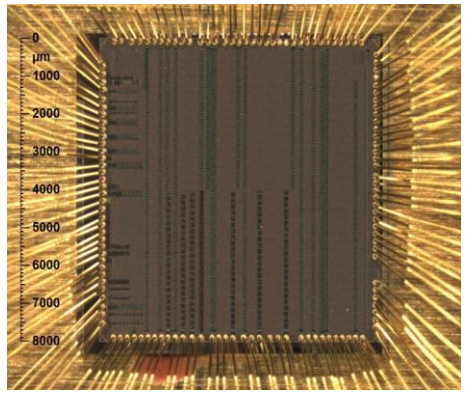
VASCO: ASIC Test Platform for Hardware Security on FD-SOI

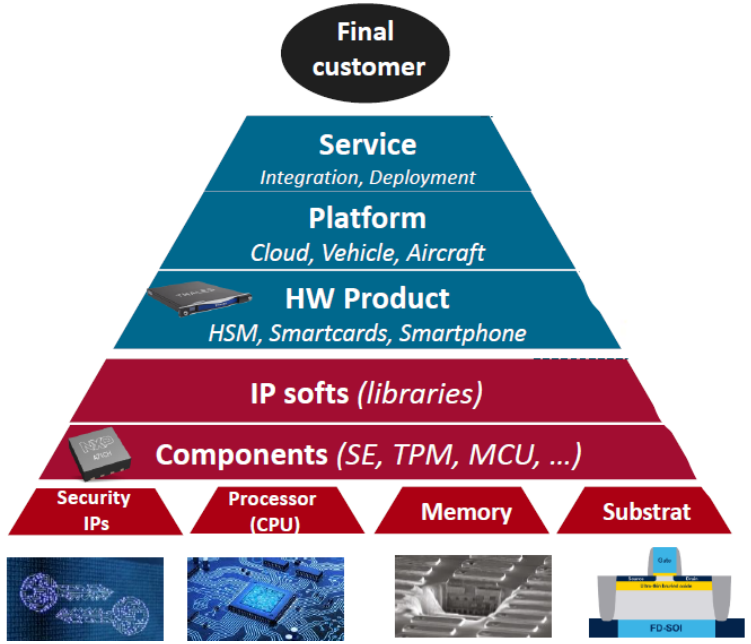
S. Di Matteo[1, 2], R. Alidori[2], L. Benea[1], M. Carmona[1], M. El Majihi[1] , F. Lepin[2], F. Pebay-Peyroula[1], M. Pezzin[2], S. Pontié[1,3], M. Ramirez-Corrales[2], O. Savry[1], E. Valea[2], R. Wacquez[1, 3]

(1) Univ. Grenoble Alpes, CEA, Leti F-38000 Grenoble, France
(2) Univ. Grenoble Alpes, CEA, List F-38000 Grenoble, France
(3) CEA-Leti, Mines Saint-Étienne, Equipe Commune, F-13541 Gardanne, France



Root of Trust

Hardware is the foundation of the entire security chain. If compromised, no software or cryptographic protection holds — the attacker owns everything above.



A Changing Threat Landscape

- Side-channel & fault injection attacks
- Supply chain vulnerabilities
- Quantum computing on the horizon

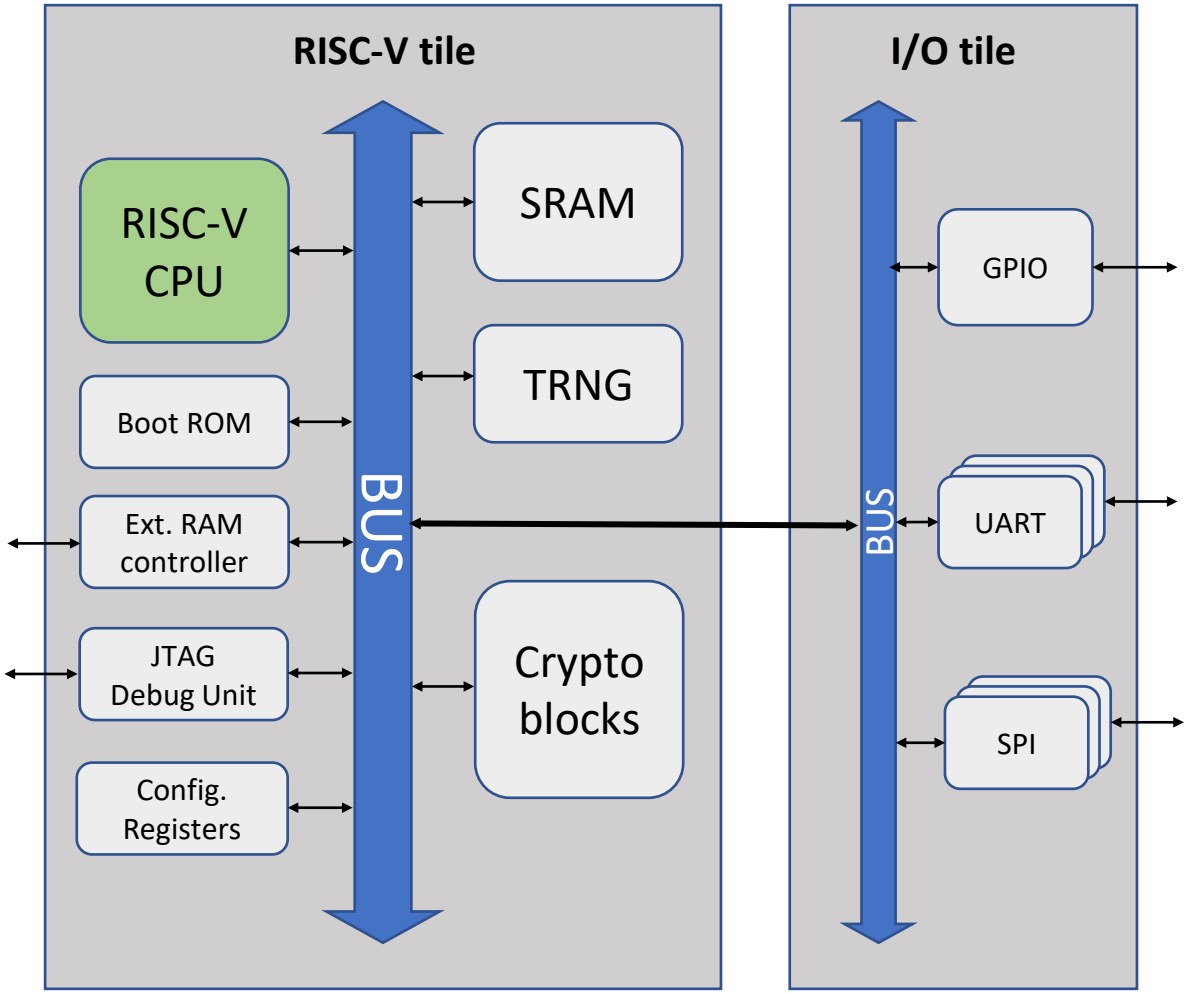
Response – New Technologies, new Standards

- Standards & certifications: NIST, ANSSI, CRA
- RISC-V for security
- FD-SOI for attacks resistance

