

Crypto-RV: High-Efficiency FPGA-Based RISC-V Cryptographic Co-Processor for IoT Security

Anh Kiet Pham¹, Van Truong Vo², Vu Trung Duong Le¹, Tuan Hai Vu^{2,3}, Hoai Luan Pham¹, Van Tinh Nguyen⁴, and Yasuhiko Nakashima¹

¹Nara Institute of Science and Technology, 8916-5 Takayama-cho, Ikoma, Nara, 630-0192 Japan.

²University of Information Technology, Ho Chi Minh City, 700000, Vietnam

³Vietnam National University, Ho Chi Minh City, 700000, Vietnam

⁴Le Quy Don Technical University, Ha Noi, Viet Nam.

Email: pham.anh_kiet.pf6@naist.ac.jp, take@lqdtu.edu.vn

Abstract—Cryptographic operations are critical for securing IoT, edge computing, and autonomous systems. However, current RISC-V platforms lack efficient hardware support for comprehensive cryptographic algorithm families and post-quantum cryptography. This paper presents Crypto-RV, a RISC-V co-processor architecture that unifies support for SHA-256, SHA-512, SM3, SHA3-256, SHAKE-128, SHAKE-256 AES-128, HARAKA-256, and HARAKA-512 within a single 64-bit datapath. Crypto-RV introduces three key architectural innovations: a high-bandwidth internal buffer (128×64-bit), cryptography-specialized execution units with four-stage pipelined datapaths, and a double-buffering mechanism with adaptive scheduling optimized for large-hash. Implemented on Xilinx ZCU102 FPGA at 160 MHz with 0.851 W dynamic power, Crypto-RV achieves 165 times to 1,061 times speedup over baseline RISC-V cores, 5.8 times to 17.4 times better energy efficiency compared to powerful CPUs. The design occupies only 34,704 LUTs, 37,329 FFs, and 22 BRAMs demonstrating viability for high-performance, energy-efficient cryptographic processing in resource-constrained IoT environments.

Index Terms—RISC-V, Cryptographic Accelerator, SHA-2/SHA-3, IoT, HARAKA

I. INTRODUCTION

Cryptography is fundamental for ensuring confidentiality, integrity, and authenticity in modern computer systems. Hash functions such as SHA-256 and SHA-512 in the SHA-2 family, SHA3-256/512 from the SHA-3 standard, and the Chinese standard SM3 are widely used in digital signatures, certificate infrastructures, blockchain protocols, and integrity verification [1]. AES-128 is the de facto block cipher for authenticated encryption in protocols such as TLS, VPNs, and IEEE 802.11, as well as for full-disk and file-level encryption in storage systems [2]. In addition, the lightweight AES-based hash function HARAKA has been proposed for high-throughput, short-input hashing in advanced constructions such as hash-based signatures [3]. These cryptographic primitives are increasingly deployed together in complex protocol stacks for applications ranging from cloud and data-center security to automotive, industrial control, and large-scale Internet-of-Things (IoT) infrastructures.

Recent work has explored both instruction-set extensions and dedicated accelerators for symmetric cryptography on RISC-V platforms. [4] systematically evaluate standardized

symmetric algorithms on RISC-V and demonstrate that cryptography extensions achieve 1.5 times to 8.6 times speedups over software, yet their study remains at the ISA level and does not propose a concrete co-processor microarchitecture. [5] optimizes AES, ChaCha20, and Keccak for RV32I through hand-crafted assembly and bit-manipulation instructions; however, all computations share a generic RISC-V pipeline, limiting multi-algorithm throughput and memory bandwidth. [6] integrate RISC-V cryptography extensions into a GPGPU and report up to 6.6 times speedup for AES-256; however, the GPU-oriented design is unsuitable for tightly coupled IoT/edge co-processors.

On the hardware accelerator side, [7] propose a unified multi-hash coprocessor for SHA-256/BLAKE-256/BLAKE2s with high throughput and area efficiency through resource sharing, but it supports only three 32-bit hash functions and operates as a standalone IP without tight CPU integration. [8] present a versatile resource-shared cryptographic accelerator for multiple algorithms, maximizing area efficiency; however, its memory hierarchy is relatively simple and lacks optimized scheduling for large sequential hash workloads. [9] introduce a reconfigurable crypto accelerator with multicore architecture and multilevel pipeline scheduling, showing substantial throughput improvements on FPGA, but at the cost of increased complexity and focus on 32-bit algorithms only. More recently, RVCP, a high-efficiency RISC-V co-processor, integrates high-bandwidth internal buffers and pipelined units to accelerate eight symmetric algorithms [10], yet RVCP lacks SHA-3 and HARAKA support and does not employ double-buffered data scheduling optimized for large-hash or tree-hash operations.

