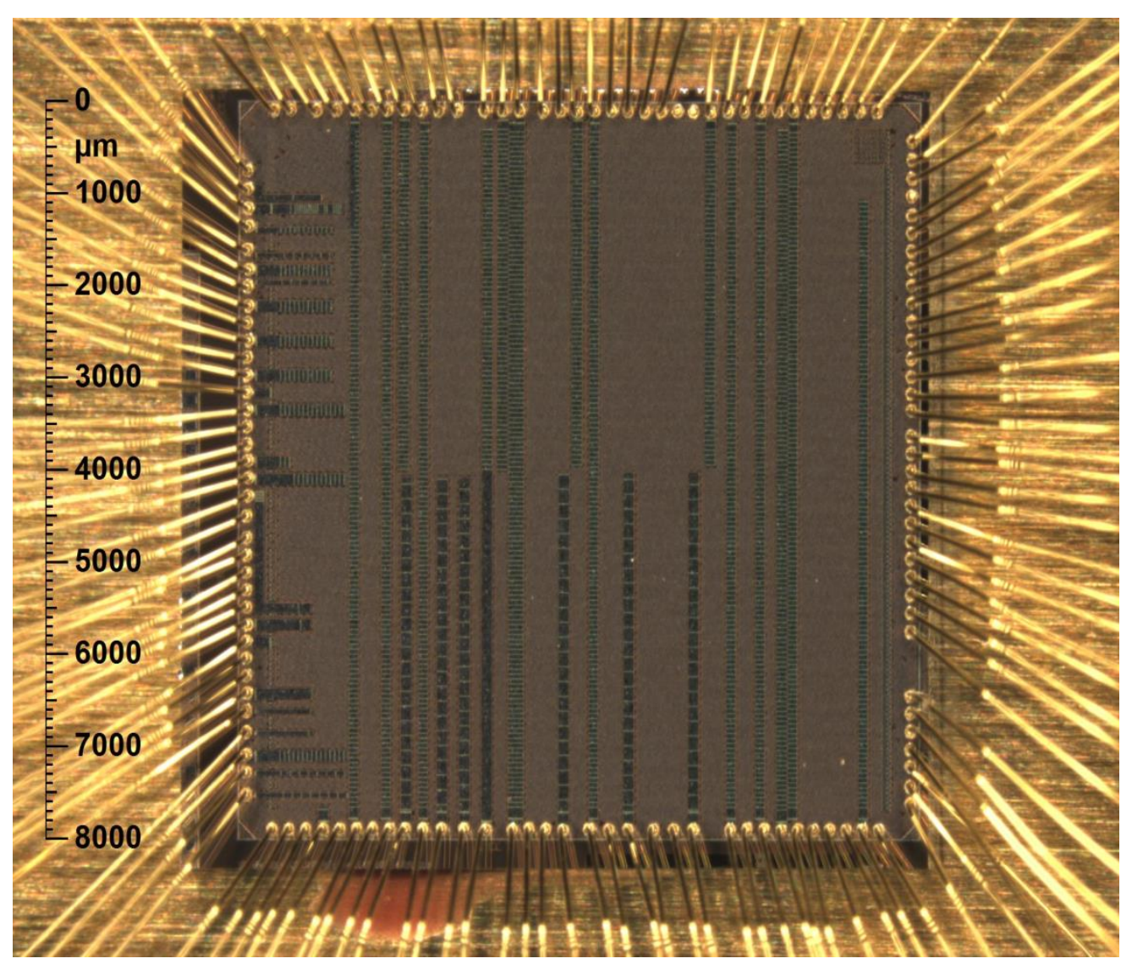
S. Di Matteo[1, 2], R. Alidori[2], L. Benea[1], M. Carmona[1], M. El Majihi[1] , F. Lepin[2], F. Pebay-Peyroula[1], M. Pezzin[2], S. Pontié[1,3], M. Ramirez-Corrales[2], O. Savry[1], E. Valea[2], R. Wacquez[1, 3]

(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



VASCO: ASIC TEST PLATFORM FOR CYBERSECURITY ON FD-SOI

A MODULAR R&D PLATFORM BUILT FOR PROTOTYPING SECURITY ON ASIC AND OPEN FOR PARTNERSHIP

- ✓ASIC is required for characterization and validation of innovation in hardware security in a real-life environment
- ✓A modular platform for design and test innovative security primitives with respect to today's challenges
- ✓Support the bulk to FD-SOI transition for embedded systems
- ✓Evaluate and characterize Intellectual Properties (IPs) in terms of performance and security on the FD-SOI technology
- ✓Opportunity to improve the maturity of different security IPs.
- ✓A platform open to collaborations with CEA partners: ANSSI, University of Pisa, University of Montpellier, and others to come.

