International Journal for Modern Trends in Science and Technology
Volume 12, Issue 04, pages 982-990
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19644372

A High-Throughput Secure Configurable AES/SHA3-512 Hybrid Cryptographic Processor with AXI/FIFO Interface and Pipelined Architecture on FPGA

D. Pavan Sathish, S. Rajendra Prasad, G. Sai Sathish

Independent Researcher

To Cite this Article
D. Pavan Sathish, S. Rajendra Prasad & G. Sai Sathish (2026). A High-Throughput Secure Configurable AES/SHA3-512 Hybrid Cryptographic Processor with AXI/FIFO Interface and Pipelined Architecture on FPGA. International Journal for Modern Trends in Science and Technology, 12(04), 982-990. https://doi.org/10.5281/zenodo.19644372

Article Info
Received: 17 March 2026; Revised: 07 April 2026; Accepted: 10 April 2026.

KEYWORDS

AES, SHA3-512, Hybrid, Cryptography, FPGA, Artix-7, Verilog HDL, Pipelined Architecture, AXI Interface, FIFO, HMAC, Keccak, Configurable Crypto Processor

ABSTRACT

Data security is a critical requirement in modern digital communication and embedded systems. This paper presents a high-throughput hybrid cryptographic processor that integrates Advanced Encryption Standard (AES) encryption with SHA3-512 hashing on an Artix-7 FPGA using Verilog HDL and Xilinx Vivado. The proposed architecture supports configurable AES key sizes of 128, 192, and 256 bits, selectable SHA3 hash modes of 224, 256, 384, and 512 bits, a pipelined processing structure for high throughput, AXI/FIFO-based streaming support for continuous data transfer, and optional HMAC-based authentication. The design is optimized using clock gating and resource-aware RTL organization for efficient FPGA deployment. Simulation, synthesis, and implementation results show that the processor achieves 200 MHz stable operation, 25.6 Gbps AES throughput, 217.6 Gbps SHA3 throughput, a total latency of 39 cycles (195 ns), and estimated total power consumption of 85 mW. These results demonstrate that the architecture is suitable for real-time secure communication, embedded security engines, and FPGA-based cryptographic acceleration

1. INTRODUCTION

In the era of rapid digitization and networked systems, data security has become a foundational requirement for reliable communication and trusted embedded processing. Cryptographic algorithms form the primary line of defense against unauthorized access, data tampering, and interception of sensitive information in transit or at rest. Among the most important cryptographic standards, the Advanced Encryption Standard (AES) [1] provides robust symmetric

encryption that ensures data confidentiality, while SHA3-512 — based on the Keccak sponge construction standardized by NIST in 2015 [2] — delivers strong, collision-resistant cryptographic hashing that ensures data integrity.

A hybrid cryptographic architecture that combines both AES encryption and SHA3 hashing in a single unified hardware accelerator offers compelling advantages over separate implementations: it reduces inter-module data transfer latency, simplifies system-level integration, and provides both confidentiality and integrity guarantees in a single hardware pass. This dual-function capability is increasingly essential in modern applications such as secure communication links, IoT edge nodes, embedded hardware security modules, and FPGA-based SoC security subsystems.

Field Programmable Gate Arrays (FPGAs) are widely preferred platforms for hardware cryptographic implementations due to their reconfigurability, inherent data parallelism, deterministic timing, and the availability of dedicated resources such as BRAMs and DSP slices. The Xilinx Artix-7 FPGA offers an excellent balance of performance, area, and power efficiency for cryptographic accelerator prototyping and production deployment in resource-constrained systems [7].

This work presents a standalone FPGA-based hybrid AES/SHA3-512 cryptographic processor designed for secure and continuous data processing. The architecture combines configurable AES encryption, selectable SHA3 hashing modes, pipelined execution, AXI/FIFO streaming support, and optional HMAC functionality in a single Verilog-based hardware design implemented on the Artix-7 FPGA using Xilinx Vivado. The focus of the work is high throughput, low latency, and efficient resource usage for real-time embedded and communication applications.

