A RISC-V BASED ACCELERATOR FOR POST QUANTUM CRYPTOGRAPHY

Ambily Suresh, Manuel Freiberger, Andrew Wilson,
Diego Gigena-Ivanovich, Willibald Krenn

Funded by

Federal Ministry
Innovation, Mobility
and Infrastructure
Republic of Austria

FFG

Das Land
Steiermark

SFG

LAND KÄRNTEN

ober
österreich

Member of
UAR INNOVATION
NETWORK

SAL
SILICON AUSTRIA LABS

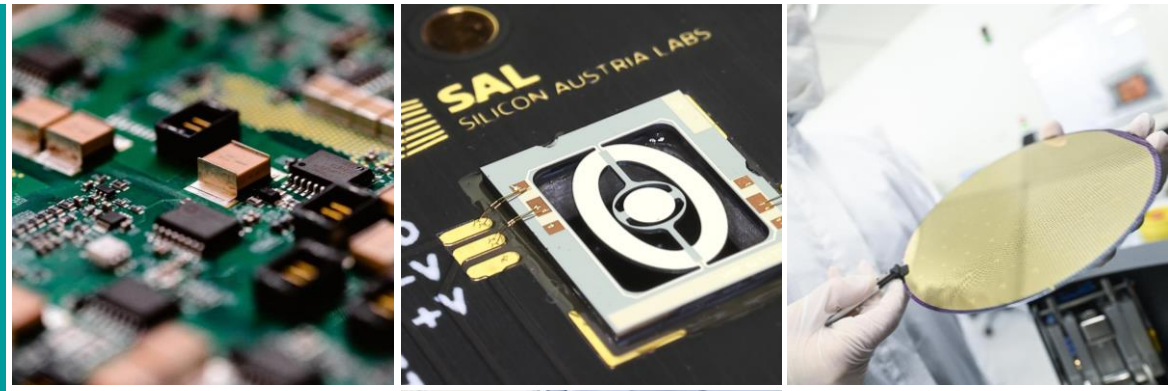
OVERVIEW

SILICON AUSTRIA LABS

What do we do?

Silicon Austria Labs (SAL), established in 2018, is a European **R&D center** with a focus on the development of efficient and trustworthy technologies in the field of **electronic systems.**

- Industry-oriented research
- R&D services
- Well-equipped research infrastructures
- Customized opportunities for co-operation