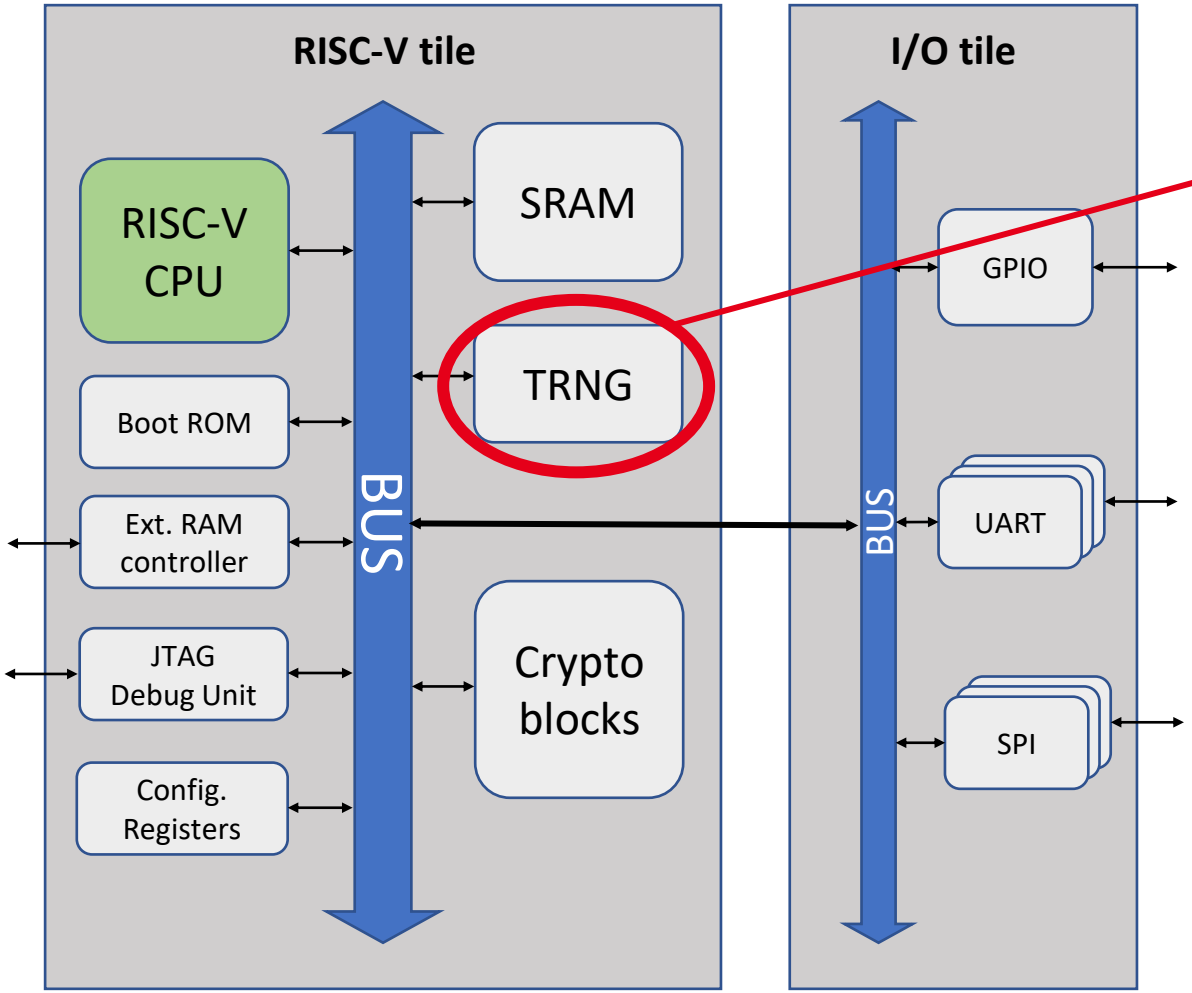
New Research Questions

- Security of RISC-V against attacks
- Security of the new PQC algorithms
- Models for Entropy Sources
- ….

Context: Security of Embedded Microcontrollers



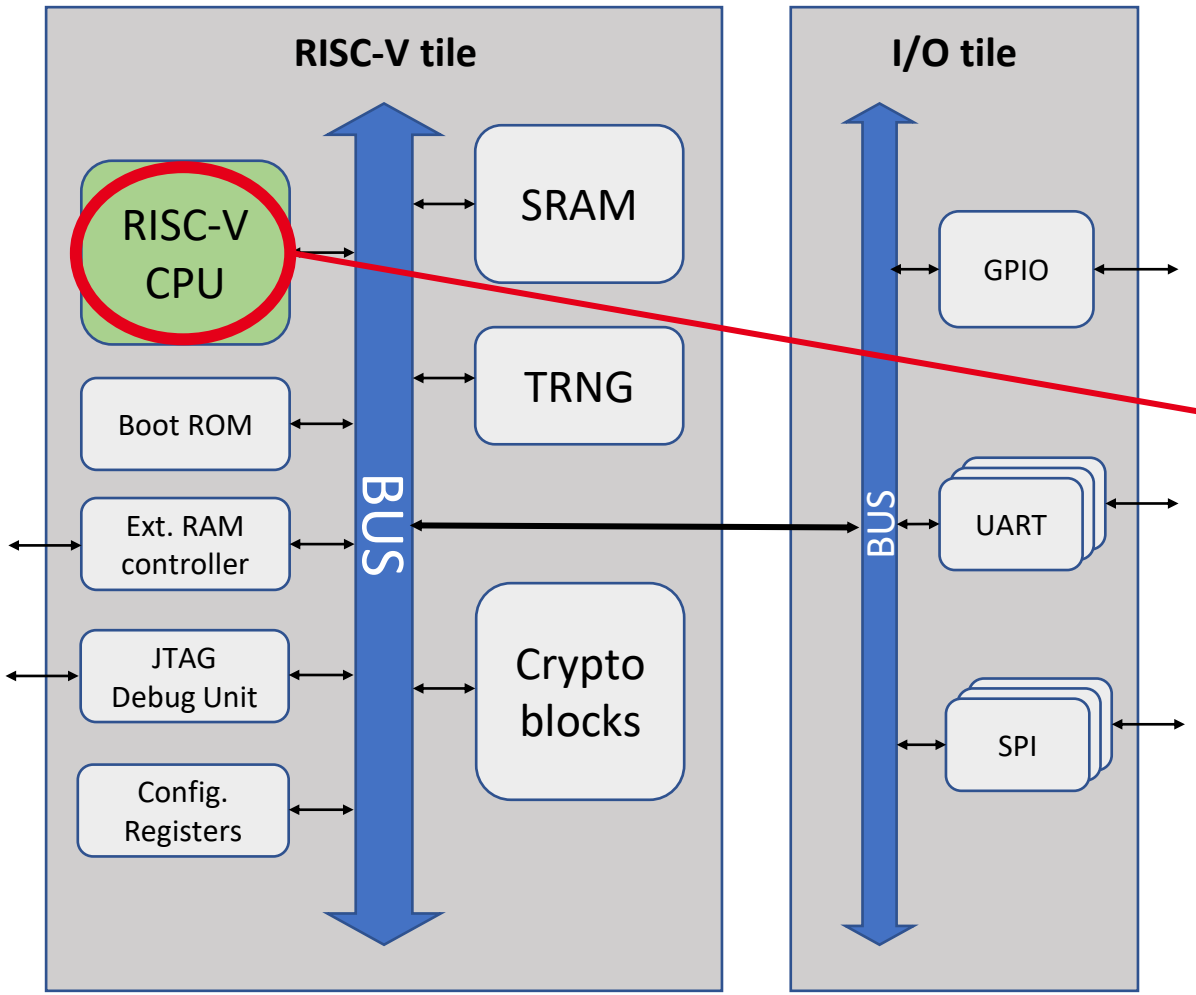
Context: Security of Embedded Microcontrollers