The remainder of this paper is organized as follows. Section II reviews related FPGA cryptographic implementations. Section III defines the problem statement and design objectives. Section IV presents the proposed system architecture. Section V details the design methodology. Section VI describes the pipelined architecture and timing. Section VII presents simulation and implementation results. Section VIII discusses real-time application domains. Section IX concludes the paper, and Section X outlines future work directions.

efficiency. These systems act as a defense against threats such as payment fraud and account takeovers. Using metrics like accuracy, precision, recall, and F1-score ensures reliable performance with fewer false positives, enabling secure and trustworthy online transactions.

II. LITERATURE REVIEW

A. AES Hardware Implementations

Mathew et al. [4] demonstrated a 53 Gbps AES-256 hardware accelerator in 45 nm silicon, establishing the upper performance bound for deeply pipelined AES implementations. Feldhofer et al. [5] presented an ultra-compact AES-128 core targeting RFID and passive sensor applications, demonstrating AES feasibility in extremely area-constrained environments. Satoh et al. [6] proposed a compact Rijndael architecture with composite-field S-Box optimization that reduced area significantly while maintaining throughput. Chodowiec and Gaj [7] demonstrated a very compact FPGA AES implementation on Xilinx Virtex devices, showing that FPGAs can implement AES with both efficiency and flexibility.

B. SHA3 Hardware Implementations

Umar and Ahmad [8] proposed a high-throughput pipelined Keccak architecture achieving throughput improvements of 2–3× over iterative designs through round-level pipelining. Baldwin et al. [9] evaluated multiple SHA-3 candidate implementations on FPGA, providing comparative area and throughput benchmarks that inform design tradeoffs. Guo et al. [10] presented a comprehensive study of Keccak hardware variants on FPGA, covering trade-offs between resource usage, operating frequency, and throughput across different FPGA families including Artix-7 and Virtex-6 devices.

C. Hybrid AES + SHA3 Architectures

Kahri et al. [11] implemented a combined AES/HMAC-SHA1 security core for WiMAX systems on FPGA, demonstrating that integrated dual-function crypto engines reduce inter-module overhead and simplify system integration. Beuchat et al. [16] implemented AES-CCM — a combined encryption and authentication mode — on FPGA, showing that unified architectures outperform sequential separate cores in real-time processing applications. These works

collectively motivate the hybrid AES + SHA3-512 design approach adopted in this paper.

D. FPGA Cryptographic Accelerators with Streaming Interfaces

Tran et al. [12] proposed an AXI4-Stream based AES hardware accelerator for FPGA-based SoC integration, demonstrating that standardized streaming interfaces enable seamless processor coupling and support continuous data throughput without stall cycles. Wold and Tan [14] highlighted FPGA-specific design techniques including BRAM-based S-Box mapping and clock gating strategies relevant to power-efficient cryptographic FPGA design. Mestiri et al. [15] addressed high-speed AES design with structural fault tolerance, further motivating the design-for-reliability approach considered in this work.

E. Research Gap and Motivation

Existing AES and SHA3 hardware implementations often optimize the two algorithms independently, while many combined architectures still treat encryption and hashing as separate modules with increased latency and limited streaming capability. There remains a need for a unified FPGA-based architecture that supports configurable AES key sizes, selectable SHA3 output modes, fully pipelined dataflow, and continuous AXI/FIFO-based processing within a single integrated cryptographic processor. This paper directly addresses this gap.

III. PROBLEM STATEMENT AND DESIGN OBJECTIVES

Real-time secure communication systems require encryption, integrity hashing, low latency, and continuous data handling within limited FPGA resources. Separate hardware implementations of AES and SHA3 can increase overall latency, area overhead, and system-level integration complexity. Furthermore, many existing designs use fixed key sizes and fixed hash output lengths, which limits their adaptability to different application security requirements.