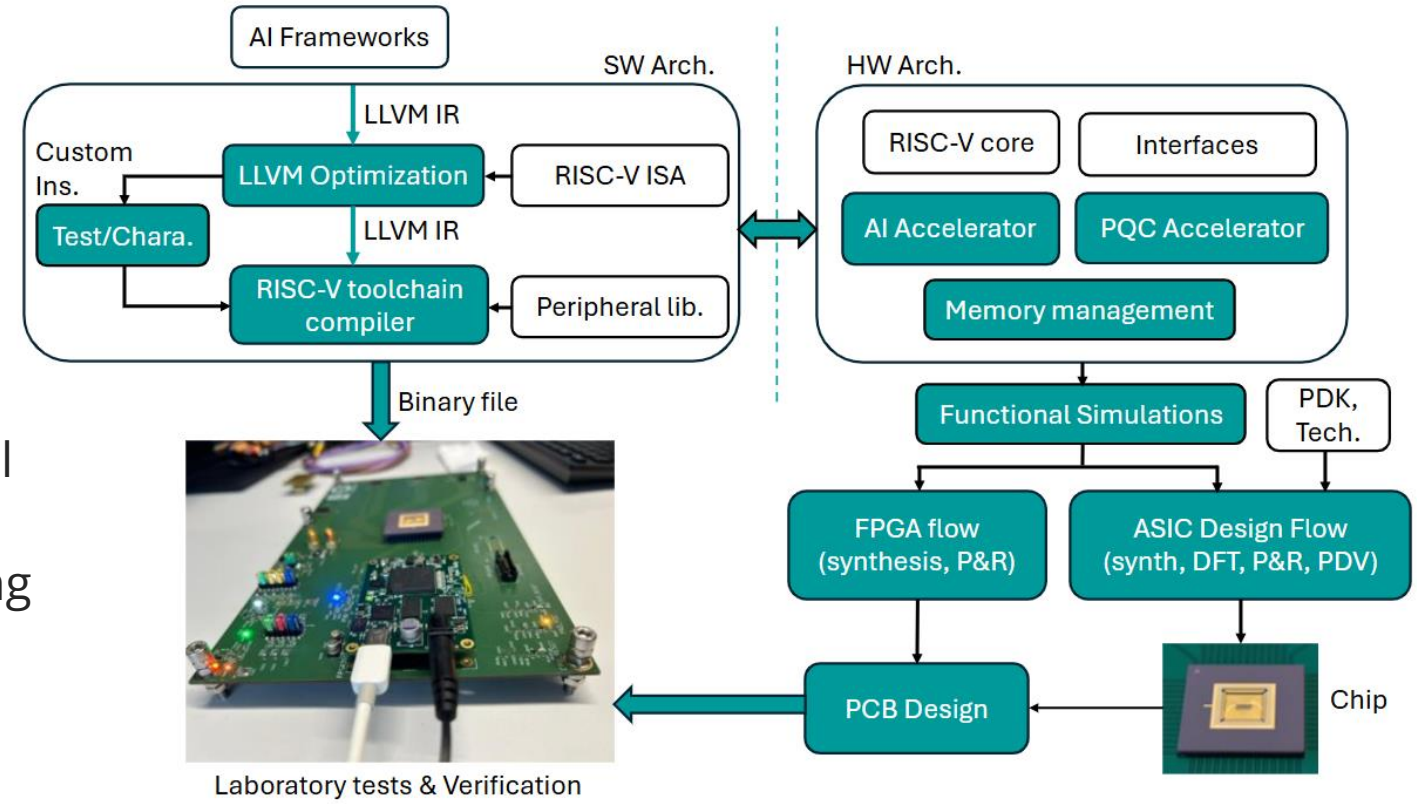
THE ISOLDE PROJECT

- H**I**gh Performance, **S**afe, Secure, **O**pen-Source **L**everaged RISC-V **D**omain-Specific **E**cosystems
- Chips-JU + FFG funding for Austrian partners
- May 2023 to April 2026
- Around 40 partners from 9 countries
- Enhance European high-performance RISC-V-based Systems-on-a-Chip (SoC)
- Development of advanced architectures, novel accelerators, and reusable IPs

*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**)*

RISC-V TOPICS @ SAL

- **Post Quantum Cryptography**
  - Evaluate candidate algorithms for hardware implementation
  - Quantum-safe encryption for resource constrained, edge environments
- **Edge AI**
  - Minimize privacy risks through local AI acceleration.
  - Speed up neural network processing for efficient, low-latency AI on edge devices
- **Integration with RISC-V platform**
  - Customizable and cost-effective RC
  - HW-SW co-development for custom instructions



Applications: Automotive, IoT

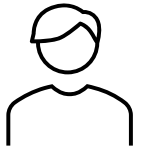
POST QUANTUM CRYPTOGRAPHY

- "...secure against both quantum and classical computers..."
- "...interoperate with existing communications protocols and networks..."
- Candidates from the NIST PQC standardization process

Hash-based	Code-based	Lattice-based	Other types
One-time signatures	Error correcting codes	Nearest point in lattices	Multivariate, Isogeny
SPHINCS+, XMSS	Classic McEliece, BIKE, HQC	CRYSTALS Kyber, Dilithium, Falcon	Rainbow, SIKE

- Final selection in 2024 - CRYSTALS Kyber (For general encryption), CRYSTALS Dilithium, Falcon, and SPHINCS+ (Digital Signatures)

THE MCELIECE CRYPTO SYSTEM



m … message (binary vector)

S … invertible matrix

G … generator matrix (error-correcting code)

