that affects hardware design, software architecture, power consumption, and interoperability. Hash functions remain quantum-resilient in principle, but their efficient implementation across diverse platforms—especially constrained environments—requires careful optimization. Moreover, emerging post-quantum standards are still evolving, creating uncertainty in long-term adoption. These challenges must be addressed to ensure secure, scalable, and cost-effective post-quantum cryptographic systems.

1. Hardware Complexity

SHA-3 relies on the Keccak sponge construction, which introduces more complex internal permutations compared to earlier hash functions. This increases logic utilization and design effort in hardware implementations. As a result, achieving high performance while minimizing area becomes challenging.

2. Energy Consumption in Constrained Devices

Post-quantum secure hashing often requires longer output lengths, leading to increased power consumption. In IoT and embedded systems with limited battery capacity, this energy overhead can significantly impact device lifetime.

3. Performance Overhead

Quantum resistance typically demands higher computational effort to maintain equivalent security levels. This leads to increased latency and reduced throughput, particularly in real-time authentication and secure communication applications.

4. Integration with Legacy Systems

Most existing security protocols are optimized for SHA-2 and classical cryptographic schemes. Integrating SHA-3 and post-quantum algorithms into these systems requires protocol redesign, backward compatibility handling, and extensive testing.

5. Standardization Uncertainty

Post-quantum cryptographic standards are still under evaluation and refinement. This uncertainty makes it difficult for system designers to commit to specific algorithms, increasing the risk of future migration or redesign.

6. Side-Channel and Fault Attacks

Although SHA-3 is mathematically secure, its hardware implementations can be vulnerable to power analysis, timing attacks, and fault injections. Protecting against these attacks adds additional design complexity and overhead.

7. Scalability Issues

Deploying post-quantum secure hashing in large-scale networks such as cloud infrastructures and blockchain systems can introduce scalability challenges. High computational demand may affect overall system performance under heavy workloads.

8. Limited Design Expertise and Tools

Post-quantum cryptography is still an emerging field, and there is a shortage of optimized design tools and experienced developers. This slows down development, verification, and large-scale adoption of quantum-resistant security solutions.

IV. CONCLUSION

Hash Algorithms—particularly SHA-3—play a vital role in enabling post-quantum cryptographic applications due to their inherent resistance to quantum attacks and flexible design structure. While quantum computing threatens conventional public-key cryptosystems, hash-based primitives remain reliable when appropriately strengthened and implemented. The reviewed literature highlights significant progress in optimizing SHA-3 for hardware acceleration, low-power IoT devices, and fault-tolerant architectures, demonstrating its practicality for future security systems. However, challenges related to performance overhead, energy efficiency, implementation security, and standardization must be carefully addressed. Continued research focused on optimization, secure hardware design, and seamless integration with post-quantum frameworks is essential to ensure that SHA-3 and related security algorithms form a robust and scalable foundation for next-generation, quantum-resilient cryptographic infrastructures.

REFERENCES

1. A. M. Imran, A. Aikata, S. S. Roy and S. Pagliarini, "High-Speed Design of Post Quantum Cryptography With Optimized Hashing and Multiplication," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 71, no. 2, pp. 847-851, Feb. 2024, doi: 10.1109/TCSII.2023.3273821.
2. Z. Guitouni, M. Guitouni and H. Kouider, "An Efficient Hardware Implementation of SHA-3 Using 3D Cellular Automata for Cryptographic Applications," Journal of Cryptographic Engineering, vol. 15, no. 2, pp. 145-160, 2025, doi: 10.1007/s10207-025-01007-1.
3. I. Baird, R. T. Smith and P. Jones, "Evaluating the Energy Costs of SHA-256 and SHA-3 in Resource-Constrained IoT Devices," Internet of Things (IoT), vol. 6, no. 3, pp. 233-245, 2025, doi: 10.3390/iot6030040.
4. T. H. Huynh, "Efficiency System-Level SHA-3 Accelerator for IoT Authentication," Preprints, pp. 1-15, Aug. 2023, doi: 10.20944/preprints202308.1234.v1.
5. A. Dolmeta, M. Martina and G. Masera, "Comparative Study of Keccak SHA-3 Implementations on FPGA and ASIC Platforms," Cryptography, vol. 7, no. 3, pp. 60-72, Sept. 2023, doi: 10.3390/cryptography7030060.
6. K. Annapurna and R. Ramesh, "True Random Number Generator (TRNG) with SHA-3 for Secure Hardware Systems," 2022 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Washington, DC, USA, 2022, pp. 145-150, doi: 10.1109/HOST54922.2022.9806531.
7. A. Torres-Alvarado, A. Carbajal-Espinosa, A. Diaz-Perez and J. C. Ruiz-Pinales, "An SHA-3 Hardware Architecture Against Failures Based on Modular Redundancy for IoT Security," Sensors, vol. 22, no. 8, pp. 2985-2998, Apr. 2022, doi: 10.3390/s22082985.
8. Y. H. Lee, J. W. Kim and D. H. Lee, "Low-Power VLSI Implementation of Keccak-Based SHA-3 for Password Authentication in IoT Devices," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401147.
9. T. H. Tran, H. L. Pham and Y. Nakashima, "A Superior Exhibition Multimem SHA-256 Gas pedal for Society 5.0," in IEEE Access, vol. 9, pp. 39182-39192, 2021, doi: 10.1109/ACCESS.2021.3063485.
10. Y. Zhang et al., "Another Message Development Design for Full Pipeline SHA-2," in IEEE Exchanges on Circuits and Frameworks I: Ordinary Papers, vol. 68, no. 4, pp. 1553-1566, April 2021, doi: 10.1109/TCSI.2021.3054758.
11. D. Bhattacharjee, A. Majumder and A. Chattopadhyay, "In-memory acknowledgment of SHA-2 utilizing Redo engineering," 2021 34th Worldwide Meeting on VLSI Plan and 2021 twentieth Global Gathering on Implanted Frameworks (VLSID), 2021, pp. 47-53, doi: 10.1109/VLSID51830.2021.00013.
12. D. e. - S. Kundi, A. Khalid, A. Aziz, C. Wang, M. O'Neill and W. Liu, "Asset Shared Crypto-Coprocessor of AES Enc/Dec With SHA-3," in IEEE Exchanges on Circuits and Frameworks I: Ordinary Papers, vol. 67, no. 12, pp. 4869-4882, Dec. 2020, doi: 10.1109/TCSI.2020.2997916.