True Random Numbers Generator (TRNG)

- ❑ Fundamental entropy source
- ❑ Cryptographic primitives rely on high-quality TRNGs
- ❑ Standards require the stochastic model of the entropy source
- ❑ It is important to validate the entropy source model on ASIC

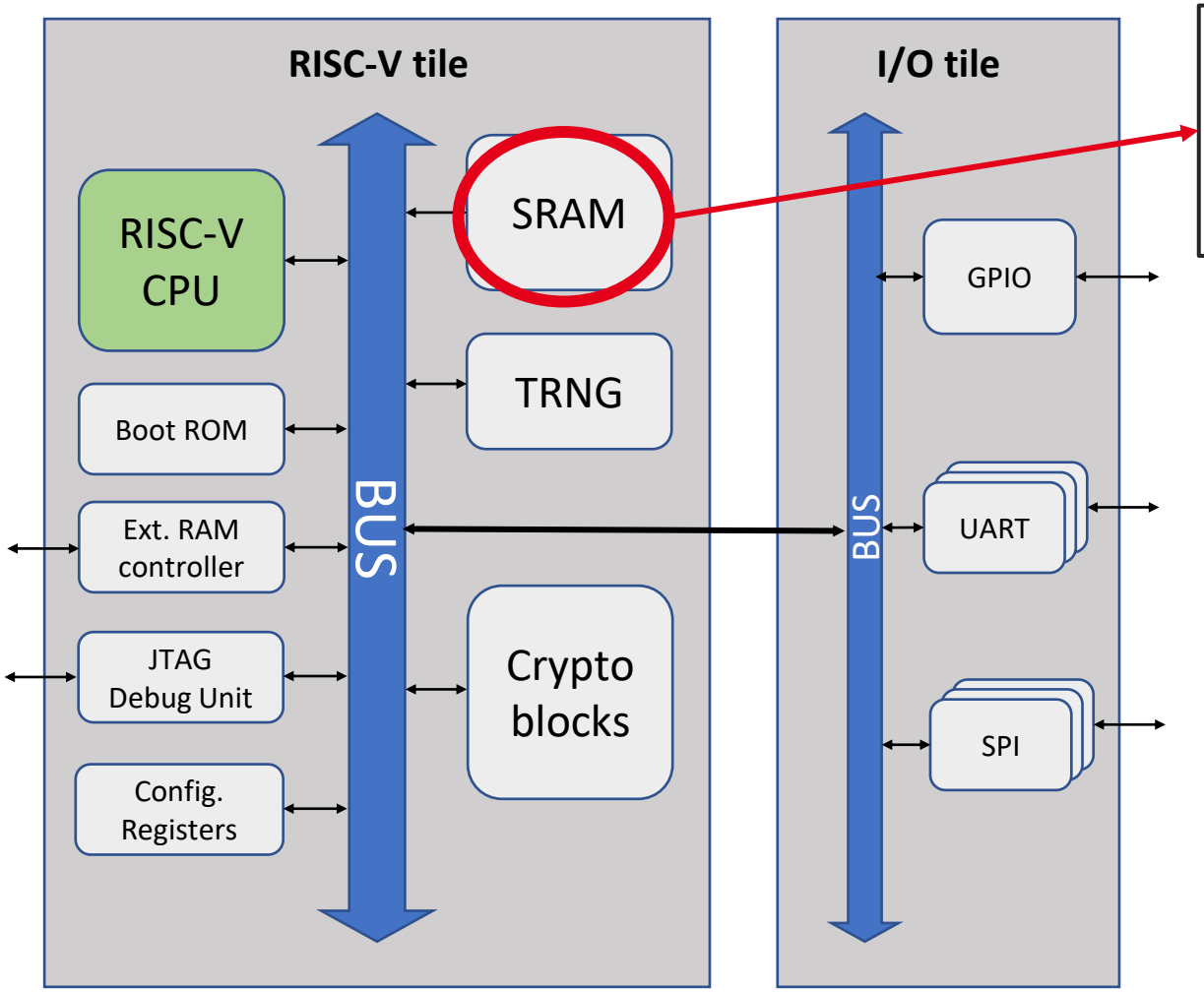
Context: Security of Embedded Microcontrollers



Secure RISC-V microarchitectures

- ❑ Some attacks rely on intrinsic properties of modern CPUs
- ❑ E.g., Spectre, Meltdown
- ❑ Need of rethinking microarchitectural security and validate on ASIC

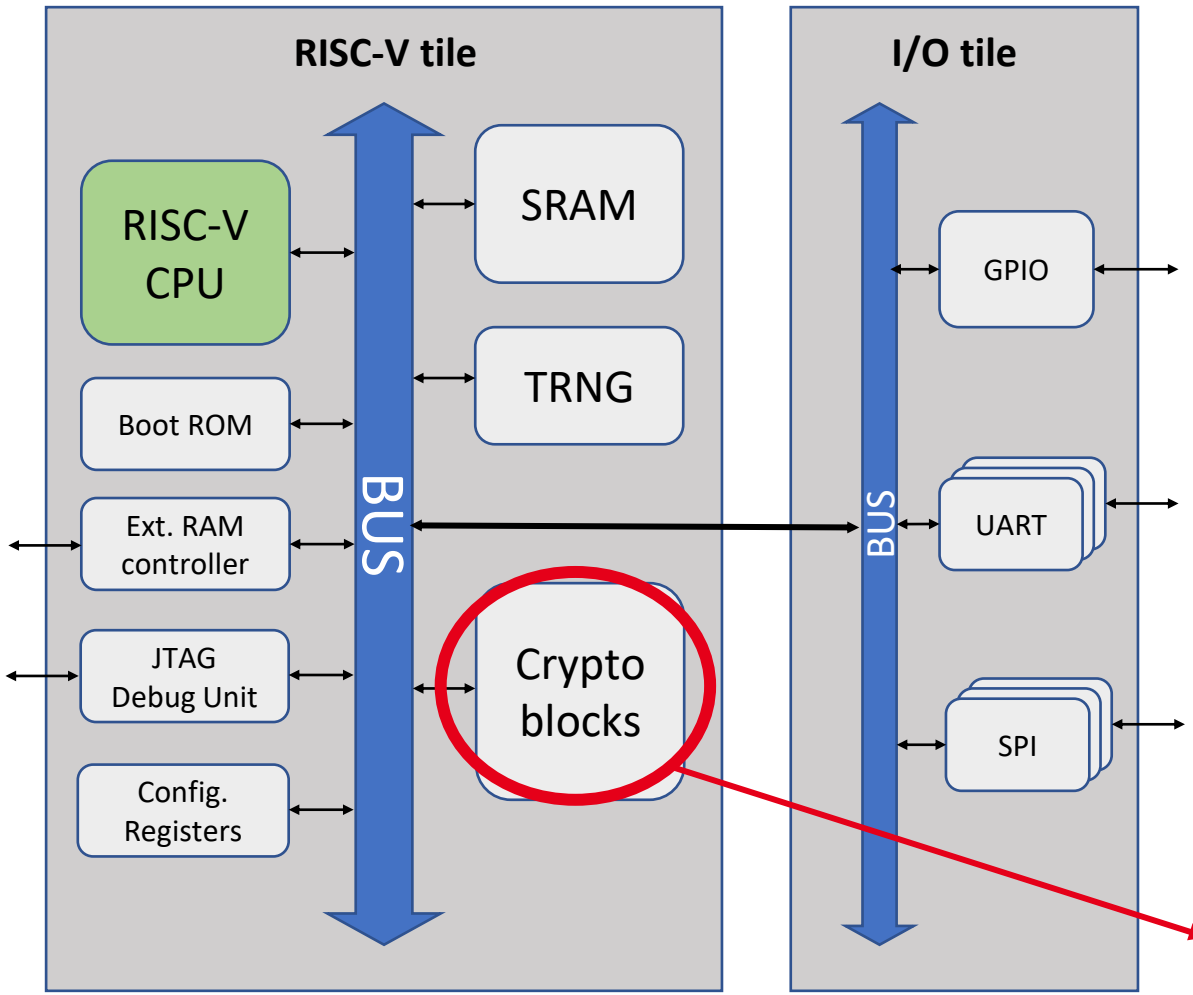
Context: Security of Embedded Microcontrollers