P … permutation matrix

$\hat{G}$ ←

$\hat{G} = SGP$

$c = m\hat{G} + e_t$ →

c

t bits of error

$c = m\hat{G} + e_t$

$c = mSGP + e_t$

t bits of error

$cP^{-1} = (mSGP + e_t)P^{-1} = mSG + e_tP^{-1}$

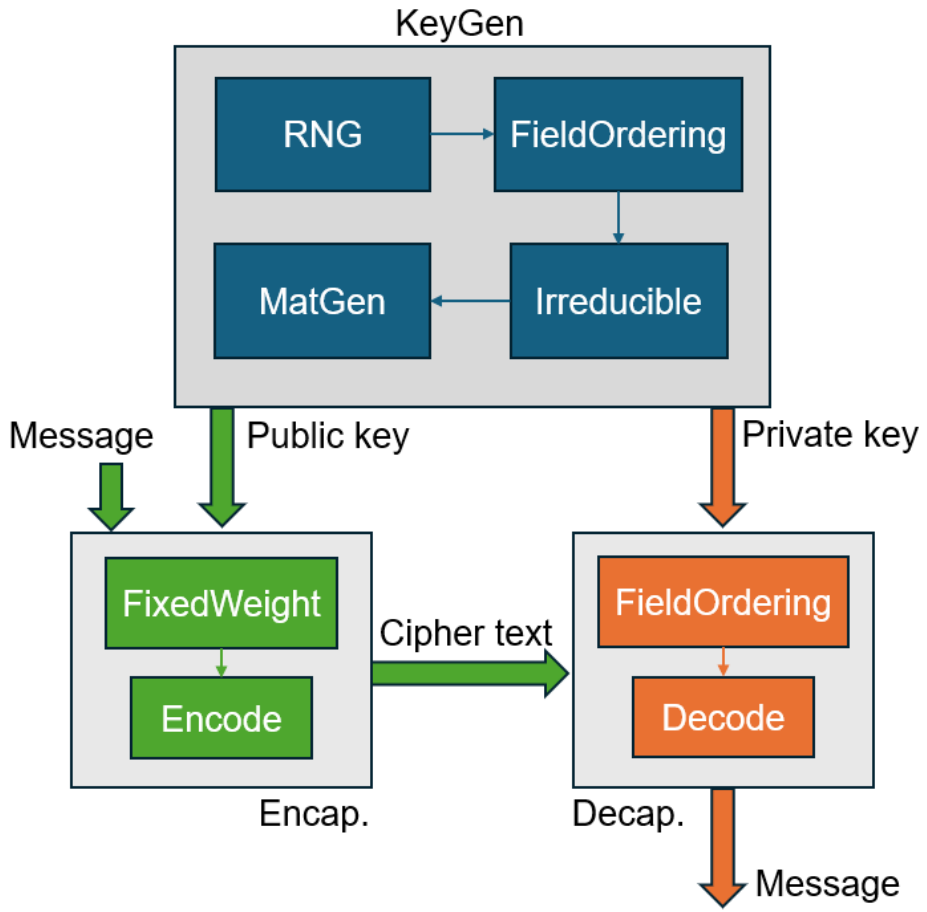
$c' = mS$

$c'S^{-1} = m$ ✓

THE MCELIECE CRYPTO SYSTEM

- Fast encrypt. & decrypt., hardened against SCA
- Proven resilience (since 1978) for high-security applications (military, space)
- Large key sizes - Handling of large memory

Parameter Set	Security Level	Public Key	Private Key Size	Ciphertext Size
mceliece348864	1 (~128-bit)	256 KB	6,492 bytes	128 bytes
mceliece460896	3 (~192-bit)	512 KB	13,060 bytes	188 bytes
mceliece6688128	5 (~256-bit)	1.0 MB	13,892 bytes	240 bytes
mceliece6960119	Level 5	1.0 MB	13,948 bytes	226 bytes
mceliece8192128	Level 5	1.3 MB	14,120 bytes	240 bytes

