Masters Project Research Log

Masters in Electronic and Computer Engineering

Student Name: Harsh Mayank Dabhi
Student ID: A00010544
Project Title: Enhancing Cryptographic Application Performance on RISC-V Processors with B and K Extensions

Date: August 2025

Project Problem / Research Question

This project investigates the design, implementation, and evaluation of hardware acceleration techniques for resource-constrained RISC-V systems. General-purpose instruction sets are often inefficient for bit-level and cryptographic workloads common in embedded systems, causing performance bottlenecks and higher energy consumption. This project addresses this gap by integrating and analyzing standardized RISC-V extensions.

Research Questions:

1. How can the RISC-V Bit Manipulation (B) and Cryptography (K, V) extensions be designed and integrated into a standard 32-bit core?

2. What is the impact of these extensions on execution cycles, binary size, and hardware area overhead?

3. How do general-purpose extensions compare to specialized cryptographic accelerators in terms of benefits and trade-offs?

4. What role does the software ecosystem (compilers, simulators) play in enabling and verifying these hardware extensions?

Paper 1

Reference: P. S. Babu, S. Sivaraman, D. N. Sarma, and T. S. Warrier, *Evaluation of Bit Manipulation Instructions in Optimization of Size and Speed in RISC-V*, Proc. 34th Int. Conf. on VLSI Design (VLSID), 2021.

Section	Content
Summary	Evaluates the RISC-V Bit Manipulation (B) extension on an RV32IMAC core with a loosely-coupled coprocessor. Using Embench benchmarks, reports up to 28% speedup and 20% code size reduction for bit-intensive workloads like CRC32 and sorting.
Relevance	Provides performance justification for the B extension and serves as a baseline for comparing tightly vs. loosely coupled designs. Directly addresses performance and code density benefits for embedded systems.
Strengths	Credible benchmarking with Embench; shows clear gains in speed and code size.
Weaknesses	Lacks hardware area analysis; coprocessor approach may introduce latency vs. integrated ALU design.

Paper 2

Reference: K. Kim, D. Harris, and K. Macsai-Goren, *Design and Synthesis of RISC-V Bit Manipulation Extensions*, Proc. 57th Asilomar Conf., 2023.

Section	Content
Summary	Implements full RISC-V BMI (Zba, Zbb, Zbc, Zbs) in CORE-V Wally ALU. Synthesized in 28nm ASIC with 1–2.5% area overhead, no timing degradation.
Relevance	Provides precise hardware cost data for B extension, complementing Babu *et al* performance results. Tightly integrated ALU design serves as architectural reference.
Strengths	Realistic ASIC synthesis; granular area breakdown per sub-extension.

Weaknesses	No performance benchmarking; relies on combining with other studies for complete performance-per-area analysis.

Paper 3

Reference: C. G. de A. Gewehr and F. G. Moraes, *Improving the Efficiency of Cryptography Algorithms on Resource-Constrained Embedded Systems via RISC-V Instruction Set Extensions*, Proc. SBCCI, 2023.

Section	Content
Summary	Implements AES and SHA-2 (Zkne, Zknh) in Ibex core. Achieves >40x AES-128 speedup over TinyCrypt software. Reports 10% area overhead and improved memory/energy efficiency.
Relevance	Central to cryptographic acceleration part of the project; offers dramatic performance results to compare with B extension.
Strengths	Holistic evaluation: performance, area, memory, energy.
Weaknesses	Results based on small core; relative area impact may vary for larger processors.

Paper 4

Reference: M. Namazi Rizi et al., *Optimised AES with RISC-V Vector Extensions*, Proc. DDECS, 2024.

Section	Content
Summary	Uses RISC-V Vector (V) extension with Vicuna coprocessor for AES. Achieves 2.5x speedup by processing multiple blocks in parallel (SIMD).
Relevance	Introduces throughput-oriented vector acceleration, contrasting with latency-focused scalar K extension. Key for comparative analysis.
Strengths	Based on ratified RVV 1.0; demonstrates effective parallelism.

Weaknesses	No direct comparison with K extension; limits head-to-head evaluation.

Paper 5

Reference: C. G. de A. Gewehr et al., *Hardware Acceleration of Authenticated Encryption with Associated Data via RISC-V Instruction Set Extensions*, Proc. LASCAS, 2024.

Section	Content
Summary	Evaluates AES-CCM, Ascon, ChaCha20-Poly1305 with hardware acceleration on Ibex. AES-CCM achieves 19.66x speedup; Ascon sees 2.45x. Tested in Zigbee packet scenario.
Relevance	Extends analysis to system-level AEAD protocols, showing cascading benefits of accelerating primitives.
Strengths	System-level evaluation; compares multiple algorithms.
Weaknesses	AES-CCM baseline less optimized, possibly exaggerating relative gains.

Paper 6

Reference: D. Markov and A. Romanov, *Implementation of the RISC-V Architecture with the Extended Zbb Instruction Set*, Proc. UralCon, 2022.

Section	Content
Summary	Adds Zbb to schoolRISCV core on FPGA; modifies RARS assembler/simulator. Reports 29.9% speedup on custom benchmarks; large FPGA area increase from small baseline.
Relevance	Demonstrates necessary toolchain modifications, reinforcing software-hardware co-design importance.

Strengths	Focus on toolchain integration; open-source implementation.
Weaknesses	Custom benchmarks limit generalization; FPGA area comparison potentially misleading.

Paper 7

Reference: M. A. Elmohr et al., *Hardware Implementation of A SHA-3 Application-Specific Instruction Set Processor*, Proc. ICM, 2016.

Section	**Content**
Summary	Designs ASIP for SHA-3 on MIPS-like core; compares native datapath vs. coprocessor integration. Coprocessor achieves 61.4% speedup at 25.8% FPGA area increase.
Relevance	Shows methodology for profiling, bottleneck identification, and custom instruction design; relevant to cryptographic ISA extension work.
Strengths	Clear ASIP design methodology; compares integration architectures.
Weaknesses	Non-RISC-V architecture; uses custom non-standard instructions.

Paper 8

Reference: M. Schlägl, M. Stockinger, and D. Große, *A RISC-V ‘V’ VP: Unlocking Vector Processing for Evaluation at the System Level*, Proc. DATE, 2024.

Section	**Content**
Summary	Develops open-source SystemC TLM Virtual Prototype supporting full RISC-V V extension. Enables high-level evaluation of vectorized software before RTL design.

Relevance	Relevant for simulation methodology; shows how VP aids architectural exploration for complex extensions.
Strengths	Open-source; efficient instruction integration via code generation.
Weaknesses	Instruction-accurate but not cycle-accurate; cannot replace RTL for final verification.