Secure memories

- Memories represent a huge attack surface due to their size
- E.g., cold-boot attacks, memory retention
- Need of developing techniques for tamper-proof secure memories

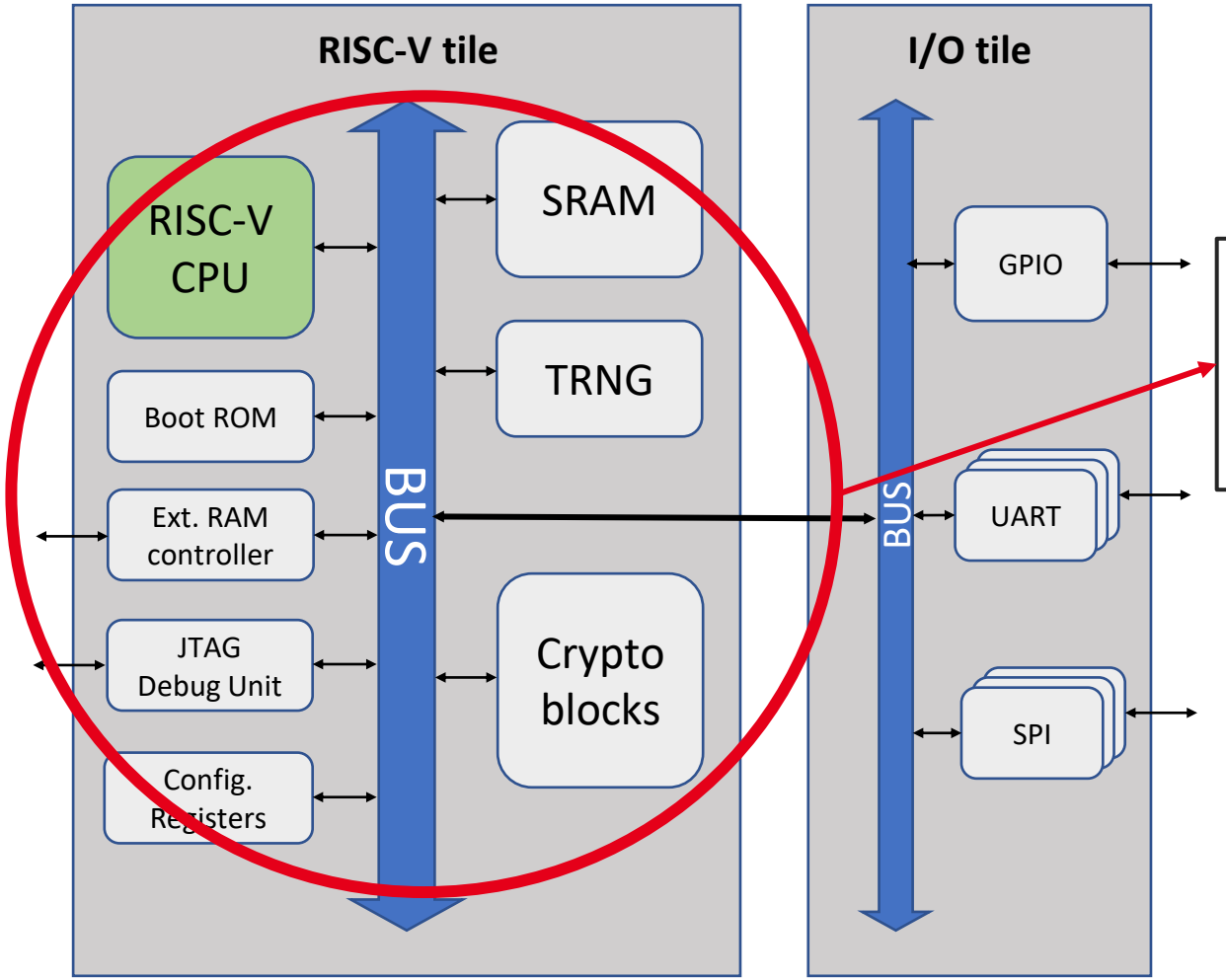
Context: Security of Embedded Microcontrollers



Post-Quantum Cryptography (PQC)

- ❑ Microcontrollers must be prepared to support PQC primitives
- ❑ Hardware accelerators for PQC need to be designed and validated
- ❑ Countermeasures against side-channel and fault injection attacks

