International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 15, Issue 7, July 2026)

VLSI Architecture for Post-Quantum Cryptography Using SHA-3: A Review

Gaurav Kumar[1], Dr. Bharti Chourasia[2], Dr. Priyanka Jaiswal[3]
[1]M.Tech Scholar, Department of ECE, Sarvepalli Radhakrishnan University, Bhopal, India
[2]Professor and HOD, Department of ECE, Sarvepalli Radhakrishnan University, Bhopal, India
[3]Professor, Department of ECE, Sarvepalli Radhakrishnan University, Bhopal, India

***Abstract*— Post-Quantum Cryptography (PQC) has emerged as an essential research area for protecting digital communication systems against future quantum-computing-based attacks that can compromise conventional cryptographic algorithms. SHA-3, based on the Keccak sponge construction, provides a strong cryptographic hashing foundation for several security applications and can be efficiently implemented through Very Large-Scale Integration (VLSI) architectures. This review examines existing VLSI architectures and hardware optimization techniques for implementing SHA-3 and its role in post-quantum cryptographic systems. It focuses on architectural approaches involving pipelining, parallel processing, loop unrolling, resource sharing, lightweight implementation, and hardware acceleration to improve throughput, area efficiency, power consumption, and processing latency. The review also analyzes important design considerations such as FPGA and ASIC implementation, datapath optimization, memory utilization, timing performance, and resistance to hardware-level attacks. Furthermore, the study identifies challenges related to resource constraints, high-speed processing, energy efficiency, side-channel security, and scalable hardware integration. The review highlights the potential of optimized SHA-3-based VLSI architectures for developing secure, high-performance, and hardware-efficient cryptographic systems suitable for future post-quantum security applications.**

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

I. INTRODUCTION

The rapid development of quantum computing has created a significant challenge for conventional cryptographic systems because sufficiently powerful quantum computers may be capable of compromising widely used public-key algorithms such as RSA and elliptic-curve cryptography. This emerging threat has led to the development of Post-Quantum Cryptography (PQC), which aims to provide cryptographic mechanisms that remain secure against both classical and quantum computing attacks. The importance of PQC has increased substantially with the progress of quantum technologies and the requirement to protect long-term sensitive information from future attacks [1]. In response to this threat, the National Institute of Standards and Technology (NIST) has standardized several post-quantum algorithms, including ML-KEM, ML-DSA, and SLH-DSA, establishing an important foundation for the transition toward quantum-resistant security [2]. These developments have also increased the need for efficient hardware architectures capable of implementing cryptographic operations with high performance, low power consumption, and limited hardware resources.

Among modern cryptographic primitives, SHA-3 has attracted considerable attention because of its strong security properties and flexible sponge-based construction. SHA-3 was standardized by NIST based on the Keccak algorithm and provides both fixed-length hash functions and extendable-output functions [3]. Unlike earlier hash standards based on the Merkle–Damgård construction, SHA-3 employs a sponge construction that provides a different internal architecture and offers flexibility for various cryptographic applications. The underlying Keccak permutation consists of a sequence of transformation

operations that can be efficiently mapped onto hardware architectures, making SHA-3 suitable for FPGA and ASIC implementations [4]. Its relevance to post-quantum cryptography is particularly important for hash-based signatures and for cryptographic schemes that use SHA-3 or related Keccak functions as internal components.

The implementation of cryptographic algorithms in Very Large-Scale Integration (VLSI) technology provides significant advantages over purely software-based solutions when high throughput, low latency, and energy efficiency are required. VLSI architectures can implement cryptographic operations directly in dedicated hardware, reducing instruction-processing overhead and enabling parallel execution of computationally intensive operations [5]. For SHA-3, hardware implementation requires efficient realization of the Keccak-f permutation, including the θ, ρ, π, χ, and ι transformation steps. The design of these operations has a direct impact on area utilization, maximum operating frequency, throughput, power consumption, and overall hardware efficiency [6]. Consequently, researchers have investigated different architectural techniques such as pipelining, loop unrolling, parallel processing, resource sharing, and compact datapath design to optimize SHA-3 implementations.