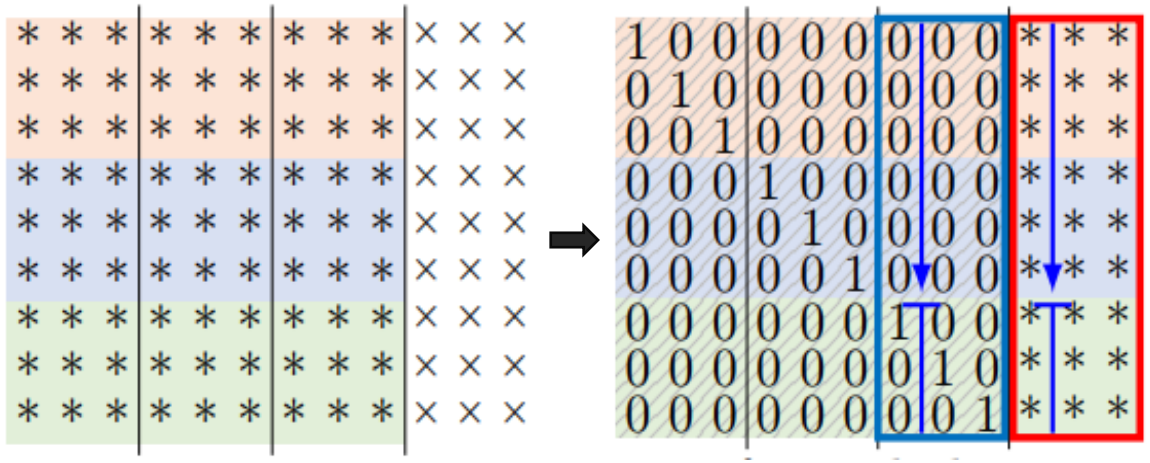


IMPLEMENTATION CHALLENGES

SAL SILICON AUSTRIA LABS

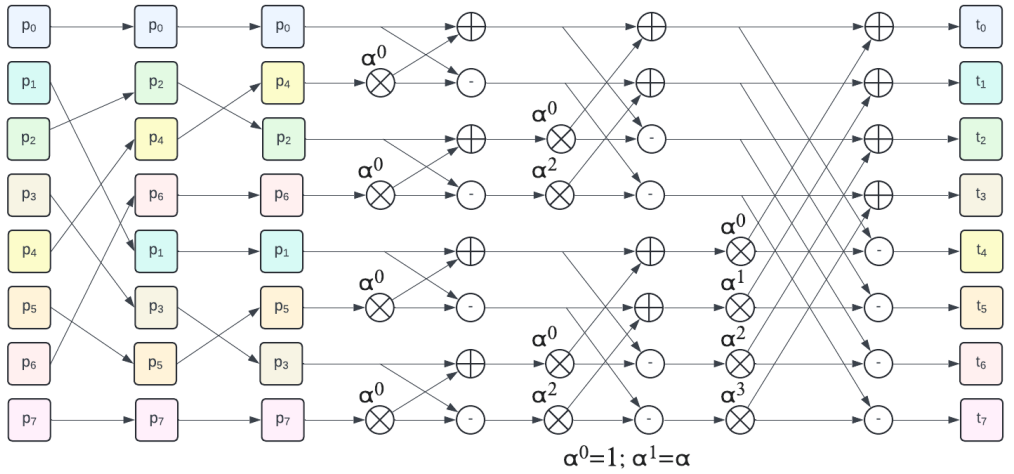
Parameter Set	Security Level	m	n	t	k	n − k	Public Key
mceliece348864	1 (128-bit)	12	3488	64	2720	768	768 × 2720
mceliece460896	3 (192-bit)	13	4608	96	3359	1249	1249 × 3359
mceliece6688128	5 (256-bit)	13	6688	128	5024	1664	1664 × 5024
mceliece6960119	5	13	6960	119	5283	1677	1677 × 5283
mceliece8192128	5	13	8192	128	6528	1664	1664 × 6528