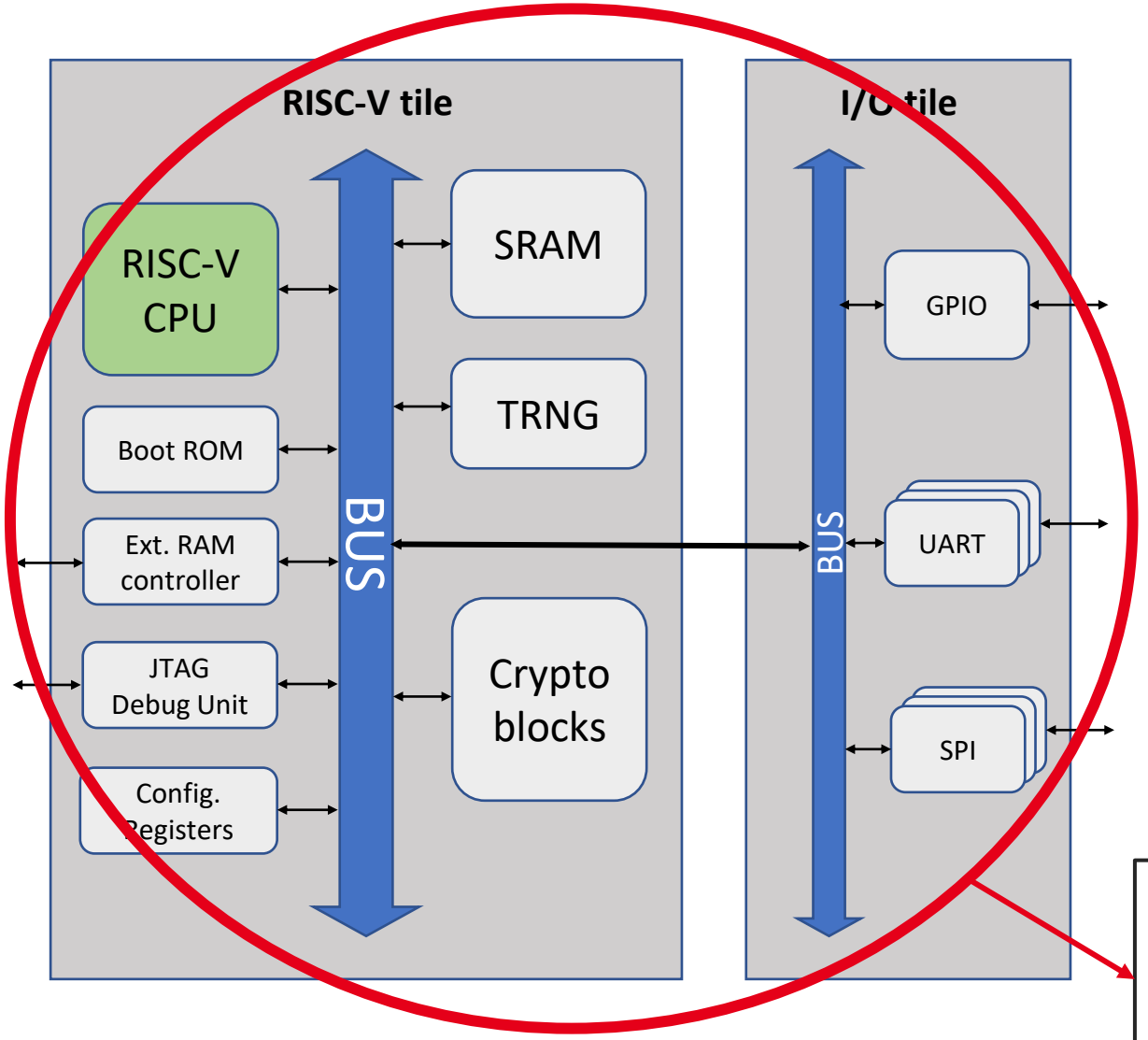
Context: Security of Embedded Microcontrollers



New architectural paradigms for security

- Hardware security can benefit of new architectural paradigms
- E.g., In-Memory Computing (IMC), Near-Memory Computing (NMC)
- They can boost the PQC transition on microcontrollers

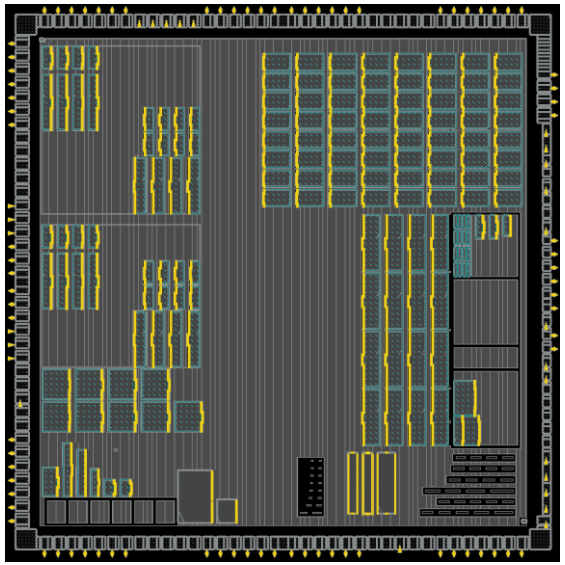
Context: Security of Embedded Microcontrollers



New semiconductor technologies

- ❑ Also the technology can play a key role in hardware security
- ❑ E.g., Fully-Depleted Silicon on Insulator (FD-SOI)
- ❑ ASIC validation of FD-SOI resistance to physical attacks

VASCO#3 General Architecture



Secure Memories

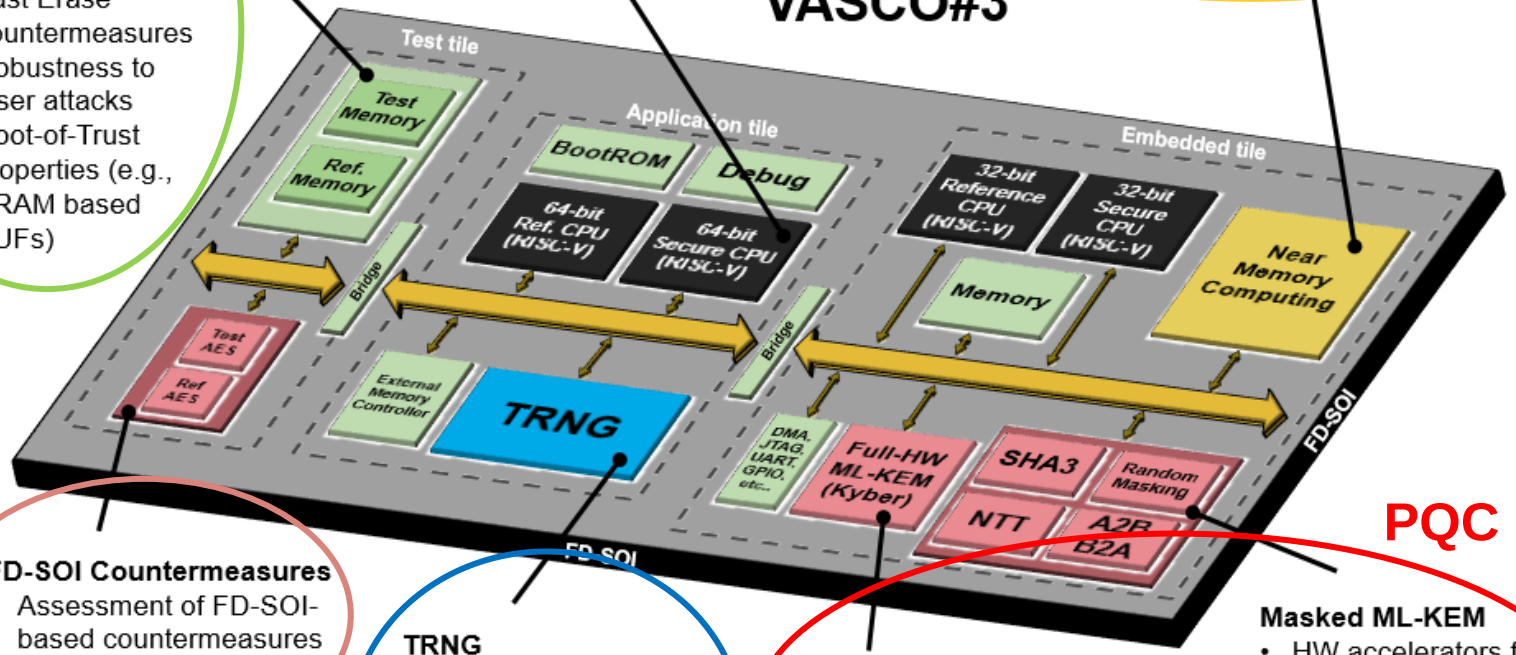
Test Memory
- Test platform for assessing security of FD-SOI SRAMs
- Fast Erase countermeasures
- Robustness to laser attacks
- Root-of-Trust properties (e.g., SRAM based PUFs)