A major consideration in VLSI-based cryptographic design is the trade-off between area, performance, and power consumption. A highly parallel SHA-3 architecture can provide greater throughput but generally requires more logic resources and may increase power consumption. Conversely, a compact architecture can reduce hardware area and energy requirements but may introduce additional processing cycles and lower throughput [7].

FPGA-based implementation has also become an important platform for evaluating SHA-3 and PQC hardware architectures because FPGAs provide reconfigurability, rapid prototyping, and access to hardware-level performance measurements. Researchers can evaluate different architectural configurations by analyzing parameters such as slice utilization, lookup tables, flip-flops, embedded memory, operating frequency, latency, and throughput [8]. ASIC implementations, on the other hand, can provide improved energy efficiency and higher optimization potential for large-scale production. However, ASIC design involves greater development cost and longer design cycles, making architecture-level optimization particularly important before fabrication [9].

An architecture can reduce overall execution time by performing hashing and related operations independently or in parallel with other cryptographic functions [10]. This approach is especially relevant for standardized PQC algorithms and future cryptographic accelerators where multiple operations must be executed efficiently under strict timing and resource constraints.

Security at the hardware level is another critical consideration. Even when a cryptographic algorithm is mathematically secure, its hardware implementation may reveal information through side channels such as power consumption, electromagnetic radiation, timing variations, or fault behavior. Consequently, VLSI implementations of SHA-3 and PQC systems need to consider countermeasures against side-channel and fault-injection attacks while maintaining acceptable hardware overhead [11]. This creates an additional design challenge because security-enhancing techniques may increase area, power consumption, latency, and implementation complexity.

A systematic review of these architectures is therefore necessary to understand current design approaches, implementation platforms, optimization

techniques, performance metrics, and research limitations [12].

II. LITERATURE SURVEY

Imran et al., [1] presented a high-speed hardware design for post-quantum cryptography by optimizing hashing and multiplication operations. The study focused on reducing the computational overhead associated with major PQC operations. Optimized SHA-3-based hashing was considered to improve the overall processing speed of the cryptographic architecture. Hardware multiplication was also optimized to achieve efficient execution of computationally intensive operations. The work demonstrated the importance of specialized VLSI architectures for achieving high-speed post-quantum cryptographic implementations.

Guitouni et al., [2] presented an efficient hardware implementation of SHA-3 using three-dimensional cellular automata for cryptographic applications. The architecture explored cellular automata as an alternative hardware mechanism for implementing cryptographic transformations. The approach aimed to improve the efficiency of SHA-3 while maintaining the required cryptographic functionality. The study investigated hardware implementation aspects relevant to area and computational performance. The work highlighted the potential of unconventional hardware structures for efficient SHA-3 implementation.

Baird et al., [3] evaluated the energy costs associated with SHA-256 and SHA-3 in resource-constrained IoT devices. The study compared the energy requirements of the two hashing algorithms in environments where power consumption is an important design constraint. The analysis provided useful insights into the suitability of different hash functions for low-power IoT applications. SHA-3 implementation characteristics were examined from an energy-efficiency perspective. The study emphasized that cryptographic hardware for IoT systems must balance security requirements with limited energy resources.

Huynh [4] investigated a system-level SHA-3 accelerator for IoT authentication. The study focused on using dedicated hardware acceleration to improve the execution efficiency of SHA-3 operations in IoT authentication systems. The accelerator was designed to reduce the processing burden associated with cryptographic authentication. Such an architecture can support secure communication while addressing the computational limitations of IoT devices. The research demonstrated the importance of system-level hardware acceleration for practical SHA-3-based security applications.

Dolmeta et al., [5] conducted a comparative study of Keccak SHA-3 implementations on FPGA and ASIC platforms. The research examined the architectural and implementation differences between reconfigurable FPGA-based and dedicated ASIC-based designs. Performance, resource utilization, and hardware efficiency were considered when evaluating the implementations. The comparison provided useful information for selecting an appropriate hardware platform for SHA-3 acceleration. The study highlighted the trade-offs between flexibility, performance, and implementation efficiency in cryptographic hardware design.