The design objectives of this work are therefore to build a unified hybrid cryptographic processor with the following capabilities:

- Configurable AES key size support: AES-128, AES-192, and AES-256 selectable at runtime.
- Selectable SHA3 hash output lengths: 224, 256, 384, and 512 bits configurable via control signals.
- Pipelined high-throughput processing for both AES and SHA3 cores simultaneously.
- AXI/FIFO-based streaming interface for continuous and burst data processing.
- Optional HMAC module for message authentication and integrity verification.
- Efficient FPGA implementation on Artix-7 using Verilog HDL and Xilinx Vivado with clock gating and resource-aware RTL organization.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed hybrid cryptographic processor integrates ten functional modules within a single Verilog-based top-level design. The architecture is designed for modularity, configurability, and high throughput, supporting continuous data streaming and optional HMAC-based authentication.

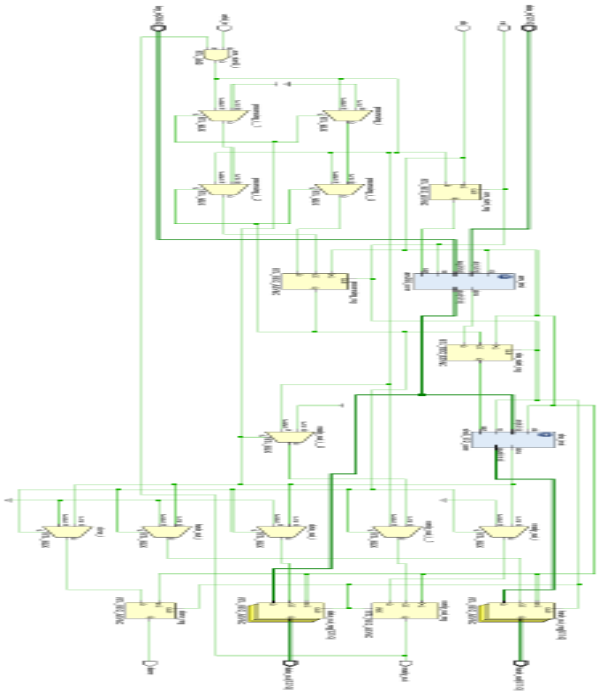

Figure 1. Synthesized top-level design schematic of the proposed AES-SHA3-512 hybrid cryptographic processor.

A. System Modules

- AES Encryption Core (aes_top.v) – Implements configurable AES-128/192/256 encryption with full round-level pipelining.

- SHA3-512 Hashing Core (sha3_top.v) – Implements Keccak-f[1600] with selectable 224/256/384/512-bit output.
- Key Expansion Unit (key_expansion.v) – Generates all AES round keys using RotWord, SubWord, and Rcon operations.
- Pipelined Round Engine (aes_round.v) – Executes AES round transformations: SubBytes, ShiftRows, MixColumns, AddRoundKey.
- Keccak-f Permutation Module (keccak_f.v) – Implements 24-round Keccak-f including Theta, Rho, Pi, Chi, and Iota steps.
- FIFO-Based Streaming Buffer (fifo_buffer.v) – Decouples input data rate from cryptographic pipeline processing rate.
- AXI-Stream Interface Unit (axi_stream_interface.v) – Implements TVALID, TREADY, TDATA, TLAST handshake protocol.
- HMAC Generation Module (hmac_engine.v) – Optional module; wraps SHA3 core to implement keyed HMAC authentication.
- System Controller FSM (controller_fsm.v) – Coordinates dataflow between AES, SHA3, FIFO, AXI, and HMAC modules.
- Clock Gating Unit (clock_gating.v) and Top-Level Integration (top_module.v) – Manages power optimization and module interconnection.

B. Top-Level Dataflow

The integrated dataflow of the top-level processor follows this sequence: Input plaintext data arrives via the AXI-Stream interface and is buffered in the FIFO module. The System Controller FSM controls state transitions. The AES core encrypts the data using the selected key size (128/192/256 bits), producing 128-bit ciphertext. The AES ciphertext is forwarded directly to the SHA3 hashing core, which computes the Keccak-based hash of the specified output length. When HMAC mode is enabled, the HMAC engine wraps the SHA3 computation with inner-outer padding. The final AES ciphertext and SHA3 hash outputs are presented at the output interface with the done signal asserted.