Matrix systemization



WSN '16, '17, '18, Chen et al. '23

Polynomial evaluation

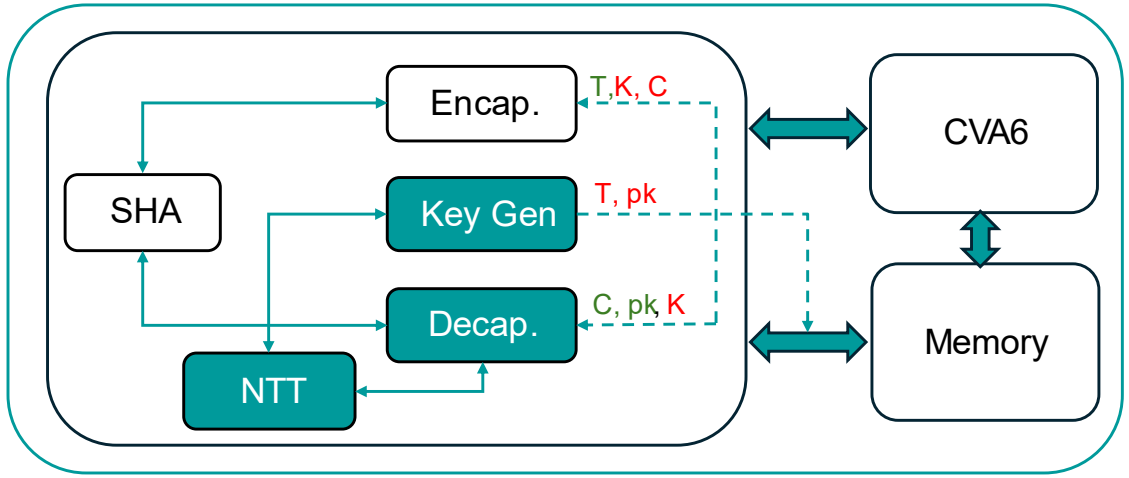


https://fprox.substack.com

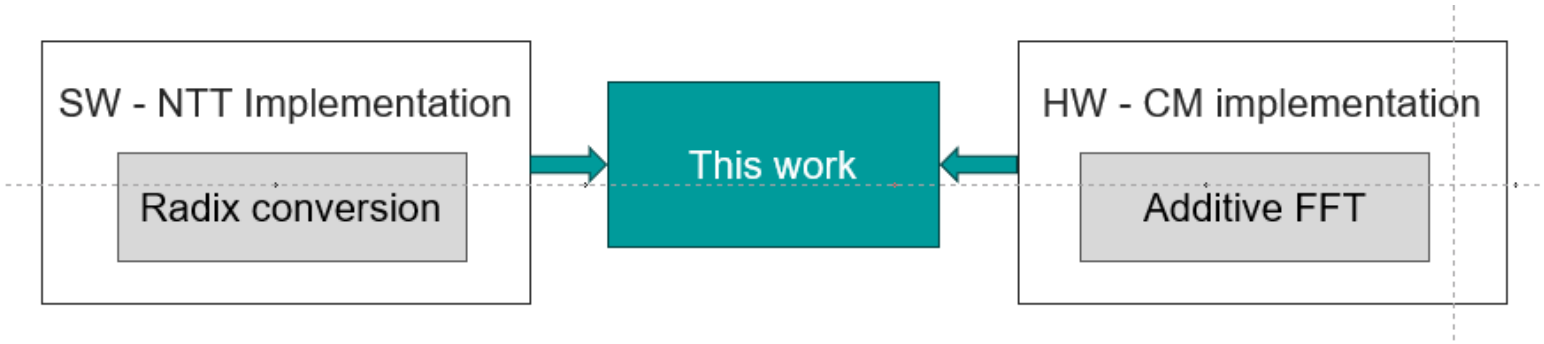
ACCELERATOR IMPLEMENTATION

Objectives

- **Accelerating primitives** in current open-source HW & SW implementations
- This work – optimizing the FFT module used in
  - Keygen for the parity check matrix H
  - Decap for the error locator polynomial $\sigma(x)$
  - Based on NTT implementations
- Optimize the timing and area performance



Open-source IPs are shown in white
Blocks from SAL are highlighted



HARDWARE IMPLEMENTATION

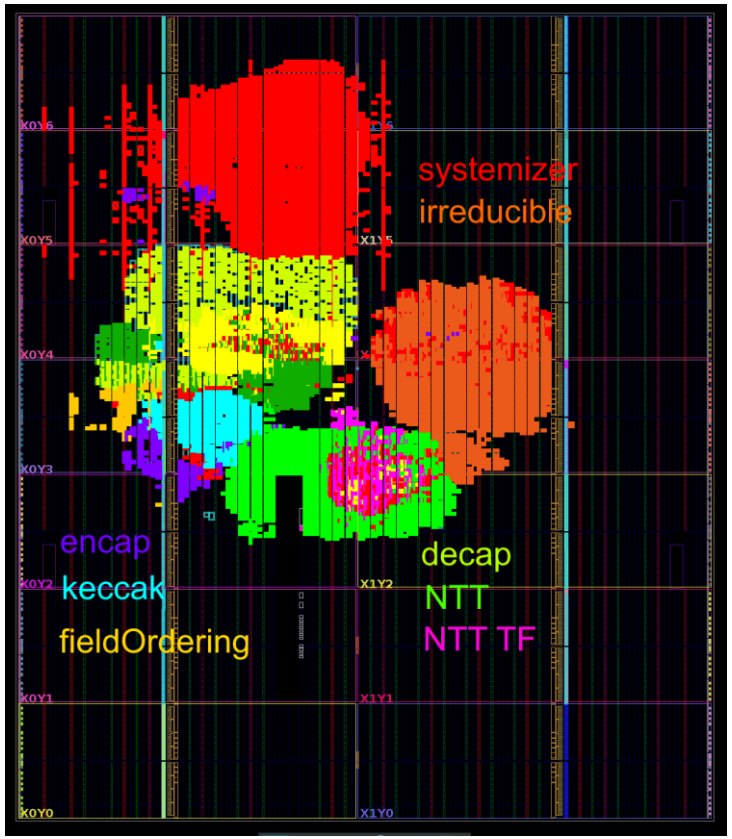
SAL SILICON AUSTRIA LABS

Current Status

- Simulations and synthesis for AMD **VCU128** FPGA
  - the ISOLDE automotive demonstrator
  - Integration with CVA6[1] core with an AXI4[2] interface – IPs from ISOLDE and TRISTAN
  - Loosely coupled accelerator
- SW codesign with a reference C implementation
  - Exploring CV-X-IF based coprocessor