To overcome these limitations, this paper proposes Crypto-RV, a high-efficiency RISC-V co-processor architecture that accelerates a comprehensive set of cryptographic primitives: SHA-256, SHA-512, SHA3-256, SHA3-512, SM3, AES-128, and HARAKA, within a unified, tightly coupled design. Crypto-RV introduces three key architectural ideas: a high-bandwidth internal buffer organization (128 × 64-bit) that minimizes memory traffic and sustains throughput for iterative hash computations; cryptography-specialized execution units with carefully balanced four-stage pipelines that share

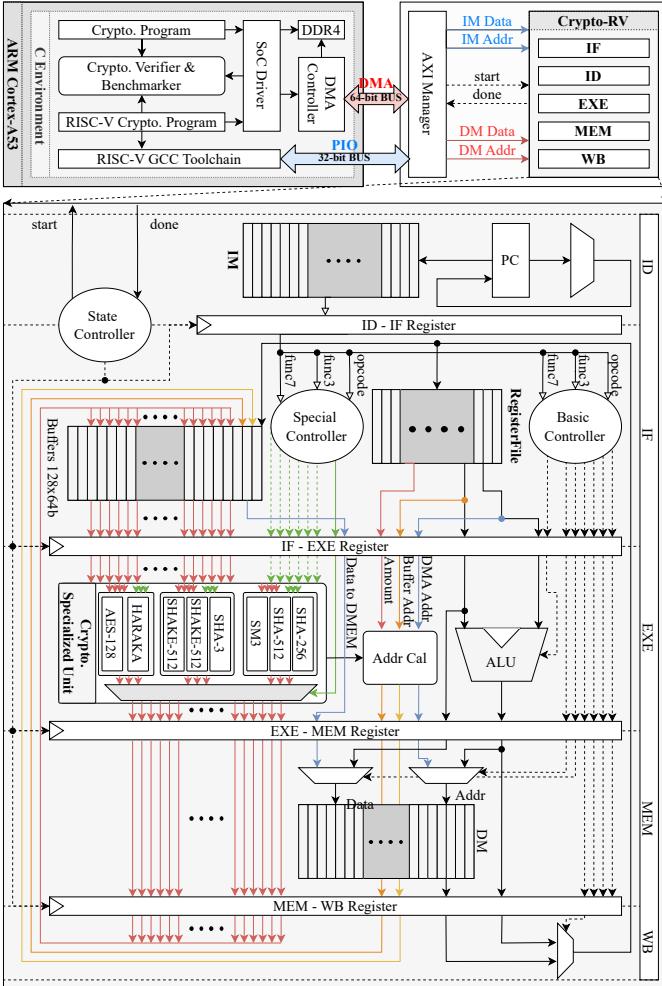


Fig. 1. Overview Crypto-RV Architecture on ZCU102 FPGA SoC

functional resources across multiple hash and block-cipher algorithms while preserving a short critical path; and a double-buffering mechanism with adaptive data scheduling tailored for large-hash operations, significantly reducing latency for long messages and tree-based constructions. Implemented on an FPGA SoC, Crypto-RV achieves substantial improvements in latency, throughput, and energy efficiency compared with baseline RISC-V cores, powerful CPU implementations, and prior accelerator designs, while also providing a flexible hardware platform that can be extended in future work to support hash-based post-quantum schemes such as SPHINCS+.

The remainder of this paper is organized as follows: Section II presents the Crypto-RV architecture. Section III shows the experimental results, and Section IV concludes the paper.

II. PROPOSED CRYPTOGRAPHY RISC-V CO-PROCESSOR

A. System Architecture and Implementation Platform

Fig. 1 shows the system-level integration of Crypto-RV on Xilinx ZCU102 FPGA. The platform comprises two parts: the Processing System (PS) with ARM Cortex-A53 CPU running

Linux, and the Programmable Logic (PL) hosting Crypto-RV. The PS executes three software components: a golden-reference crypto program for functional verification, a RISC-V crypto program that offloads kernels to Crypto-RV, and a benchmarking framework. The RISC-V GCC toolchain compiles programs into instructions while a SoC driver manages data transfers.

An AXI Manager bridges PS and Crypto-RV through two interfaces: a 64-bit DMA channel transfers bulk data between DDR4 and on-chip data memory (DM), while a 32-bit PIO interface delivers configuration and control signals to instruction memory (IM) and control registers. Once initialized, Crypto-RV's five-stage RISC-V pipeline (IF, ID, EXE, MEM, WB) autonomously fetches instructions and accesses data without further software intervention. Within the core, a state controller and custom instruction decoder manage the 128×64-bit internal buffer array and crypto-specialized unit. The buffer serves as high-bandwidth storage for constants and intermediate values, while the specialized unit implements pipelined engines for SHA-256/512, SM3, SHA3-256, SHAKE-128/256, AES-128, and HARAKA-256/512 via custom instructions. An address-calculation block manages data movement between DM, buffers, and the specialized unit, enabling full exploitation of internal bandwidth while maintaining RISC-V compatibility.