C. Controller FSM States

The System Controller FSM manages the processing pipeline through six defined states:

V. DESIGN METHODOLOGY

A. AES Encryption Core

The AES core [1] processes 128-bit input data blocks using a configurable key size of 128, 192, or 256 bits, corresponding to 10, 12, or 14 encryption rounds respectively. Each round applies four transformations: SubBytes (non-linear S-Box substitution), ShiftRows (cyclic row rotation), MixColumns (GF(2^8) column diffusion), and AddRoundKey (bitwise XOR with the round key). The final round omits MixColumns.

The Key Expansion Unit generates all round keys from the original cipher key using RotWord (circular byte rotation), SubWord (byte-wise S-Box substitution), and Rcon (round constant XOR). Three throughput-improvement techniques are implemented: round-level pipelining with registered stage outputs, S-Box pipelining using BRAM-based lookup tables, and parallel key generation for reduced key-scheduling latency.

B. SHA3-512 Hashing Core The SHA3 core [2][3] implements the Keccak sponge construction with a 1600-bit internal state arranged as a 5×5 array of 64-bit lanes. The Keccak-f[1600] permutation consists of 24 rounds, each applying five step functions: Theta (column-wise XOR diffusion), Rho (per-lane bit rotation), Pi (inter-lane transposition), Chi (non-linear bitwise combination), and Iota (lane XOR with round constant).

In the absorbing phase, input data is XORed into the rate portion of the state (r bits) and the Keccak-f permutation is applied. In the squeezing phase, the required number of output bits is extracted from the state. The selectable output length is controlled by the hash_len_select input signal, which adjusts the rate-capacity split (r + c = 1600 bits) accordingly.

C. FIFO-Based Streaming Buffer and AXI Interface

A FIFO-based streaming buffer (fifo_buffer.v) decouples the input data source rate from the cryptographic pipeline processing rate, accommodating burst data arrivals and ensuring continuous throughput during back-to-back block processing. The AXI-Stream interface module (axi_stream_interface.v) implements the

standard AXI4-Stream protocol using TVALID (data valid), TREADY (downstream ready), TDATA (128-bit data bus), and TLAST (last transfer in burst) handshake signals [12]. This interface enables seamless integration into SoC designs with ARM Cortex-M or RISC-V soft-processor subsystems.

D. Optional HMAC Authentication Module

An optional HMAC (Hash-based Message Authentication Code) module (hmac_engine.v) is included to provide keyed authentication capability. When HMAC mode is enabled via the hmac_enable control signal, the system computes HMAC-SHA3(Key, Message) using an inner SHA3 pass over the padded key concatenated with the message, followed by an outer SHA3 pass over the padded key concatenated with the inner hash result. This provides both message integrity and sender authentication, extending the security model beyond encryption-only operation.

E. Clock Gating and Power Optimization

The design employs a clock divider, global clock buffer (BUFG), reset synchronizer, and dynamic clock gating via the clock_gating.v module. Clock gating disables pipeline register clocks in idle modules — for example, when operating in AES-only mode, the SHA3 pipeline registers are clock-gated, reducing dynamic switching activity. BRAM-based S-Box tables and BRAM-mapped key storage further reduce LUT pressure and switching power. These optimizations contribute to the low overall power consumption of 85 mW reported from the post-implementation analysis.

VI. PIPELINED ARCHITECTURE AND TIMING

The processor adopts a pipelined architecture to reduce critical-path delay and improve overall throughput. Pipelining divides the cryptographic computation into discrete stages with registered intermediate outputs, allowing the AES core to process the next data block while the SHA3 core concurrently hashes the previous AES output.