RISC-V Security

Secure 64-bit RISC-V
- The pipeline is hardened against fault injection attacks using homomorphic integrity tags

Near Memory Computing

Computational SRAM
- Near-Memory Computing (NMC) technologies for crypto acceleration
- Enhanced perofrmances and energy efficiency for vector computing (e.g., PQC)



FD-SOI Countermeasures
- Assessment of FD-SOI-based countermeasures for cryptography

TRNG
- Characterization of new entropy sources
- ERO, MURO, COSO
- Adjustable back-gate voltage

Full-HW ML-KEM
- Full-HW implementation of ML-KEM (Kyber)

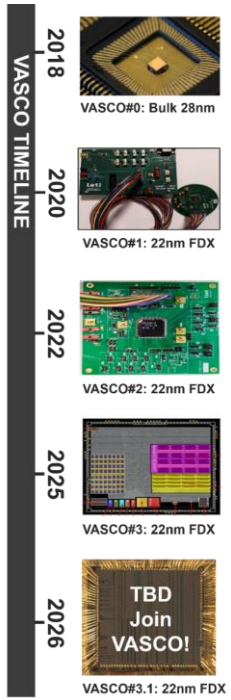
PQC

Masked ML-KEM
- HW accelerators for masked ML-KEM (Kyber)
- Securiy evaluation on FD-SOI

TRNG

VASCO: an ASIC Platform for Cybersecurity

VASCO is a **test** platform for Cybersecurity deleloped by **CEA** on **FD-SOI** technology



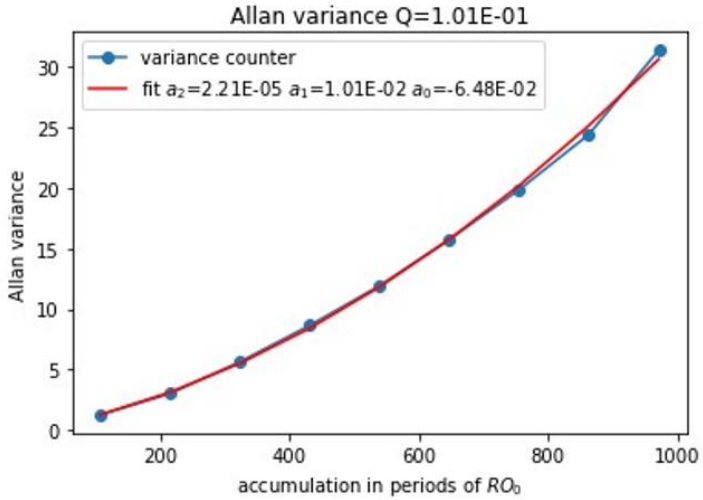
- Test HW and SW innovations
- Test the capabilities of FD-SOI for resilience against SCAs and FI attacks
- Anticipate the migration to FD-SOI for embedded systems
- Digital twin: use hardware to build models (e.g. TRNGs)
- Build security component at different abstraction levels
- Open to **parterships**

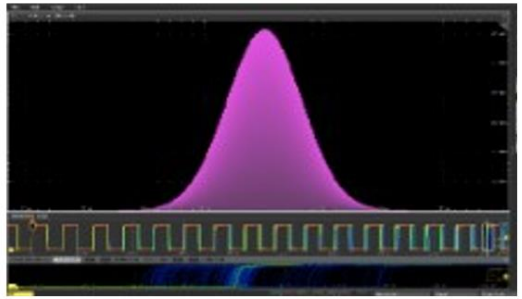
Secure protocols: TLS	**Software**	**Secure SW implementation of PQC**
Microarchitectural leakage of RISC-V	**Hardware**	**Secure HW accelerators for PQC**
True Random Number Generators		**Secure Memories**
Assessment and characterization on FD-SOI technology	**Technology**	**Countermeasures based on FD-SOI**

True Random Number Generators

- **Entropy source model required by TRNG Standards**
  - NIST SP 800-90B
  - BSI AIS-31

- **In VASCO#3 we validate the entropy source models on silicon**
  - Proposition of new Entropy Sources: ERO, MURO, COSO
  - Jitter analysis with pre-silicon simulations
  - Jitter measured is aligned with simulations
  - Flicker and Thermal noise coefficients are aligned with expectations