B. Internal buffer for High performance

In conventional RISC-V cores, cryptographic kernels repeatedly load intermediate states and message blocks from memory into registers, perform arithmetic operations, and spill results back, a pattern that dominates execution for hash functions processing tens of rounds per block. This creates severe memory bottlenecks: 70–85% of cycles are spent on load/store operations rather than cryptographic computation, a problem intensified for multi-hash workloads (Merkle trees, SPHINCS⁺) where intermediate values shuttle repeatedly between core and memory.

Crypto-RV addresses this through a dedicated 128×64-bit internal buffer tightly coupled to the execution pipeline. Rather than repeatedly accessing memory, the processor initializes buffers once with message words and constants, maintaining all intermediate states on-chip throughout the round sequence. Custom data-movement instructions enable bulk transfers of up to 128 words in single operations, decoupling high-bandwidth intra-round data reuse from low-bandwidth off-chip accesses. This architecture drastically reduces load/store instruction count, enables crypto-specialized units to one pipeline iteration per cycle after warm-up, and shares buffer layout across all algorithms for seamless data reuse without returning to external memory, delivering 17.42×–58.15× latency reduction compared to baseline RISC-V.

C. Cryptography Specialized Unit

The Cryptography Specialized Unit in Crypto-RV consists of three unified engines that execute multiple algorithms

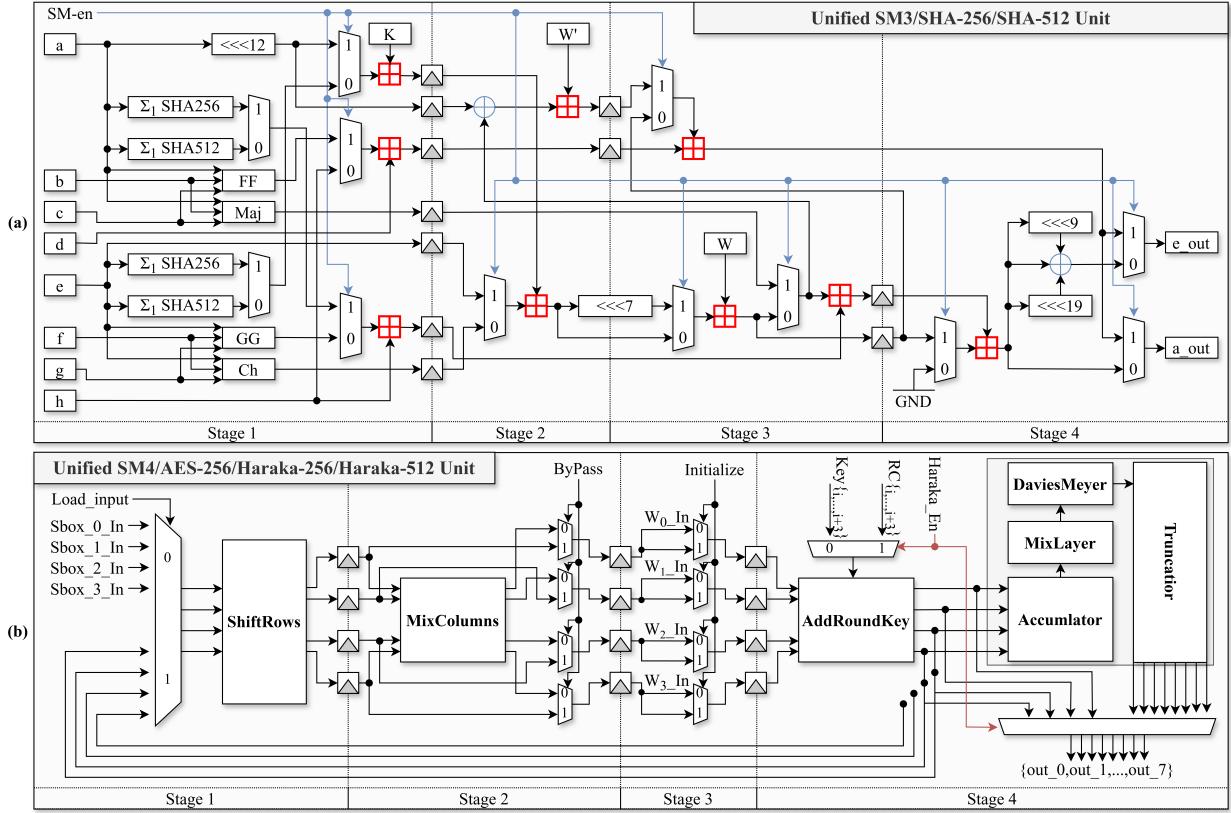


Fig. 2. Propose (a) Unified SM3/SHA-256/SHA-512 Unit, (b) Unified AES-128/Haraka-256/Haraka-512 Unit