Annapurna and Ramesh [6] developed a True Random Number Generator (TRNG) integrated with SHA-3 for secure hardware systems. The study combined random number generation with a cryptographic hashing mechanism to strengthen hardware security. SHA-3 was utilized as an important component for processing or securing generated random information. The architecture targeted applications requiring reliable

randomness and cryptographic protection. The research demonstrated how SHA-3 can be integrated with other hardware security primitives to construct comprehensive secure hardware systems.

Torres-Alvarado et al., [7] presented an SHA-3 hardware architecture incorporating modular redundancy to improve failure tolerance for IoT security applications. The architecture used redundant hardware resources to detect or tolerate failures during cryptographic processing. This approach is particularly important for IoT devices that may operate in unreliable or exposed environments. The study considered fault resilience as an important characteristic alongside cryptographic functionality. The research demonstrated that SHA-3 hardware can be designed with additional reliability mechanisms without changing its fundamental cryptographic operation.

Lee et al., [8] presented a low-power VLSI implementation of Keccak-based SHA-3 for password authentication in IoT devices. The study concentrated on reducing power consumption while maintaining efficient cryptographic processing. The Keccak architecture was optimized for implementation in resource-constrained IoT hardware. The design addressed the requirements of password authentication, where security and energy efficiency are both important. The research highlighted the suitability of optimized SHA-3 VLSI architectures for low-power embedded security applications.

Tran et al., [9] investigated a high-performance SHA-256 hardware accelerator for applications associated with Society 5.0. The study focused on improving hashing performance through an optimized hardware architecture. Although the work concentrated on SHA-256 rather than SHA-3, it provided useful insights into hardware acceleration techniques for cryptographic hash functions. The architecture emphasized high processing performance and efficient hardware utilization. The study provides a comparative basis for understanding the architectural requirements of high-throughput SHA-based cryptographic processors.

Zhang et al., [10] presented a full-pipeline SHA-2 architecture designed to improve message-processing performance. The proposed design employed pipeline-based processing to increase the throughput of cryptographic operations. Full pipelining enabled multiple processing stages to operate concurrently, reducing the effective processing time for successive message blocks. The study demonstrated the benefits of architectural parallelism for high-speed cryptographic hardware. These principles are also relevant to SHA-3 VLSI design, particularly where high throughput is a primary requirement.

Bhattacharjee et al., [11] investigated an in-memory implementation of SHA-2 using a specialized memory-oriented architecture. The study aimed to reduce data movement between processing and memory components during cryptographic computation. In-memory processing can potentially improve energy efficiency and reduce latency by performing computational operations closer to stored data. The approach provides an alternative direction for implementing cryptographic functions in hardware. The research highlights the importance of memory architecture and data movement optimization in designing efficient VLSI cryptographic systems.

Kundi et al., [12] presented a resource-shared cryptographic coprocessor integrating AES encryption/decryption with SHA-3. The architecture used shared hardware resources to support multiple cryptographic functions while reducing overall hardware requirements. Resource sharing can lower silicon area and improve hardware utilization, which is

particularly beneficial for embedded security applications. The integration of AES and SHA-3 provides a flexible foundation for supporting multiple security operations within a single coprocessor. The study demonstrated the potential of integrated and resource-efficient cryptographic hardware for secure systems.

III. CHALLENGES

VLSI architecture for Post-Quantum Cryptography (PQC) using SHA-3 faces several challenges related to achieving high security, performance, low power consumption, and efficient hardware utilization simultaneously. Although SHA-3 provides a strong hashing foundation for quantum-resistant cryptographic systems, its hardware implementation involves complex permutation operations and requires careful architectural optimization. The increasing computational requirements of PQC algorithms, limited resources of IoT and embedded devices, vulnerability to hardware-level attacks, and differences between FPGA and ASIC platforms further complicate the design process. Therefore, future SHA-3-based VLSI architectures need to achieve an effective balance between area, throughput, latency, energy consumption, reliability, and security while supporting scalable integration with complete post-quantum cryptographic systems.