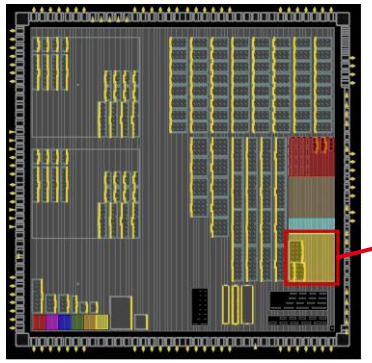


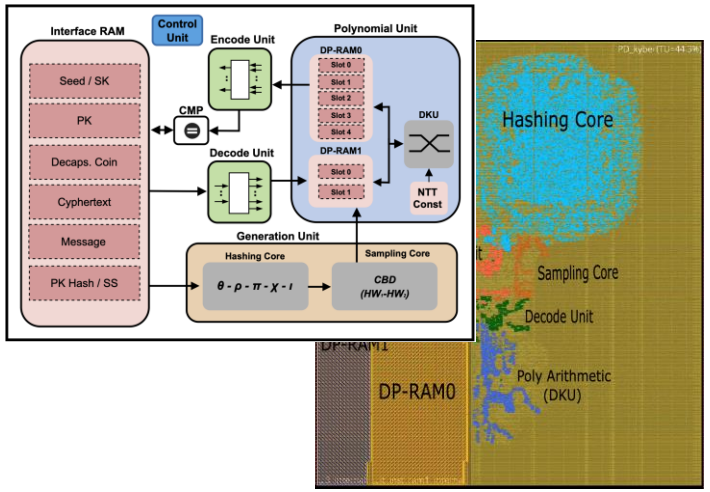


Jitter measurement of the Ring Osccilators

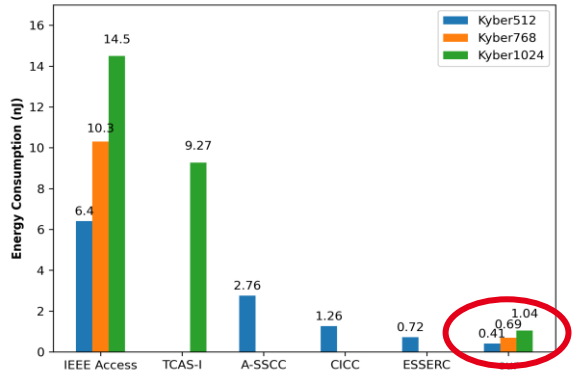
Post Quantum Cryptography

1. Full-HW ML-KEM

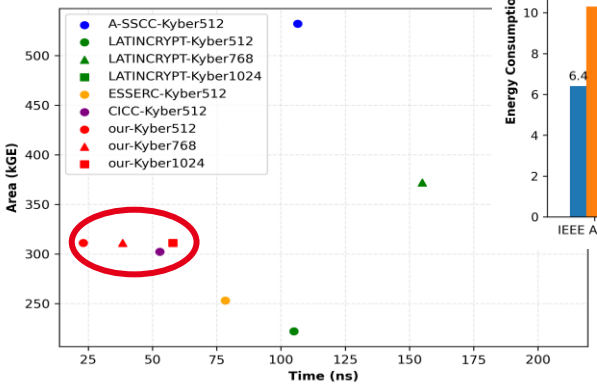




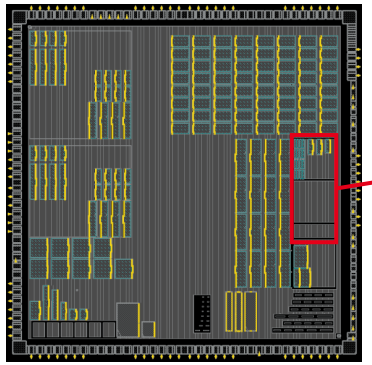
Lowest Energy Consumption



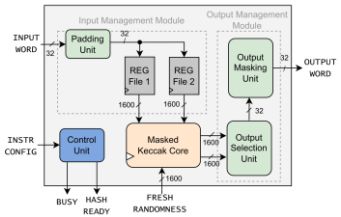
Best Area-Time



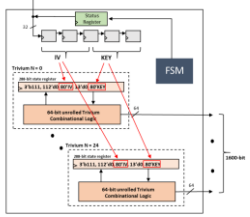
2. First Masked ML-KEM on ASIC



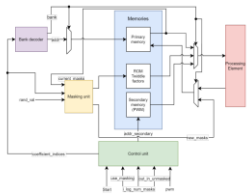
Masked SHA3



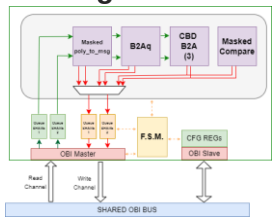
Randomness Generation



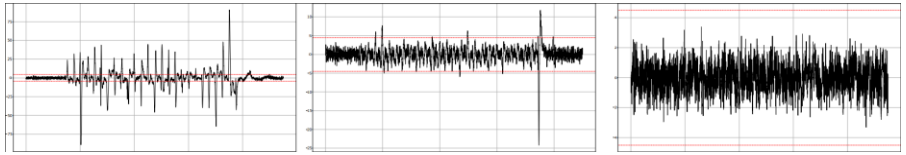
NTT



Masking Conversions



Work	Algorithm	Area	Technology	C.C.	Speed
Our	Masked ML-KEM-768	560 kGE	FD-SOI 22nm	285 249	0,95 ms
[1]	Masked ML-KEM-768	597 kGE	UMC 65nm	1 235 460	15.83 ms

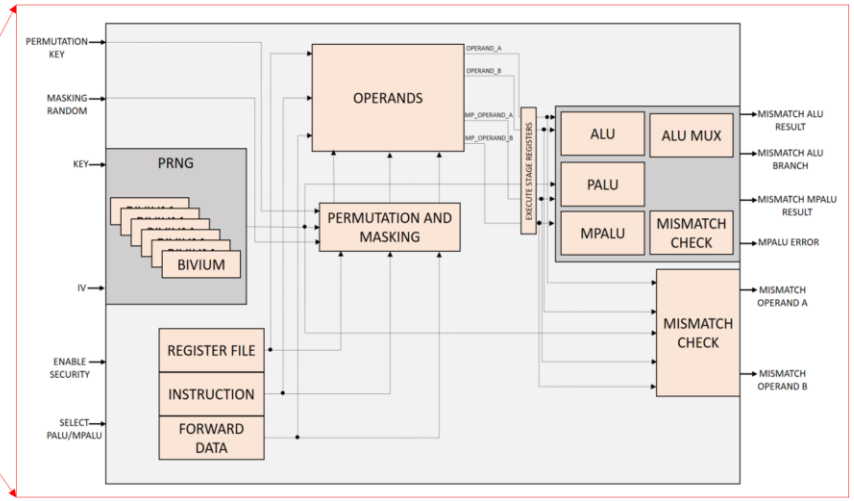


[1] Fritzmann, T., Van Beirendonck, M., Roy, D. B., Karl, P., Schamberger, T., Verbauwhede, I., & Sigl, G. (2022). Masked accelerators and instruction set extensions for post-quantum cryptography. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 414-460.

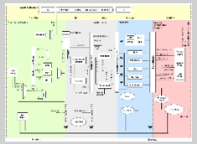
Microarchitectural Leakage of RISC-V Processors

CVA6 processor

Security modules



- CVA6 from OpenHWGroup
- Linux capabilities



RISC-V processor

Permuted ALU

- Support of all CVA6 extensions
- Protection of the issue and execute stage against faults injection

Masked permuted ALU

- A protection against faults injection and leakage

Security assesment

- To be carry out on the silicon technology at CEA

Secure Memories

Objective: Enable certification-ready SRAM data sanitization

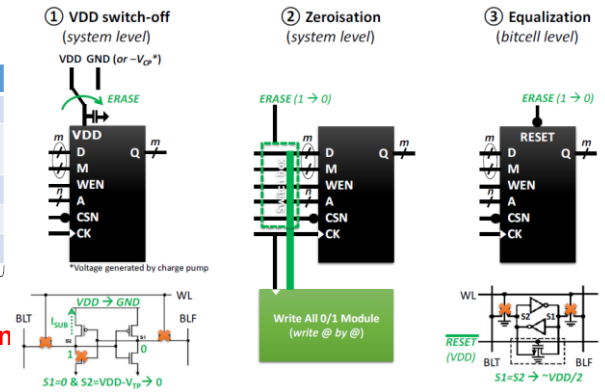
- ❑ Key criteria:
  - ✓ Constant-time erase operation
  - ✓ Atomic erase capability
  - ✓ Verifiable & auditable erase mechanism

FIPS Level 3 Validated 140-3 ✓ ISO/IEC 15408 ✓

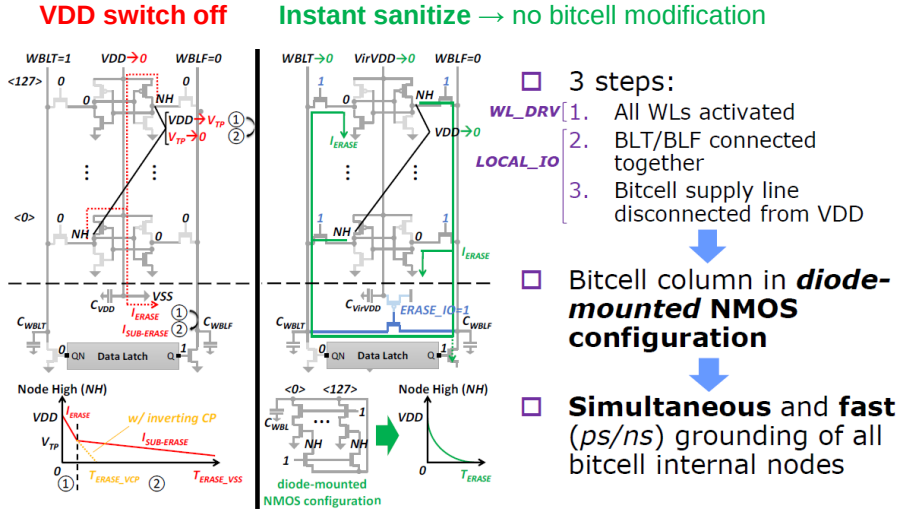
- ❑ Existing solutions:

