A Hardware Accelerator for Secure Communication through Post Quantum Cryptography

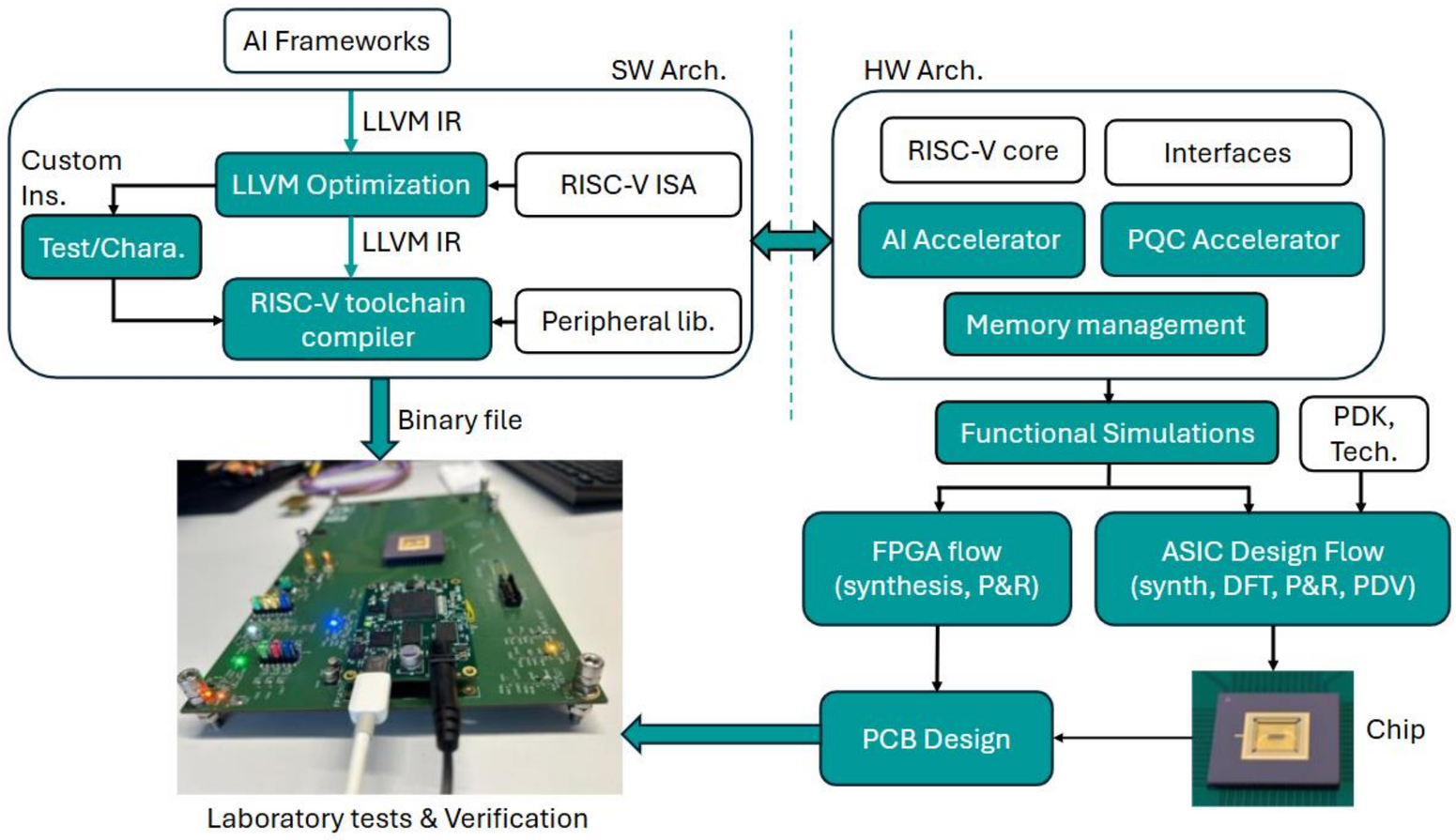
Ambily Suresh, Andrew Wilson, Diego Gigena-Ivanovich, Manuel Freiberger, Willibald Krenn, Silicon Austria Labs GmbH