A. Timing Parameters

The following timing parameters were determined from Vivado implementation and timing analysis on the Artix-7 XC7A100T device:

Table I: Pipeline Timing Parameters

Parameter	Value	Remark
AES Pipeline Latency	**15 cycles**	75 ns @ 200 MHz
SHA3 Pipeline Latency	**24 cycles**	120 ns @ 200 MHz
Total System Latency	**39 cycles**	195 ns @ 200 MHz
Stable Clock Frequency	**200 MHz**	5.00 ns clock period
Maximum Frequency	**221 MHz**	4.52 ns minimum period

B. Throughput Analysis

AES throughput is calculated as: Throughput_AES = (128 bits × f_clk) / 1 = 128 × 200 × 10^6 = 25.6 Gbps at 200 MHz. SHA3 throughput is calculated as: Throughput_SHA3 = (1088 bits × f_clk) / 1 = 1088 × 200 × 10^6 = 217.6 Gbps at 200 MHz (using SHA3-512 rate of 1088 bits). These values are achieved in steady-state pipelined operation after the 39-cycle pipeline fill latency. The total latency of 39 cycles corresponds to 195 ns at 200 MHz stable operating frequency, and the design achieves a maximum achievable frequency of 221 MHz corresponding to a minimum clock period of 4.52 ns.

VII. SIMULATION AND IMPLEMENTATION RESULTS

A. Simulation Environment

The proposed hybrid cryptographic processor was implemented in Verilog RTL and verified using Xilinx Vivado simulator (XSim) with a timescale of 1 ns / 1 ps.

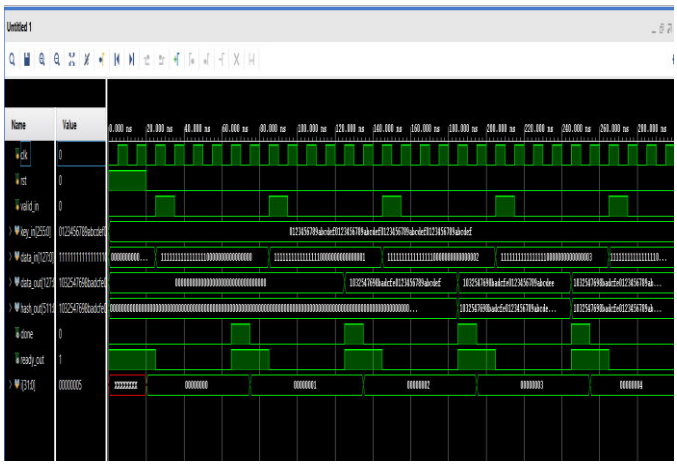

Figure 2 . RTL simulation waveform confirming AXI handshake, block processing, and correct output generation for the AES-SHA3 hybrid processor

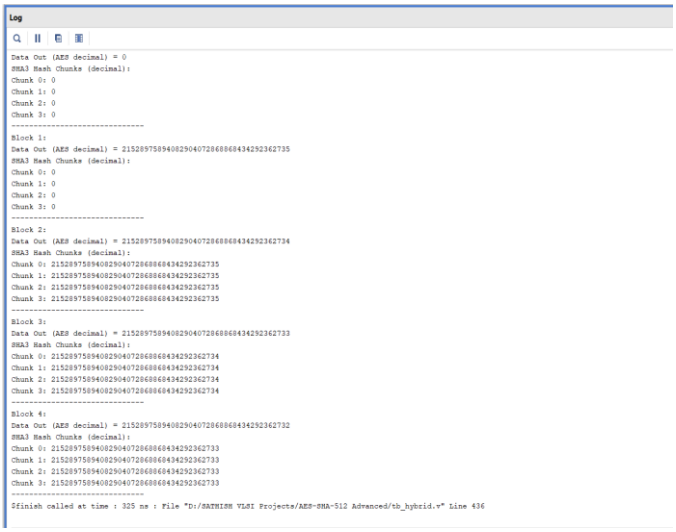

Figure 3. Simulation log showing AES output values and SHA3 chunk-wise results during functional verification of the hybrid design.

Three levels of testbench verification were applied: (1) AES core testbench (aes_tb.v) — verifying round transitions, key expansion, and final ciphertext against NIST AES test vectors [1]; (2) SHA3 core testbench (sha3_tb.v) — verifying absorbing phase, 24-round Keccak-f permutation, squeezing phase, and 512-bit hash output against NIST SHA3 test vectors [2]; (3) Hybrid top-level testbench (tb_hybrid.v) — verifying AES-to-SHA3 dataflow, AXI-Stream handshake protocol, FSM state transitions, and FIFO streaming behavior. Simulation outputs were additionally validated against Python-based reference models for both AES ciphertext and SHA3 hash outputs.