	① VDD switch off	② Zeroisation	③ Equalization
Erasure time	🔴⬌🟡	🟡⬌🔴	🟢
Erase type	Metastable + Randomization	Zeroisation	Metastable + Randomization
Area overhead	🟢⬌🔴	🟡	🟡
Power	🔴	🟡	🟢
Dev. cost	🟢⬌🟡	🟢	🔴

~~key criteria~~ bitcell modification



- ❑ Innovation: *instant sanitization fully compatible with **all commercial SRAM designs***



- ❑ 3 steps:
  1. All WLs activated (WL_DRV)
  2. BLT/BLF connected together (LOCAL_IO)
  3. Bitcell supply line disconnected from VDD
- ❑ Bitcell column in ***diode-mounted* NMOS configuration**
- ❑ **Simultaneous** and **fast** (*ps/ns*) grounding of all bitcell internal nodes

Silicon results (nominal condition):

- ❑ Capacity*- & data-independent sanitization time:
  - ✓ **≤ 20 ns = 2 clock cycles** @100MHz
    - T_{CYCLE_1} → erase
    - T_{CYCLE_2} → set/reset

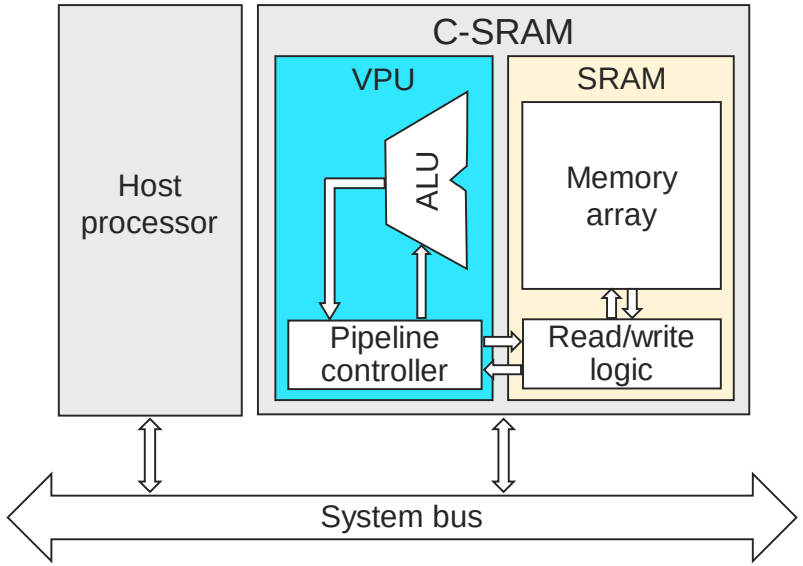
Next steps (security assessment):

- ❑ Temperature/voltage sensitivity (cold boot attack)
  - ✓ -40°C ↔ 125°C
  - ✓ minimum supply voltage?
- ❑ Information leakage (power analysis)
  - ✓ versus *address-by-address* overwriting

Near Memory Computing

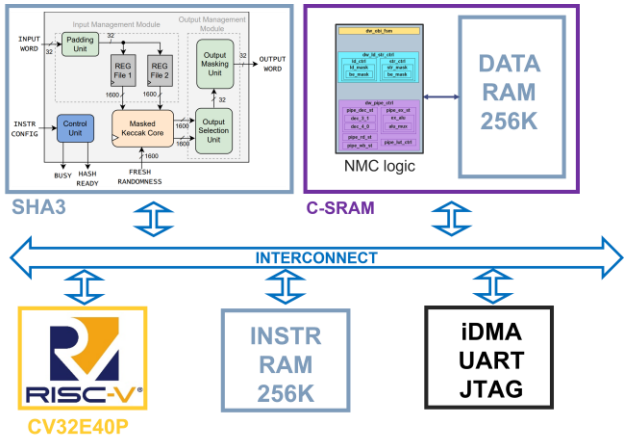
- **NMC** solution compatible with any existing SRAM memory macros (**off-the-shelf SRAM compilers**)
- Coupled with a **Vector Processing Unit (VPU)** executing NMC instructions issued from the CPU
- A **set of generic instructions** is supported by the Computational SRAM
- In SoC architectures **data RAM** can be advantageously **replaced by a C-SRAM** (w/o latency penalty)

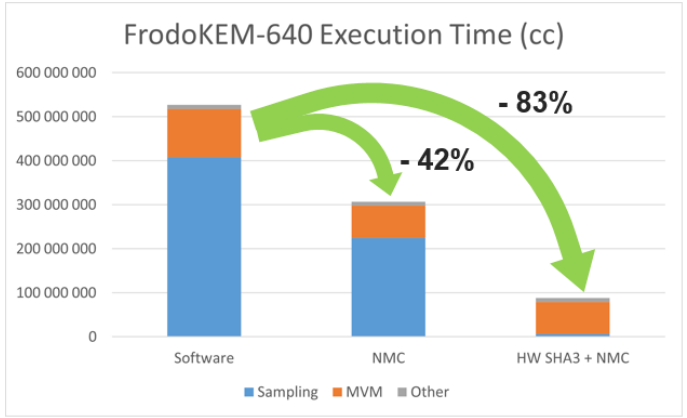
C-SRAM Architecture



PQC acceleration through NMC

- FrodoKEM is a lattice-based PQC scheme whose main bottlenecks are:
  - Pseudo-randomness sampling based on SHA-3 functions
  - Matrix-Vector Multiplication (MVM) with big sizes





	Area (kGE)	Overhead
Software	4582	
NMC	4664	**1.79%**
HW SHA-3 + NMC	4736	**3.35%**

Conclusions

- **Hardware is the root of trust for secure systems**

- **The continuous evolution of the security ecosystem requires the development of new technologies:**
  - Physical attacks
  - Quantum threat
  - Evolution of standards and certifications

- **The VASCO platform provides a framework for developing security-oriented test chips**

- **The VASCO#3 test chip was used to validate research activities on different subjects:**
  - TRNG modelling
  - PQC hardware implementations
  - Secure memories
  - Emerging architectural paradigms
  - Secure RISC-V microarchitectures
  - Advanced semiconductor technology

    - If you want a peek, come and visit our demo!

Thanks

S. Di Matteo[1, 2], R. Alidori[2], L. Benea[1], M. Carmona[1], M. El Majihi[1] , F. Lepin[2], F. Pebay-Peyroula[1], M. Pezzin[2], S. Pontié[1,3], M. Ramirez-Corrales[2], O. Savry[1], E. Valea[2], R. Wacquez[1, 3]

(1) Univ. Grenoble Alpes, CEA, Leti F-38000 Grenoble, France
(2) Univ. Grenoble Alpes, CEA, List F-38000 Grenoble, France
(3) CEA-Leti, Mines Saint-Étienne, Equipe Commune, F-13541 Gardanne, France