Module	LUTs	Latency	Time x Area	Speed-up*
Encap	977	0.14 ms	0.13	-
Decap	17109	0.16 ms	2.74	1.6
Keygen	26674	1.16 ms	30.94	1.3

* comparing cycle counts to SOTA Taylor series-based algorithm



Vivado Implementation for mceliece348864 in VCU128

1: https://github.com/openhwgroup/cva6
2: https://github.com/pulp-platform/axi

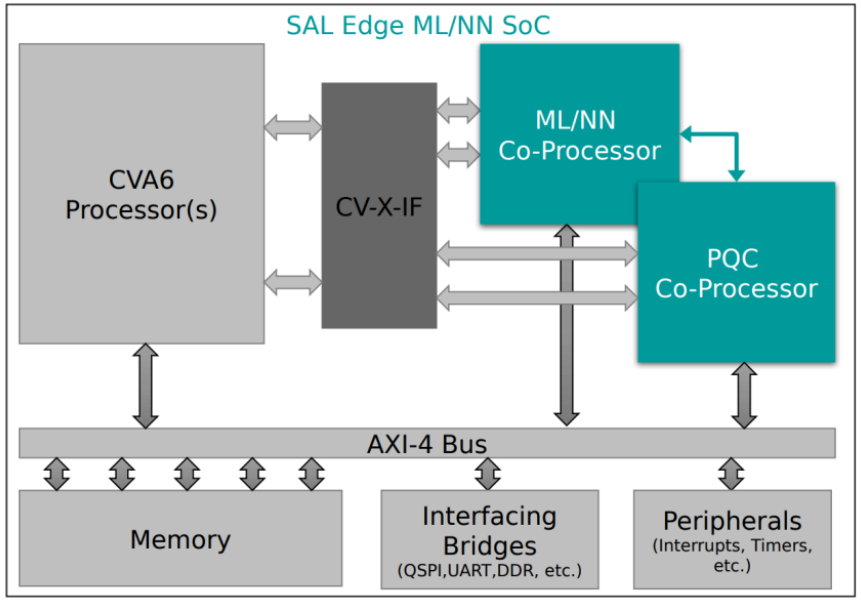
SUMMARY AND FUTURE

- The CM cryptosystem has proven resilience despite the memory challenges
- Multiple operations to optimize
  - Primitives can be reused for multiple applications – PQC or otherwise
- Current design is WIP – but feasible approach for embedded HW in timing & area estimates
- RISC-V based design – seamless integration of toolchains, simulator, peripheral IPs
  - Tightly coupled coprocessors through X-IF
- Chips-JU projects play a crucial role in advancing the RISC-V ecosystem

Visit our poster - P1.1.10!