within deeply pipelined datapaths. The SM3/SHA-256/SHA-512 and AES-128/Haraka units are implemented as four-stage pipelines, while the SHA3-256/SHAKE-256/SHAKE-512 engine uses a two-stage unrolled structure to balance latency and critical path for sponge-based permutations.

1) *Unified SM3/SHA-256/SHA-512 Unit:* SM3 and SHA-2 (SHA-256, SHA-512) are Merkle–Damgård hash functions with similar iterative structures but differing word sizes (32-bit vs 64-bit), round counts (64/80), and Boolean operations. Related hardware implementation requires separate datapaths for each algorithm, resulting in significant area overhead and resource underutilization.

Crypto-RV addresses this with a unified SM3/SHA-256/SHA-512 engine sharing functional units across all three algorithms. The design comprises a Message Expander (ME) that expands 16 input words into 64 or 80 round words, a Message Compressor (MC) performing core compression with shared adders and mode-select multiplexers, and a Value Rotator (VR) storing results back to buffers. Organized as a four-stage pipeline with one adder per stage, this balanced partitioning maintains a critical path matching the baseline RISC-V ALU. In SHA-512 mode, the unit processes one 1024-bit block per cycle; in SHA-256/SM3 mode, the 32-bit datapath processes two blocks in parallel, effectively doubling throughput while sharing over 80% of arithmetic and logic resources.

2) *Unified AES-128/Haraka-256/Haraka-512 Unit:* AES-128 and the Haraka hash family (Haraka-256/512) are both

AES-based primitives that rely on substitution-permutation networks (SPN) for diffusion and confusion. AES-128 operates on 128-bit blocks through 10 rounds of SubBytes, ShiftRows, MixColumns, and AddRoundKey transformations, while Haraka processes 32/64-byte inputs through multiple AES rounds in a sponge-like structure. A critical challenge for Haraka acceleration is that real-world deployments require full functionality: computing round constants (RC) from seed key (SK) and public key (PK) before hashing input data. Without RC acceleration, Haraka implementations can only speed up 30% of total computation, rendering hardware acceleration ineffective for practical SPHINCS+ signatures or similar schemes.

Crypto-RV solves this bottleneck with a unified AES-128/Haraka-256/Haraka-512 engine featuring a four-stage pipeline that accelerates all Haraka computations, as shown in Fig. 2(b). The pipeline handles SubBytes (Stage 1), ShiftRows/MixColumns (Stage 2), AddRoundKey (Stage 3), and output accumulation (Stage 4) for both AES encryption/decryption and full Haraka sponge operations including RC generation from SK/PK. Mode-select multiplexers enable seamless switching between AES 10-round block processing and Haraka’s variable round counts (32 for Haraka-256, 64 for Haraka-512), with dedicated control logic for RC precomputation. This comprehensive acceleration eliminates Haraka’s RC bottleneck, delivering 3× higher effective throughput than partial implementations while sharing over 75% of resources across all three algorithms, making Crypto-RV uniquely suited

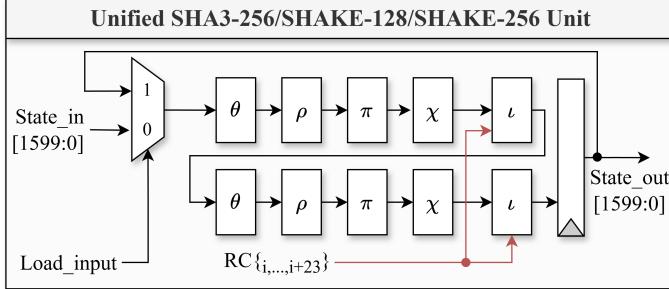


Fig. 3. Unified SHA3-256/SHAKE-128/SHAKE-256 Unit.

for complete hash-based cryptographic workloads.

3) Unified SHA3-256/SHAKE-128/SHAKE-256 Unit:

SHA3-256 and the SHAKE extendable-output functions rely on a 1600-bit sponge permutation requiring 24 sequential rounds of θ , ρ , π , χ , and ι operations. A direct hardware mapping of the 24-round permutation is challenging due to the large state size and complex round function, which creates a long critical path and high latency even with pipelining.

