Marian: An Open Source RISC-V Processor with Zvk Vector Cryptography Extensions

Thomas Szymkowiak Endrit Isufi Markku-Juhani Saarinen

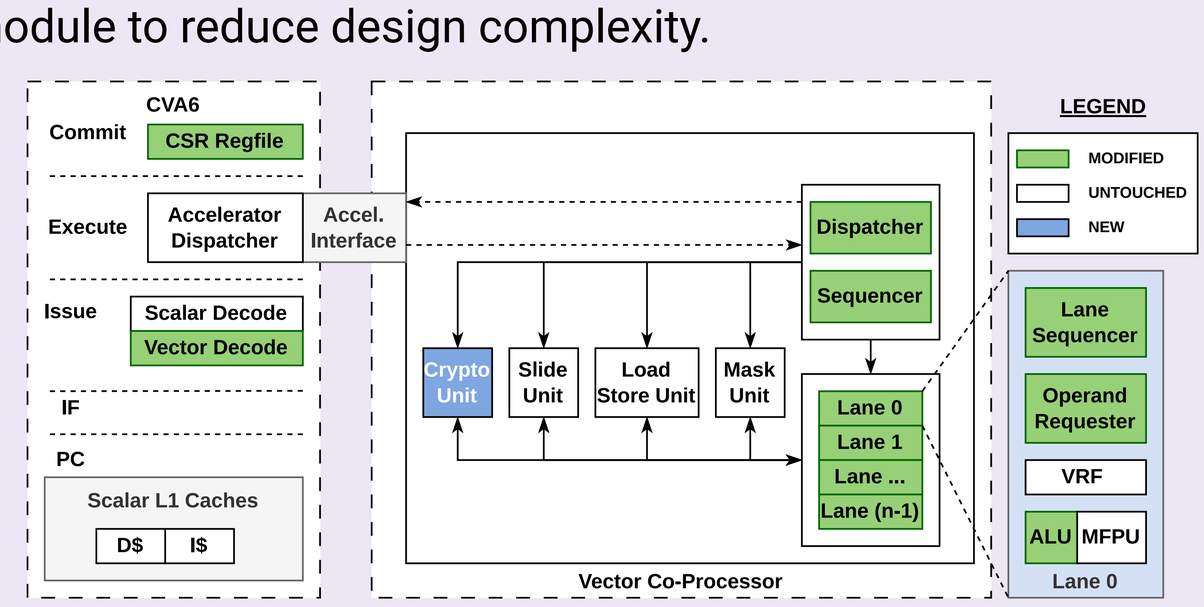
Tampere University, Tampere, Finland

Marian

- The RISC-V Vector Crypto Extensions (Zvk) were ratified in 2023 and support high-speed symmetric cryptography operating on the vector register file, to offer significant performance improvements over scalar cryptography extensions (Zk) due to data parallelism.
- Marian is the **first open-source hardware implementation** of a vector processor with the Zvk extensions.
- Design is based on the PULP "Ara" [1] vector unit.
- Implementation is in SystemVerilog and has been tested using a Virtex Ultrascale+ FPGA prototype, with a planned tapeout targeting a 22nm process node.