Future plans

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



ETH zürich

Barcelona Supercomputing Center
Centro Nacional de Supercomputación

fentISS

Codasip

CONSOLINNO energy

SAL SILICON AUSTRIA LABS

Continental

Beia CONSULT INTERNATIONAL

Bytefabrik.AI

IMT

HM

E4 COMPUTER ENGINEERING

THALES
Building a future we can all trust

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

SILVACO

UNIVERSITÄT ZU LÜBECK

RAPITA SYSTEMS
A DANLAW COMPANY

SAL SILICON AUSTRIA LABS

intel

ACP AG
Advanced Circuit Pursuit

LEONARDO

NXP

Infineon

FZI

POLITECNICO DI TORINO

POLITECNICO MILANO 1863

tobii

SYSGO
EMBEDDING INNOVATIONS

OFFIS
INSTITUT FÜR INFORMATIK

www.isolde-project.eu

Contact: info@isolde-project.eu

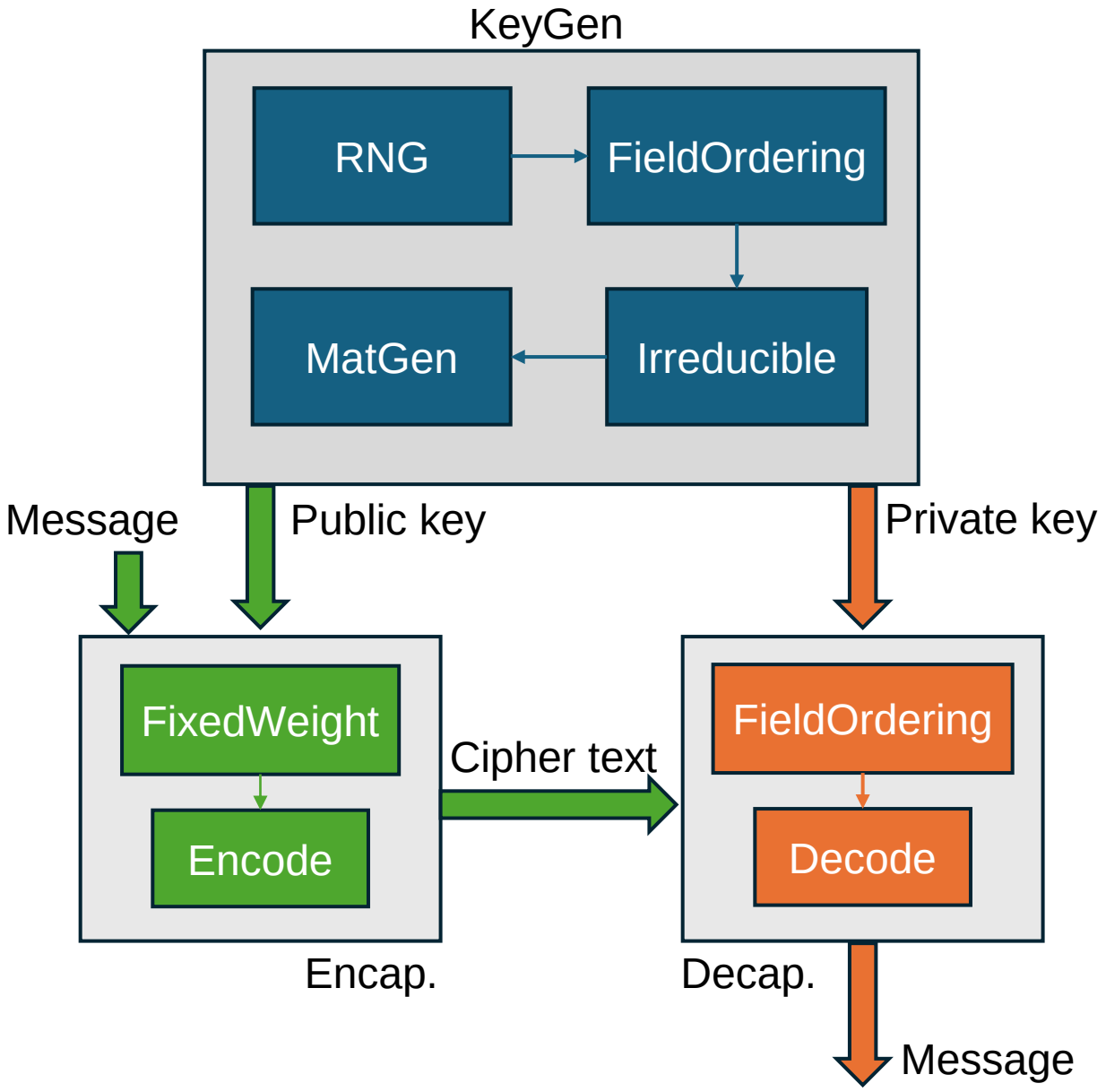
www.linkedin.com/company/isolde-project/

SAL
SILICON AUSTRIA LABS

UNFOLD THE FUTURE

WWW.SILICON-AUSTRIA-LABS.COM

Hash-based	Code-based	Lattice-based	Other types
One-time signatures	Error correcting codes	Nearest point in lattices	Multivariate, Isogeny
SPHINCS+, XMSS	Classic McEliece, BIKE, HQC	CRYSTALS Kyber, Dilithium, Falcon	Rainbow, SIKE



SAL
SILICON AUSTRIA LABS


SW - NTT Implementation
Radix conversion
This work
HW - CM implementation
Additive FFT