Crypto-RV addresses this through a unified SHA3/SHAKE engine that selectively unrolls two consecutive Keccak rounds per clock cycle within a carefully optimized combinational datapath, reducing effective iteration depth from 24 to 12 rounds while preserving timing closure. As shown in Fig. 3, the design stacks two parallel round pipelines ($\theta \rightarrow \rho \rightarrow \pi \rightarrow \chi \rightarrow \iota$ stages), each processing half the permutation while sharing round constants $RC_{i,\dots,i+23}$. This two-round unroll halves latency compared to a single-round design while maintaining a critical path aligned with the baseline RISC-V ALU, enabling 160 MHz operation. Mode-select multiplexers seamlessly switch between SHA3-256 fixed-length output and SHAKE-128/256 variable-length squeeze phases, all within the same hardware. The design shares state registers and constant generation across all three algorithms, delivering high performance for all Keccak-based functions while preserving timing closure.

D. Double-Buffering for Continuous Big-Hash Processing

Modern hash accelerators struggle to maintain continuous computation when processing large workloads due to a fundamental throughput mismatch between specialized crypto cores and memory subsystem bandwidth. While hash computations proceed at high throughput, data movement via DMA becomes a significant bottleneck, causing the majority of execution cycles to be consumed by memory transfers rather than cryptographic operations. This memory-bound behavior severely restricts core utilization and prevents sustained pipeline operation.

Crypto-RV overcomes this through hierarchical double-buffering between a 1024x64-bit Data Memory (DM) and 128x64-bit internal Buffer (B). DM preloads the entire workload (constants K, initial states S_0^i , messages M_i) at startup; fresh data streams into the buffer while computation proceeds, achieving perfect compute-DMA overlap with $T_{total} \approx T_{compute}$. The design supports two modes: long-

TABLE I
DETAIL UTILIZATION AND POWER CONSUMPTION OF CRYPTO-RV
SPECIALIZED UNITS

Algorithms	Hardware Resource		Power (W)
	LUT	FF	
SHA2-256	3,666	2,096	0.127
SHA2-512			
SM3			
SHA3-256	5,329	3,724	0.200
SHAKE-128			
SHAKE-256			
AES-128	11,308	10,895	0.491
HARAKA-256			
HARAKA-512			

message chaining maintains constants and state on-chip while message blocks stream via sliding window ($S_n = \text{Hash}(S_{n-1} + M_n)$), while many-hash workloads treat DM as a circular buffer processing 8 instances per batch, immediately streaming digests to output. This continuous operation achieves efficient core utilization, significantly reducing execution time for hash-intensive PQC workloads such as SPHINCS+ signature generation compared to software implementations, while the architecture generalizes across diverse cryptographic algorithms.

III. VERIFICATION AND EVALUATION RESULTS

A. Verification and Implementation Results on FPGA

To validate Crypto-RV functionality, we implemented the complete SoC on Xilinx ZCU102 FPGA, successfully processing 100% of 10,000,000 test cases across SHA-256/512, SM3, SHAKE-128/256, SHA3-256, AES-128, HARAKA-256/512 at **160 MHz**. The design occupies **34,704 LUTs**, **37,329 FFs**, and **22 BRAMs** with total SoC power consumption of **4.03 W** (**3.33 W** dynamic, **0.7 W** static), of which Crypto-RV contributes **0.851 W** dynamic power, show in Table I.

The cycle count comparison in Fig. 5 demonstrates substantial speedups over baseline RISC-V: SHA-256/512/SM3 achieve 660x/604x/789x improvements respectively, SHAKE-128/256 reach 220x speedup, and AES-128/HARAKA-256/512 achieve the most dramatic gains at 965x/1061x/780x respectively. These results confirm that the double-buffering architecture and pipelined design achieve significant cycle reduction while maintaining minimal area and power overhead, validating Crypto-RV's efficiency for cryptographic acceleration.

B. Comparison with state-of-the-art CPUs

To evaluate Crypto-RV's efficiency, we compare it with Intel i9-10940X (31.5 W), Intel i7-12700H (23.6 W), and ARM Cortex-A53 (2.7 W). Fig. 6 shows energy efficiency results. Crypto-RV achieves power efficiency from 62.76 to 187.08 Mbps/W across all algorithms.