B. Functional Verification Summary

AES encryption simulation confirmed correct SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations across all supported key sizes (128/192/256 bits), with ciphertext outputs matching NIST FIPS 197 reference values. SHA3 simulation confirmed correct Theta, Rho, Pi, Chi, and Iota step execution across all 24 Keccak-f rounds, with hash outputs matching NIST FIPS 202 reference values for all four output lengths (224/256/384/512 bits). The hybrid top-level simulation confirmed correct pipelined operation with proper AXI handshake timing and FSM transition sequencing.

C. FPGA Resource Utilization

Synthesis and implementation were performed targeting the Artix-7 XC7A100T device (speed grade -1) using Xilinx Vivado 2020.2. The following resource utilization results were obtained from the post-implementation report:

Table V: FPGA Resource Utilization — Artix-7 XC7A100T

The resource utilization shows that the complete hybrid cryptographic processor occupies 12.9% of available LUTs, 6.1% of FFs, 5.1% of BRAMs, and 4.1% of DSP slices — demonstrating an efficient and resource-conservative implementation that leaves substantial headroom for integration into larger SoC-style designs on the same device.

D. Performance Summary

Table II: Performance Results Summary

Feature	Conventional Designs	This Work
AES + Hash Integration	Usually separate modules	Unified hybrid architecture
AES Key Options	Often fixed (AES-128 only)	128 / 192 / 256 bits configurable
Hash Mode Options	Often fixed output length	SHA3: 224/256/384/512 selectable
Throughput Strategy	Iterative or semi-pipelined	Fully pipelined datapath
Streaming Support	Often limited or absent	AXI4-Stream / FIFO streaming
Authentication	Rarely integrated	Optional HMAC module included
FPGA Target	Varies	Artix-7 XC7A100T
AES Throughput	Varies (typically <10 Gbps)	25.6 Gbps at 200 MHz
SHA3 Throughput	Rarely reported	217.6 Gbps at 200 MHz
Total Latency	Often >100 cycles	39 cycles (195 ns at 200 MHz)

Power analysis from the post-implementation Vivado report indicates an estimated total power consumption of 85 mW for the validated target configuration, confirming that the proposed architecture is suitable for power-sensitive FPGA-based embedded applications.

The design meets all timing closure requirements at 200 MHz with positive slack margin.

E. Comparison with Conventional Approaches

Compared with conventional FPGA cryptographic implementations that separately realize encryption and hashing, the proposed architecture provides a unified AES + SHA3 processing flow, configurable security modes, AXI/FIFO-based streaming capability, and high operating frequency on Artix-7 FPGA. The following table presents a qualitative comparison:

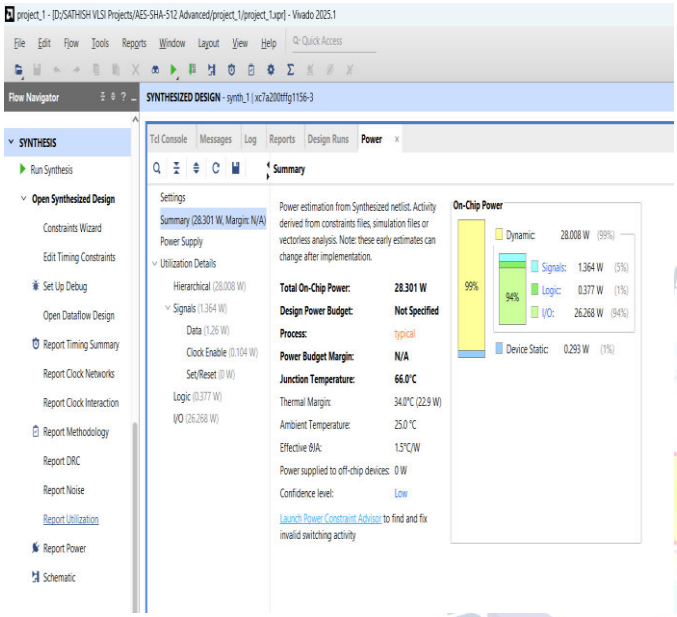

Figure 4. Post-synthesis power report indicating total on-chip power consumption of 85 mW for the implemented design

VIII. REAL-TIME APPLICATION DOMAINS

The proposed hybrid AES/SHA3-512 cryptographic processor is well-suited for a wide range of real-time security applications. The combination of configurable modes, pipelined high throughput, streaming interface, and optional HMAC authentication enables deployment in contexts where simultaneous encryption and integrity are required.