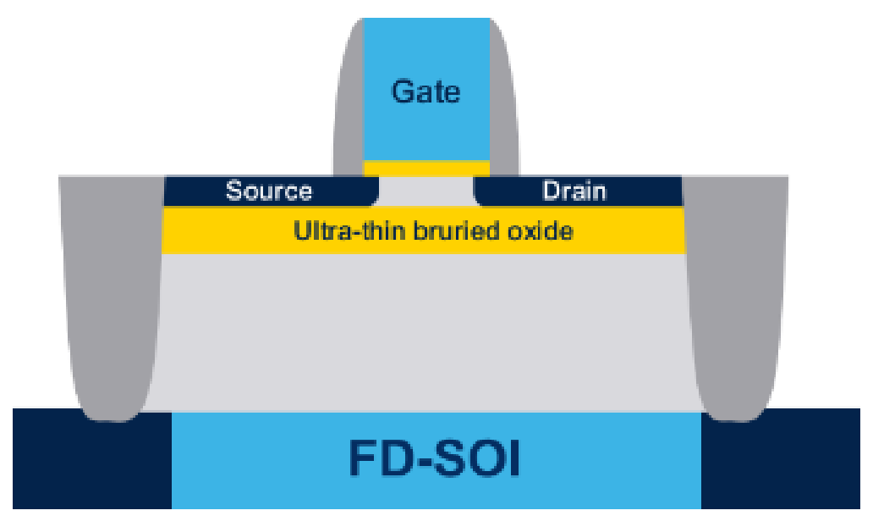
TECHNOLOGY

HW Components

At the core of the Root of Trust of many security products. Under constantly increasing pressure in terms of performance and security trade-off

Advanced attacks

Quantum-based attacks, AI-based attacks, micro-architectural attacks



Technological migration

FD-SOI is a key technology for low power scenarios. Cybersecurity applications can leverage the advantages of this technology

INTELLECTUAL PROPERTIES

Post-Quantum cryptography

Transition to quantum resistant cryptography

Entropy Sources

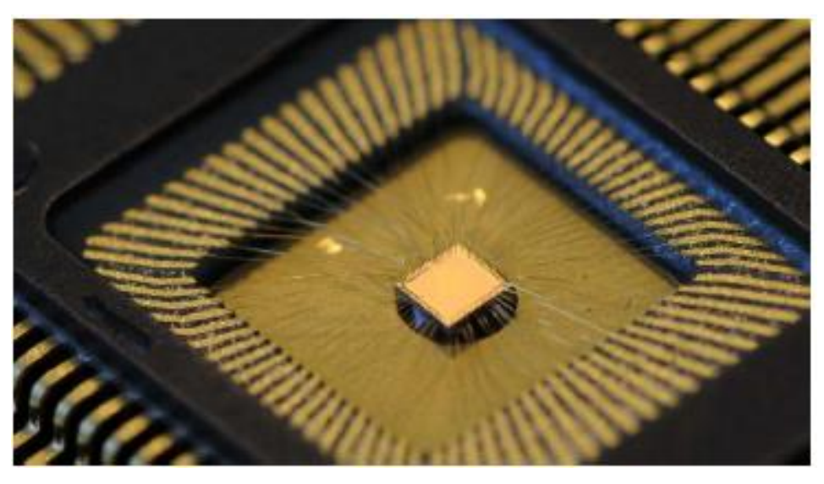
Provide the unpredictable character of primitives. Standards require more guarantees on the entropy sources

Security of RISC-V processors

Taking advantage of the open source ISA RISC-V to design intrinsically secure processors