Intel i9-10940X: Crypto-RV provides **4.0 times to 11.8 times** better efficiency. Notably, SHA-512 reaches 11.8 times (187.08 vs. 15.89 Mbps/W), SHAKE-128 achieves 11.4 times

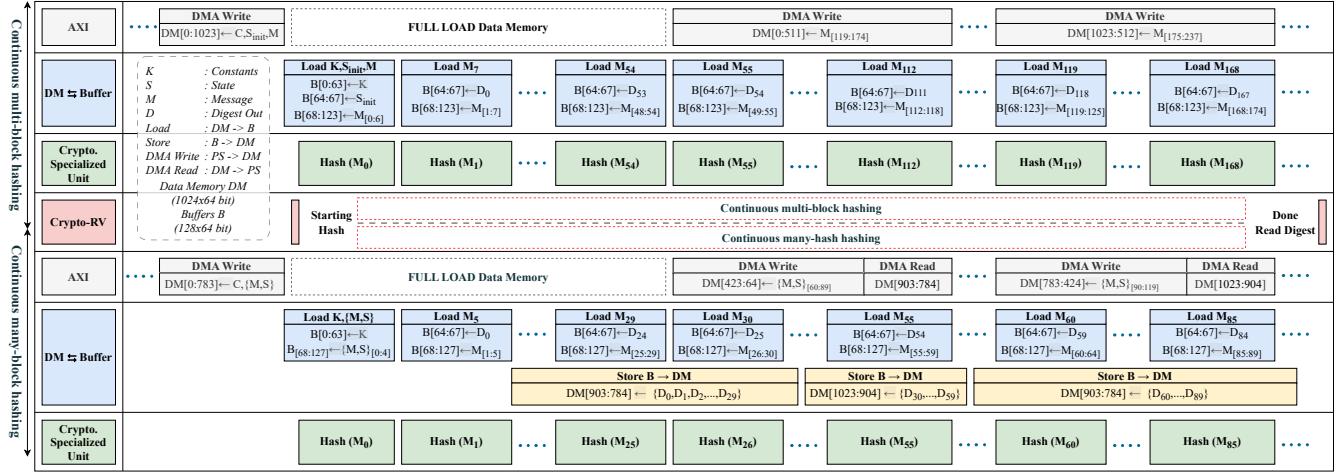


Fig. 4. Double-buffering schedule.

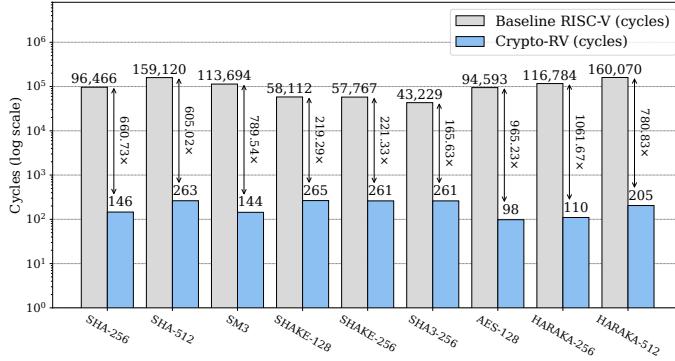


Fig. 5. Total cycles per algorithm: Crypto-RV vs RISC-V baseline.

(145.05 vs. 12.74 Mbps/W), and SHAKE-256 provides 11.6 times (147.27 vs. 12.67 Mbps/W). Hash functions (SHA-256, SM3) deliver 8.8 times to 10.2 times improvements. Post-quantum primitives show 4.8 times to 7.3 times gains, with HARAKA-256 and HARAKA-512 achieving 4.8 times and 5.8 times respectively.

Intel i7-12700H: Crypto-RV delivers **3.2 times to 9.5 times** improvements. SHA-512 reaches 9.5 times (187.08 vs. 19.74 Mbps/W), SHAKE variants achieve 9.2 times to 9.3 times, and SM3 provides 8.1 times. AES-128 shows 3.2 times efficiency gain, while HARAKA variants deliver 7.1 times to 7.6 times improvements.

ARM Cortex-A53: Crypto-RV achieves **1.2 times to 3.2 times** efficiency gains. SHA-512 reaches 3.2 times (187.08 vs. 59.24 Mbps/W), SHAKE-128/256 provide 3.1 times, and SM3 delivers 2.6 times. SHA-256 shows modest 1.2 times gain due to ARM A53's high efficiency on this algorithm. HARAKA variants achieve 2.5 times to 3.2 times improvements.

These results validate specialized hardware acceleration effectiveness for post-quantum (HARAKA) and memory-intensive algorithms (SHAKE), making Crypto-RV ideal for power-constrained IoT systems.