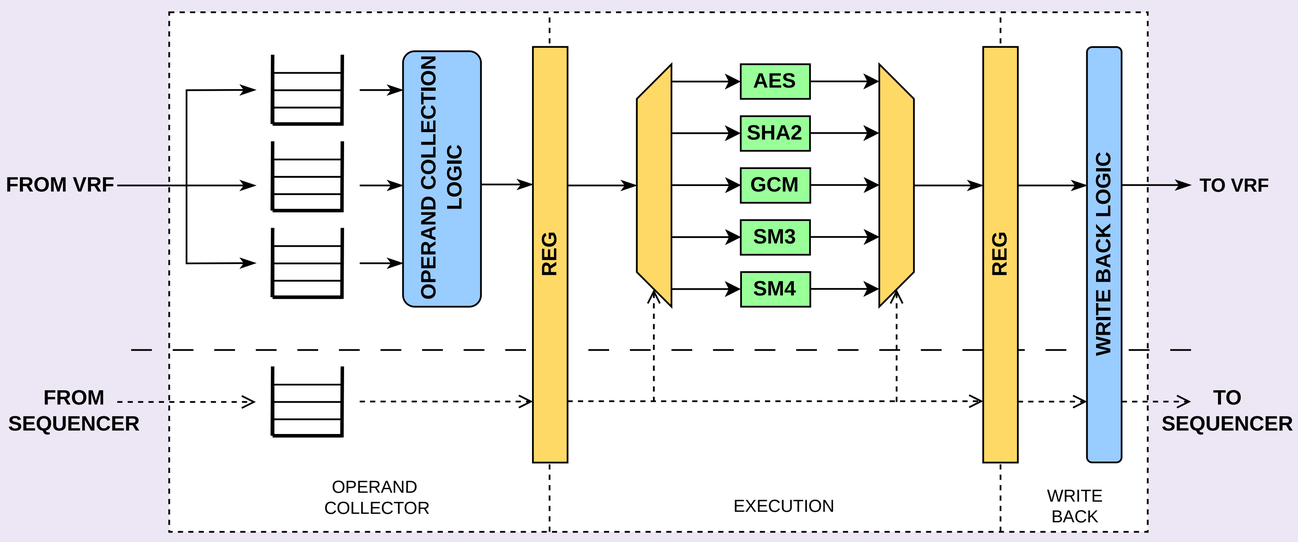
Architecture

- The maximum element width (ELEN) and the bit width of the lane data paths are both fixed at 64b within Ara. Many instructions within Zvk specification perform operations on Element Groups (EG) with an Element Group Width (EGW) greater than 64b.
- Arithmetic logic of the cryptographic operations was separated from the vector lane logic and placed into a dedicate Crypto Unit module to reduce design complexity.



Crypto-Unit Design

- The Crypto Unit is a three-stage, latency-insensitive pipeline consisting of an operand collection stage, an execution unit stage, and a write-back stage.
- Instructions are executed and results are written back in-order.



Implementation Results

- Marian has been successfully prototyped on an AMD-Xilinx VCU118 (Virtex Ultrascale+) FPGA running at 75MHz. The ASIC physical design flow for Marian is currently underway, targeting a 22nm low-power process and an F_{max} of 1GHz.
- The Gate Equivalent (GE) values are calculated using a two-input NAND gate in the target technology.

Top Module	Registers	LUT (logic)	LUT (RAM)	BRAM (kB)	DSP
Marian	115,767	420,056	1908	360	225
CVA6	24,924	40,900	884	117	28
Vector Unit	67,680	322,474	1,024	0	197
Lane (single)	14,513	57,175	256	0	49
Crypto Unit	2,800	33,465	0	0	0

Benchmarking Results

- An initial performance evaluation of Marian was performed against C-language reference implementations of cryptographic primitives taken from OpenSSL 3.3.1 [2].
- The equivalent operations were subsequently executed using code with Zvk instructions.
- The RISC-V *instret* and *cycle* performance CSRs were used to measure the number of instructions retired and CPU cycles elapsed during execution.
- Observed a 6x - 100x speedup in terms of execution cycles and between 12x - 300x reduction in terms of executed instructions.

Operation		Reference		Zvk	
		Cycles	Instret	Cycles	Instret
AES128	**Enc.**	18,794	12,482	343	53
	Dec.	23,731	15,077	226	53
AES256	**Enc.**	24,493	17,478	441	65
	Dec.	32,677	21,213	278	65
SHA256	**Hash**	156,205	82,179	12,106	3,802
SHA512	**Hash**	109,905	45,903	9,140	2,712
SM3	**Hash**	304,031	70,075	8,134	1,410
SM4	**Enc.**	4,187	1,423	272	39
	Dec.	2,564	1,425	178	39

References

[1] M. Perotti, M. Cavalcante, R. Andri, L. Cavigelli, and L. Benini. "Ara2: Exploring Single- and Multi-Core Vector Processing with an Efficient RVV 1.0 Compliant Open-Source Processor". In: *IEEE Transactions on Computers* 73.7 (July 2024), pp. 1822–1836.

[2] OpenSSL. *OpenSSL*. https://github.com/openssl/openssl/tree/openssl-3.3.1. 2024.

Tampere University

github.com/soc-hub-fi/Marian

sochub.fi/