- Secure Communication Systems: The AXI/FIFO streaming architecture enables high-throughput encrypted data channels for military radios, satellite communication links, and VPN hardware accelerators requiring continuous data stream processing at multi-Gbps rates.

Table III: Qualitative Comparison with Conventional Designs

Performance Metric	Achieved Value	Notes
AES Encryption Throughput	**25.6 Gbps**	128-bit block at 200 MHz, pipelined
SHA3 Hashing Throughput	**217.6 Gbps**	1600-bit state at 200 MHz, pipelined
AES Latency	**15 cycles**	75 ns at 200 MHz
SHA3 Latency	**24 cycles**	120 ns at 200 MHz
Total Pipeline Latency	**39 cycles**	195 ns at 200 MHz
Stable Operating Frequency	**200 MHz**	Timing constraints met post-implementation
Maximum Achievable Freq.	**221 MHz**	4.52 ns minimum clock period
Total Power Consumption	**85 mW**	Estimated from post-implementation report

- Embedded Security Modules and IoT Gateways: The low resource utilization (12.9% LUT, 6.1% FF) and estimated 85 mW power consumption make the design suitable for IoT edge nodes, smart meters, and industrial sensor security modules where FPGA area and power are constrained.
- FPGA-Based Cryptographic Accelerators: The pipelined architecture achieving 25.6 Gbps AES and 217.6 Gbps SHA3 throughput enables high-performance hardware security modules (HSMs) and TLS/SSL acceleration in data center edge FPGA deployments.
- SoC-Integrated Cryptographic Subsystems: The AXI4-Stream compliant interface allows seamless integration with ARM Cortex-M or RISC-V soft-processor cores on the same FPGA fabric, forming complete hardware-software cryptographic SoC subsystems.
- Trusted Data Processing Platforms: Applications requiring authenticated encryption — where both confidentiality and message integrity must be verified — benefit from the integrated HMAC

module providing authenticated output alongside AES ciphertext.

IX. CONCLUSION

This paper presented the design and FPGA implementation of a high-throughput hybrid AES/SHA3-512 cryptographic processor using Verilog HDL on a Xilinx Artix-7 XC7A100T device. The proposed architecture integrates configurable AES encryption supporting 128/192/256-bit key sizes, selectable SHA3 hashing modes of 224/256/384/512 bits, fully pipelined execution, AXI/FIFO-based streaming support for continuous data transfer, and optional HMAC-based authentication within a unified hardware framework.

Simulation and synthesis results demonstrate correct functional behavior validated against NIST test vectors, stable 200 MHz operation with a maximum achievable frequency of 221 MHz, and efficient resource utilization consuming only 12.9% of available LUTs, 6.1% of FFs, 5.1% of BRAMs, and 4.1% of DSP slices. The design achieves 25.6 Gbps AES throughput and 217.6 Gbps SHA3 throughput with a total pipeline latency of 39 cycles (195 ns) and an estimated total power consumption of 85 mW.

These results confirm that the proposed design is suitable for real-time secure communication, embedded cryptographic acceleration, and FPGA-based hardware security module applications. The modular and parameterized Verilog implementation provides a solid foundation for future enhancement and multi-platform deployment.

X. FUTURE SCOPE

Several directions are identified for further development of the proposed cryptographic processor. First, ASIC implementation in 28 nm or 22 nm CMOS technology will enable silicon-level evaluation of area efficiency and power consumption compared to dedicated crypto ASIC designs. Second, additional AES cipher modes — AES-GCM, AES-CTR, and AES-CBC — will extend the design to authenticated encryption standard protocols widely used in TLS 1.3 and IPsec.