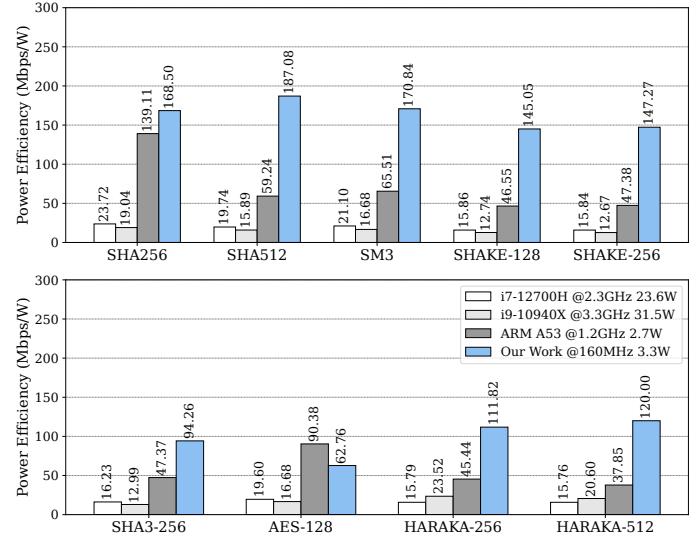


Fig. 6. Power efficiency comparison between Crypto-RV and powerful CPUs.

C. Comparison with related RISC-V work

Table II presents a comprehensive execution cycle comparison between Crypto-RV and related RISC-V cryptographic accelerators, highlighting the superior throughput of Crypto-RV. Crypto-RV demonstrates a significant reduction in cycles per byte across various cryptographic algorithms, outperforming prior designs. The detailed results are as follows:

- SHA-256:** Crypto-RV achieves a throughput that is **56.70 times** higher than the reference design [11], with 146 cycles (2.28 cycles/byte).
- SHA-512:** Crypto-RV shows an improvement ranging from **25.54 times to 1,291.68 times** compared to reference designs [12], [13], executing in 263 cycles (2.05 cycles/byte).
- SM3:** Crypto-RV is **49.18 times** faster than the reference design [14], completing in 144 cycles (2.25 cycles/byte).
- SHAKE-128/256:** Crypto-RV achieves 265 and 261 cycles (2.61–2.65 cycles/byte), delivering consistent effi-

TABLE II
EXECUTION CYCLE COMPARISON BETWEEN
PRIOR WORKS AND CRYPTO-RV

Reference	Algorithm	Cycles	Cycles/Byte	Improve
[11]	SHA-256	8,278	129.30	56.70×
[12]	SHA-512	13,975	109.20	53.14×
[13]	SHA-512	339,712	2.65	1,291×
[14]	SM3	7,082	110.70	49.18×
[15]	AES-128	10,306	644.10	105.16×
[16]	AES-128	38,328	2.40	391.10×
[17]	SHA-256	2,495	38.98	17.09×
	SHA-512	6,716	52.47	25.54×
	SM3	2,038	31.84	14.15×
	AES-128	5,590	349.38	57.04×
[18]	AES-128	1,395	87.19	14.23×
Crypto-RV	SHA-256	146	2.28	-
	SHA-512	263	2.05	-
	SM3	144	2.25	-
	SHAKE-128	265	2.65	-
	SHAKE-256	261	2.61	-
	SHA3-256	261	4.08	-
	AES-128	98	6.13	-
	HARAKA-256	110	3.44	-
	HARAKA-512	205	3.20	-

ciency across sponge-based functions.

- **SHA3-256:** Crypto-RV completes in 261 cycles (4.08 cycles/byte), enabling efficient post-quantum cryptography support.
- **AES-128:** Crypto-RV demonstrates superior performance ranging from **14.23 times to 391.10 times** better than reference designs [15], [16], executing in 98 cycles (6.13 cycles/byte).
- **HARAKA-256/512:** Crypto-RV achieves 110 and 205 cycles (3.44 and 3.20 cycles/byte), providing critical acceleration for hash-based post-quantum signatures.

Overall, Crypto-RV’s consistent 2.0 to 4.1 cycles/byte across all algorithms underscores the effectiveness of the unified architecture in transforming memory-bound operations into compute-bound execution. The comparison results demonstrate Crypto-RV’s significantly enhanced throughput compared to existing RISC-V designs, particularly for hash functions (SHA-256, SHA-512, SM3) and post-quantum primitives (HARAKA), enabling sustainable high-throughput processing without memory bottlenecks.

IV. CONCLUSION

This paper presents Crypto-RV, a high-efficiency RISC-V co-processor that unifies SHA-2, SHA-3, SM3, AES-128, and HARAKA within a single 64-bit datapath. Crypto-RV achieves multi-algorithm flexibility with minimal area overhead, sustains high-throughput computation through hierarchical buffering, and eliminates memory stalls via continuous double-buffering, transforming cryptographic operations from memory-bound to compute-bound execution. The architecture demonstrates exceptional efficiency for IoT and edge computing systems where power and area constraints are critical. Future work will extend Crypto-RV to fully accelerate SPHINCS+ signature generation through specialized tree-hash cores and optimized Merkle-layer state management, establishing it as a unified platform for quantum-safe IoT security.