ambily.suresh@silicon-austria.com

Research Focus

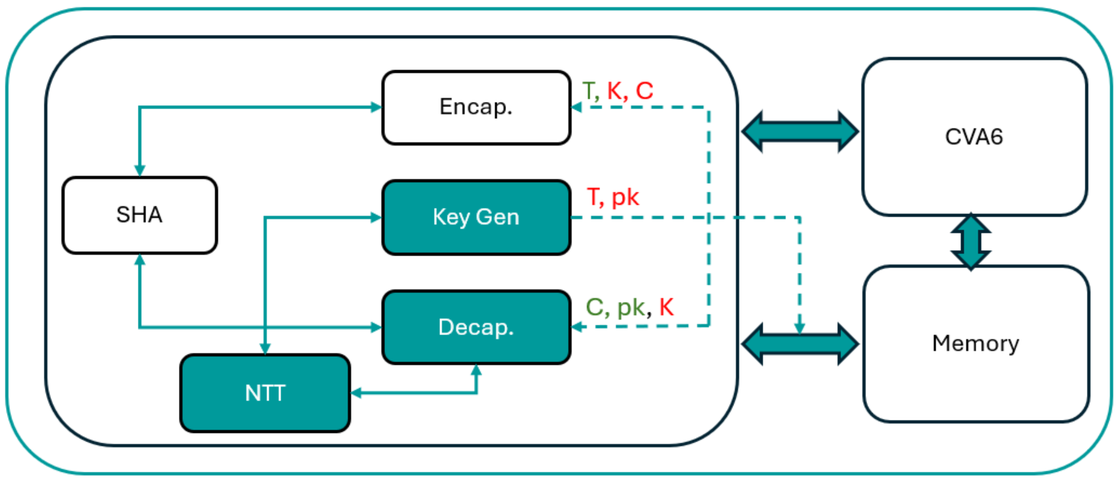
- Enhancing neural network processing at the edge
- Optimizing for classical AI applications
- Seamless integration with the RISC-V ecosystem

Space presents one of the most challenging edge application
- Resource constrains
- Harsh environment
- Reliability and security needs



The McEliece Cryptosystem

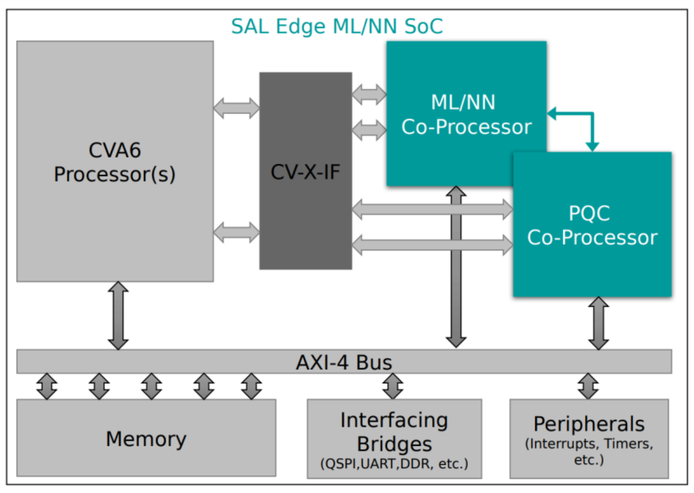
- Code-based cryptography – Finalist in the NIST PQC standardization efforts
- Proven resilience for high-security applications (military, space)
- Relies on the Syndrome Decoding problem – Large key sizes - Handling and storage of large memory
- Accelerating primitives in the open-source HW implementations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



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

In future

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



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
- Nicolás Rodríguez, 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 the Chips Joint Undertaking and its members Austria, Czechia, France, Germany, Italy, Romania, Spain, Sweden, 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