1. High Hardware Resource Utilization

SHA-3 and PQC algorithms can require considerable hardware resources, particularly when high levels of parallelism are used. Multiple processing units, registers, multiplexers, and logic blocks may be required to improve throughput. Excessive resource utilization increases chip area and can make the architecture unsuitable for small embedded and IoT devices. Therefore, efficient resource sharing and optimized datapath design are required.

2. Power and Energy Consumption

Power consumption is a major concern for VLSI-based cryptographic systems, especially in battery-operated IoT and edge devices. High-speed architectures generally require greater switching activity and hardware resources, resulting in increased dynamic power consumption. Reducing power without significantly affecting security and throughput remains a challenging design objective. Techniques such as clock gating, optimized logic structures, and low-power architectures can help address this issue.

3. Throughput and Latency Trade-off

High throughput and low latency are important requirements for cryptographic accelerators used in high-speed communication systems. Techniques such as pipelining, loop unrolling, and parallel processing can significantly increase throughput but may also increase area and power consumption. Conversely, compact architectures may reduce hardware requirements while increasing processing latency. Designing an architecture that provides an appropriate balance between throughput, latency, area, and power is therefore challenging.

4. Integration with PQC Algorithms

SHA-3 may function as a hashing or auxiliary component within larger post-quantum cryptographic algorithms. Integrating a SHA-3 hardware core with complete PQC architectures requires compatibility with other computational modules, memory structures, and data-processing units. Different PQC algorithms may have significantly different computational requirements. Developing a flexible architecture capable of supporting multiple PQC schemes without excessive hardware overhead remains an important challenge.

5. Side-Channel and Hardware Security

A mathematically secure cryptographic algorithm can still be vulnerable when implemented in physical hardware. Power analysis, electromagnetic analysis, timing attacks, and fault injection can potentially reveal sensitive information from VLSI implementations. Countermeasures such as masking, hiding, redundancy, and balanced logic may improve security but generally introduce additional area, power, and timing overhead. Therefore, achieving strong side-channel resistance with minimal hardware cost is difficult.

6. FPGA and ASIC Optimization

SHA-3 architectures may behave differently when implemented on FPGA and ASIC platforms. FPGA designs benefit from reconfigurability and rapid development, while ASIC implementations can provide better optimization for area, power, and performance. An architecture optimized for one platform may not provide the same efficiency on another. Consequently, hardware designers must consider the target technology and optimize the architecture according to its specific resources and implementation constraints.

7. Fault Tolerance and Reliability

Cryptographic hardware used in IoT, aerospace, automotive, industrial, and other critical systems must continue operating reliably even when hardware faults occur. Faults may result from manufacturing defects, environmental conditions, voltage variations, radiation, or deliberate fault-injection attacks. Adding redundant components and fault-detection mechanisms can improve reliability but increases hardware overhead. Developing lightweight fault-tolerant SHA-3 architectures is therefore an important research challenge.

8. Scalability and Future Security Requirements

PQC hardware must remain useful as cryptographic standards, security requirements, and hardware technologies evolve. A fixed architecture may become inefficient when new PQC algorithms or parameter sets are introduced. Therefore, future VLSI designs should provide scalability, configurability, and support for different security levels. Developing flexible SHA-3-based cryptographic accelerators that can accommodate future PQC requirements while maintaining low area and power consumption remains a significant research opportunity.

IV. CONCLUSION

VLSI architectures for Post-Quantum Cryptography using SHA-3 provide a promising approach for developing secure, high-performance, and hardware-efficient cryptographic systems capable of addressing future quantum-based security threats. The reviewed studies demonstrate that techniques such as pipelining, parallel processing, resource sharing, low-power design, hardware acceleration, fault tolerance, and FPGA/ASIC optimization can significantly improve SHA-3 implementation efficiency. However, achieving an optimal balance among hardware area, throughput, latency, power consumption, scalability, and resistance to side-channel and fault attacks remains challenging. Future research should focus on lightweight, reconfigurable, and secure SHA-3 architectures that can be efficiently integrated with different PQC algorithms and deployed in resource-constrained IoT, embedded, edge, and high-performance computing environments. Overall, optimized SHA-3-based VLSI architectures can play an important role in building reliable and scalable hardware foundations for next-generation post-quantum security.

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.