ACKNOWLEDGMENT

This research was funded by JST-ALCA-Next (JPM-JAN23F4) and the Vietnam National Foundation for Science and Technology Development (NAFOSTED) under Grant 102.01-2025.50.

REFERENCES

- [1] NIST, “FIPS 180-4: Secure hash standard (shs),” Federal Information Processing Standards Publication, 2015.
- [2] ———, “FIPS 197: Advanced encryption standard (aes),” Federal Information Processing Standards Publication, 2001.
- [3] S. Kölbl, M. Lauridsen, C. Rechberger, P. Schwabe, and G. Seiler, “Haraka: Efficient short-input hashing for post-quantum applications,” in *Progress in Cryptology – ASIACRYPT 2016*, ser. LNCS, vol. 10031. Springer, 2016, pp. 353–377.
- [4] G. Nişancı, P. G. Flikkema, and T. Yalçın, “Symmetric cryptography on RISC-V: Performance evaluation of standardized algorithms,” in *Cryptography*, vol. 6, no. 3. MDPI, 2022, p. 41.
- [5] K. Stoffelen, “Efficient cryptography on the RISC-V architecture,” in *Progress in Cryptology – LATINCRYPT 2019*, ser. LNCS, vol. 11774. Springer, 2019, pp. 323–340.
- [6] R. Adams *et al.*, “Cryptography acceleration in a RISC-V GPGPU,” in *CARRV 2021: 5th Workshop on Computer Architecture Research with RISC-V*, 2021.
- [7] P. H. Luan, T. S. Duong, V. T. D. Le, T. H. Tran, and Y. Nakashima, “Energy-efficient unified multi-hash coprocessor for securing IoT systems integrating blockchain,” in *IEEE 66th Int. Midwest Symp. on Circuits and Systems (MWSCAS)*, 2023, pp. 355–359.
- [8] V. T. D. Le, H. L. Pham, T. H. Tran, Q. D. N. Nguyen *et al.*, “Versatile resource-shared cryptographic accelerator for multi-domain applications,” in *2023 Int. Conf. on IC Design and Technology (ICICDT)*, 2023, pp. 104–107.
- [9] V. T. D. Le, H. L. Pham, T. H. Tran, V. D. Tran, and Y. Nakashima, “High-efficiency reconfigurable crypto accelerator utilizing innovative resource sharing and parallel processing,” in *16th IEEE Int. Symp. on Embedded Multicore/Manycore SoCs (MCSoC)*, 2023.
- [10] D. H. A. Le *et al.*, “RVCP: High-efficiency RISC-V co-processor for security applications in IoT and server systems,” in *International SoC Design Conference (ISOCC)*. IEEE, 2024.
- [11] J. Wu, X. Zheng, S. Zeng, H. Gao, and X. Xiong, “High-performance cryptographic soc virtual prototyping platform based on risc-v vp,” in *HP3C ’22*. Association for Computing Machinery, 2022, p. 84–90.
- [12] G. Nişancı, P. G. Flikkema, and T. Yalçın, “Symmetric cryptography on risc-v: Performance evaluation of standardized algorithms,” *Cryptography*, vol. 6, no. 3, p. 41, 2022.
- [13] H. Cheng, D. Dinu, and J. Großschädl, “Efficient implementation of the sha-512 hash function for 8-bit avr microcontrollers,” in *SecITC 2019*. Cham: Springer International Publishing, pp. 273–287.
- [14] X. Zheng, J. Wu, X. Lin, H. Gao, S. Cai, and X. Xiong, “Hardware/software co-design of cryptographic soc based on risc-v virtual prototype,” *TCAS-II*, vol. 70, no. 9, pp. 3624–3628, 2023.
- [15] A. Adomnicai and T. Peyrin, “Fixslicing AES-like ciphers: New bitsliced AES speed records on ARM-cortex m and RISC-v,” *Cryptology ePrint Archive*, Paper 2020/1123, 2020, <https://eprint.iacr.org/2020/1123>.
- [16] Y.-M. Kuo, F. Garcia-Herrero, and J. A. Maestro, “Versatile risc-v isa galois field arithmetic extension for cryptography and error-correction codes,” 06 2021.
- [17] V. T. D. Le, T. H. Y. Tran, D. H. A. Le, T. H. Vu, and H. L. Pham, “Rvcp: High-efficiency risc-v co-processor for security applications in iot and server systems,” in *2024 International Conference on Advanced Technologies for Communications (ATC)*, 2024, pp. 602–607.
- [18] V. T. Nguyen, P. H. Pham, V. T. D. Le, H. L. Pham, T. H. Vu, and T. D. Tran, “Aes-rv: Hardware-efficient risc-v accelerator with low-latency aes instruction extension for iot security,” *IEICE Electronics Express*, vol. advpub, p. 22.20250329, 2025.