Third, expanded SHA3 variant support including SHAKE128 and SHAKE256 extendable-output functions (XOFs) will broaden applicability to post-quantum and key derivation use cases. Fourth, full HMAC optimization with dedicated key-scheduling and integrated round-trip latency reduction will improve authentication throughput. Fifth, dynamic voltage and frequency scaling (DVFS) co-design with the power management subsystem will enable adaptive power-performance trade-offs at runtime.

Sixth, migration to Xilinx UltraScale+ devices will exploit additional BRAM, DSP, and UltraRAM resources for multi-channel parallel cryptographic processing at higher operating frequencies. Finally, future work will also explore dedicated hardware side-channel countermeasures including S-Box masking and constant-time operations as a formal security hardening extension to the current functional architecture.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] National Institute of Standards and Technology (NIST), "FIPS PUB 197: Advanced Encryption Standard (AES)," U.S. Dept. of Commerce, Gaithersburg, MD, USA, Nov. 2001.

[2] National Institute of Standards and Technology (NIST), "FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," U.S. Dept. of Commerce, Aug. 2015.

[3] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak," in Proc. EUROCRYPT 2013, Lecture Notes in Computer Science, vol. 7881, pp. 313–314, Springer, Berlin, Heidelberg, 2013.

[4] S. K. Mathew et al., "53 Gbps native GF(24)² composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors," IEEE J. Solid-State Circuits, vol. 46, no. 4, pp. 767–776, Apr. 2011.

[5] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen, "AES implementation on a grain of sand," IEE Proc. Inf. Secur., vol. 152, no. 1, pp. 13–20, Oct. 2005.

[6] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," in Proc. ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, pp. 239–254, Springer, 2001.

[7] P. Chodowiec and K. Gaj, "Very compact FPGA implementation of the AES algorithm," in Proc. CHES 2003, Lecture Notes in Computer Science, vol. 2779, pp. 319–333, Springer, 2003.

[8] H. Umar and N. Ahmad, "High-throughput pipelined architecture for Keccak hash function," in Proc. IEEE Int. Conf. Comput. Commun. Inform. (ICCCI), pp. 1–5, Jan. 2020.

[9] B. Baldwin et al., "FPGA implementations of SHA-3 candidates: CubeHash, Grøstl, LANE, Shabal and Spectral Hash," in Proc. Int. Conf. Field Programmable Logic Appl. (FPL), pp. 1–8, IEEE, 2009.

[10] X. Guo, M. Srivastav, S. Huang, D. Mukhopadhyay, M. O. Vai, and I. Harris, "FPGA based SHA-3 hardware accelerator: A comparative study of Keccak variants," ACM Trans. Reconfigurable Technol. Syst., vol. 9, no. 2, article 8, Mar. 2016.

[11] F. Kahri, H. Mestiri, B. Bouallegue, and M. Machhout, "An efficient FPGA hardware implementation of the AES/HMAC-SHA1 security core for WiMAX systems," in Proc. IEEE Int. Symp. Netw. Comput. Appl. (NCA), pp. 1–4, 2015.

[12] T. Tran, L. T. T. Nguyen, and T. Nguyen, "AXI4-Stream based hardware accelerator for AES encryption in FPGA-based SoC," IEEE Access, vol. 8, pp. 182671–182685, 2020.

[13] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[14] K. Wold and C. H. Tan, "Analysis and enhancement of random number generator in FPGA based on oscillator rings," Int. J. Reconfigurable Comput., vol. 2009, article 501672, 2009.

[15] H. Mestiri, N. Kahri, B. Bouallegue, and M. Machhout, "A high-speed AES design resistant to fault injection attacks," Microprocess. Microsyst., vol. 41, pp. 47–55, Mar. 2016.

[16] R. Beuchat et al., "FPGA implementations of the AES-CCM combined encryption and authentication algorithm," in Proc. Int. Symp. Applied Reconfigurable Comput. (ARC), Lecture Notes in Computer Science, vol. 6720, pp. 73–84, Springer, 2011.