A RISC-V based accelerator for Post Quantum Cryptography

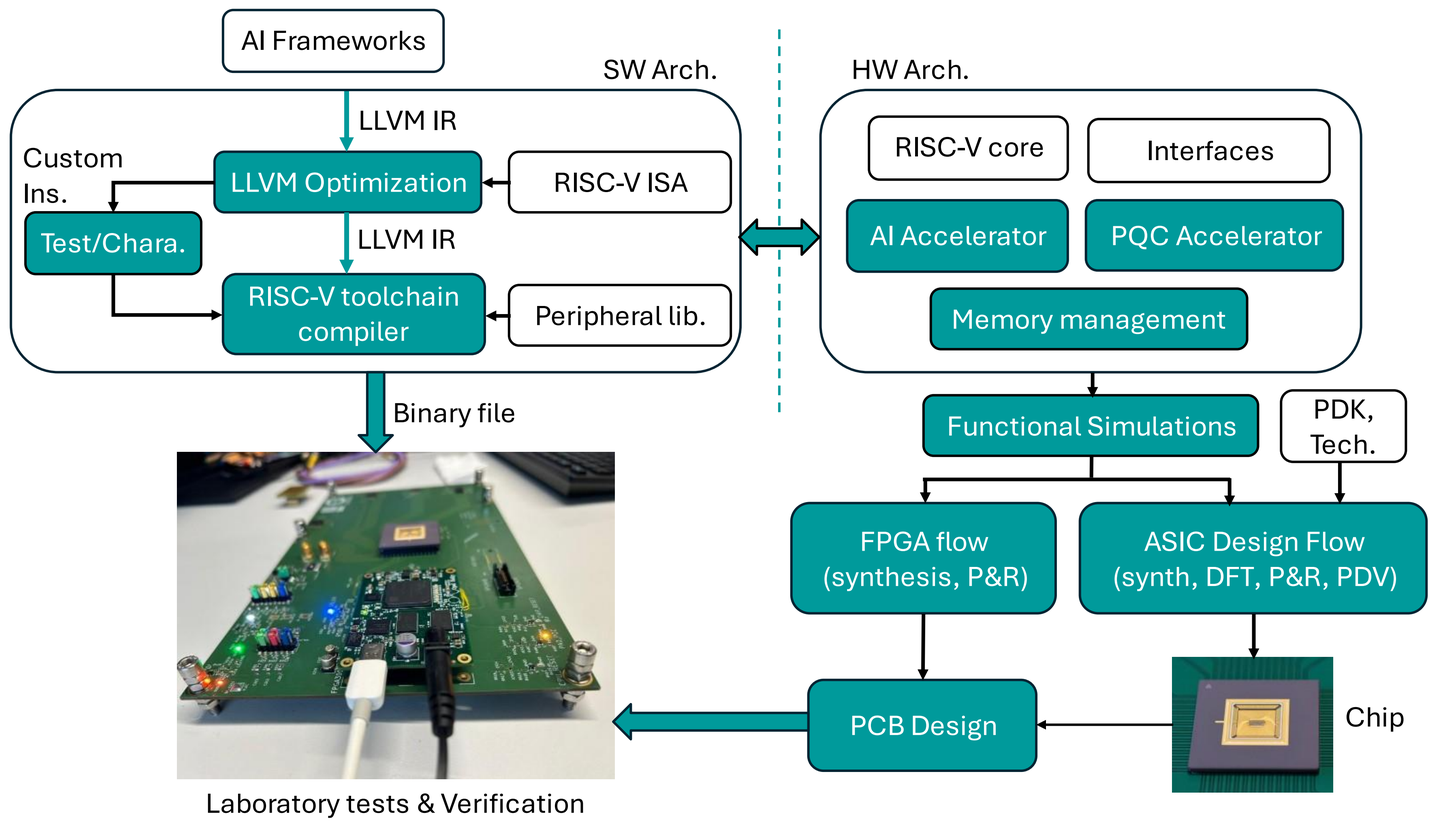
Ambily Suresh, Andrew Wilson, Diego Gigena-Ivanovich, Manuel Freiberger, Willibald Krenn,
Silicon Austria Labs
✉ *ambily.suresh@silicon-austria.com*

Research Focus

- Accelerating neural network processing at the edge
- Optimizing for classical AI applications
- Integration with RISC-V ecosystem

The ISOLDE Chips-JU Project

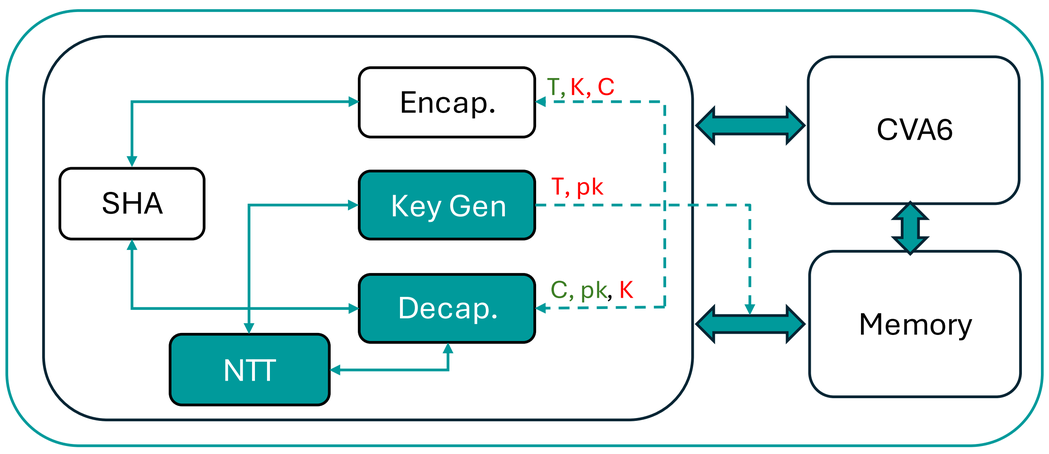
- Enhance European high-performance RISC-V-based SoCs
- Development of advanced architectures, novel accelerators, and reusable IPs



Scope of the RISC-V based research at SAL

The McEliece Cryptosystem

- Code-based cryptography – Finalist in the NIST PQC standardization efforts
- Large key sizes - Handling and storage of large memory
- Proven resilience for high-security applications (military, space)
- Accelerating primitives in the open-source HW implementations (e.g., Chen et al, 2022)



Architecture of our McEliece PQC Implementation

Module	Inputs	Outputs	Major steps	Primitives to accelerate
Encap	Public key	Cipher text, Session key	FixedWeight, Encode, Hash	Keccak
Decap	Cipher text, private key	Session key	FieldOrdering, Decode, Hash	NTT, Keccak
Keygen	None/McEliece parameters	Public key, private key	KeyGen, FieldOrdering, Irreducible, Hash	NTT, Systemizer, Keccak

Key algorithms and primitives in the implementation

Module	LUTs	Latency	Time x Area
Encap	977	0.14 ms	0.13
Decap	17109	0.16 ms	2.74
Keygen	26674	1.16 ms	30.94

Performance for mceliece348864 for VCU128

In Future

- Integration of the FW and SW framework (LLVM/MLIR)
- SoC for acceleration of distributed learning tasks via Quantum-Safe Cryptography

Extended abstract

Selected References

- Po-Jen Chen et al, *Complete and improved FPGA implementation of Classic McEliece*. IACR Transactions on Cryptographic Hardware and Embedded Systems, page 71–113, 2022
- Rodríguez N., et al. *RISC-V based SoC platform for neural network acceleration*. Argentine Conference on Electronics, page 142–147, 2024
- https://docs.openhwgroup.org/projects/cva6-user-manual/index.html

This research received funding from the Austrian Research Promotion Agency and the Austrian ministry for Climate Action, Environment, Energy, Mobility, Innovation, and Technology under project FO999899263 and the Chips Joint Undertaking and its members Austria, Czechia, France, Germany, Italy, Romania, Spain, Sweden, and Switzerland under the ISOLDE project (no. 101112274)

Silicon Austria Labs GmbH
Sandgasse 34, 8010 Graz, Austria
www.silicon-austria-labs.com
contact@silicon-austria.com