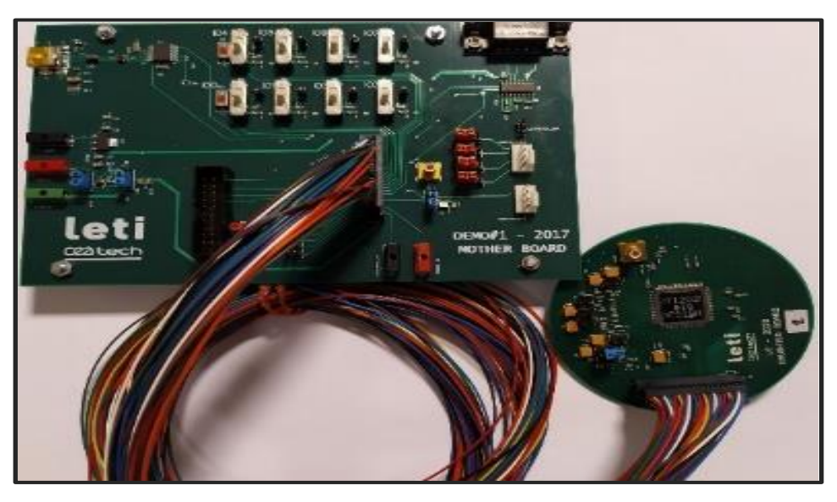
VASCO TIMELINE

2018



VASCO#0: Bulk 28nm

2020

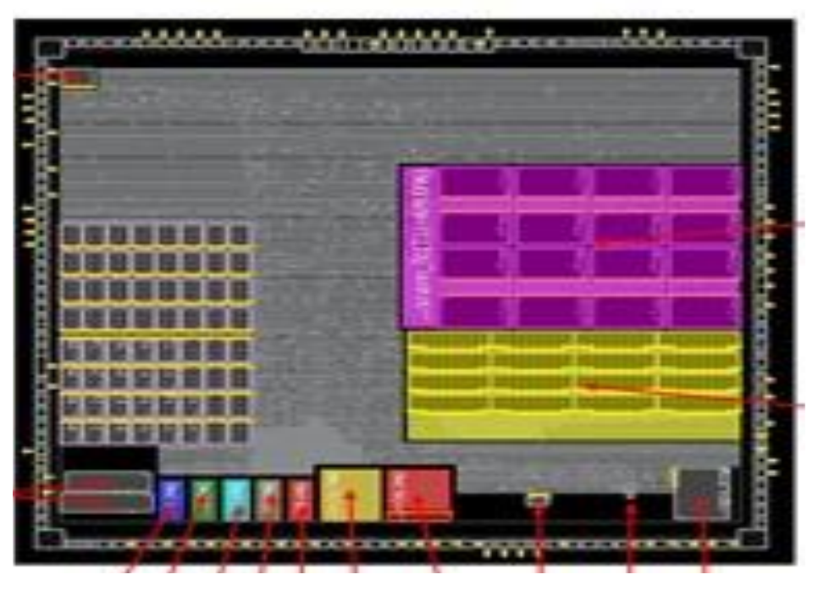


VASCO#1: 22nm FDX

2022

VASCO#2: 22nm FDX

2025

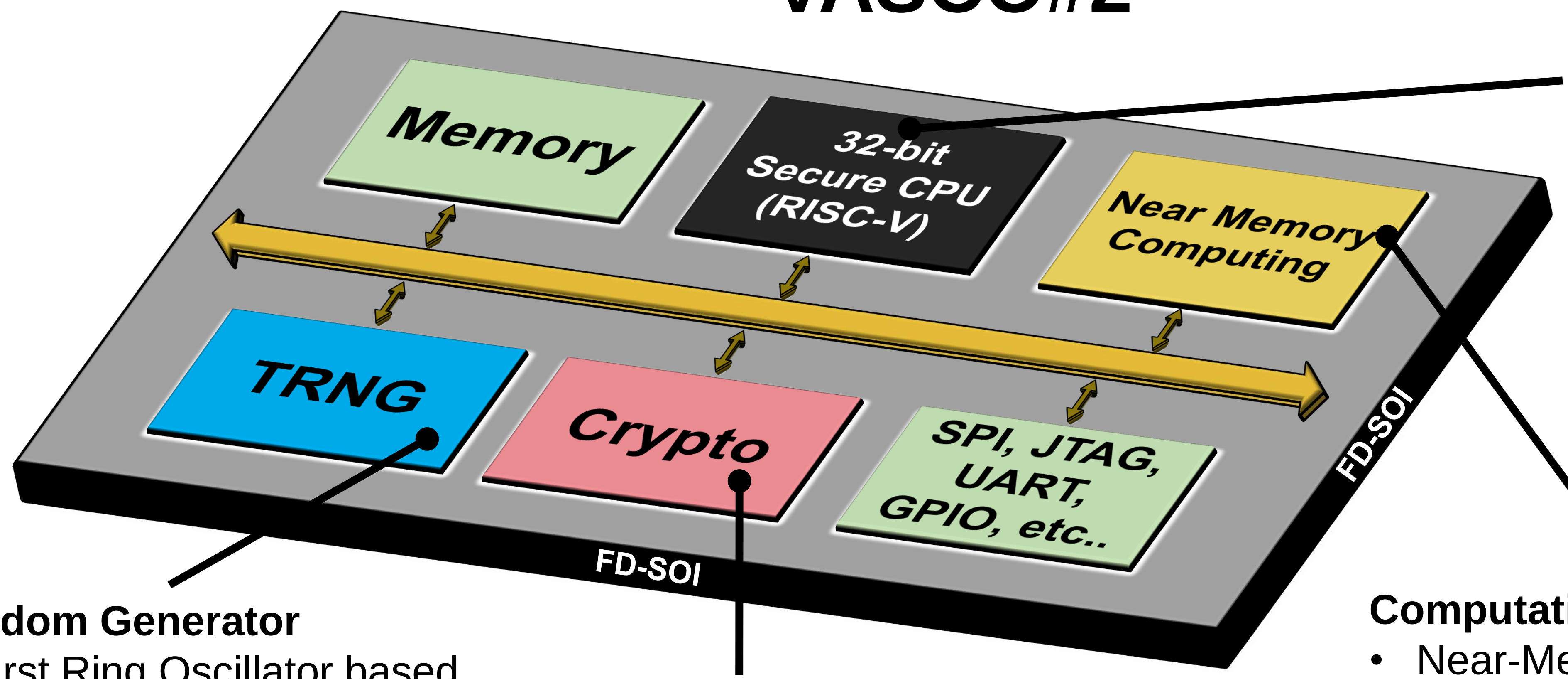


VASCO#3: 22nm FDX

2026

VASCO#3.1: 22nm FDX

VASCO#2



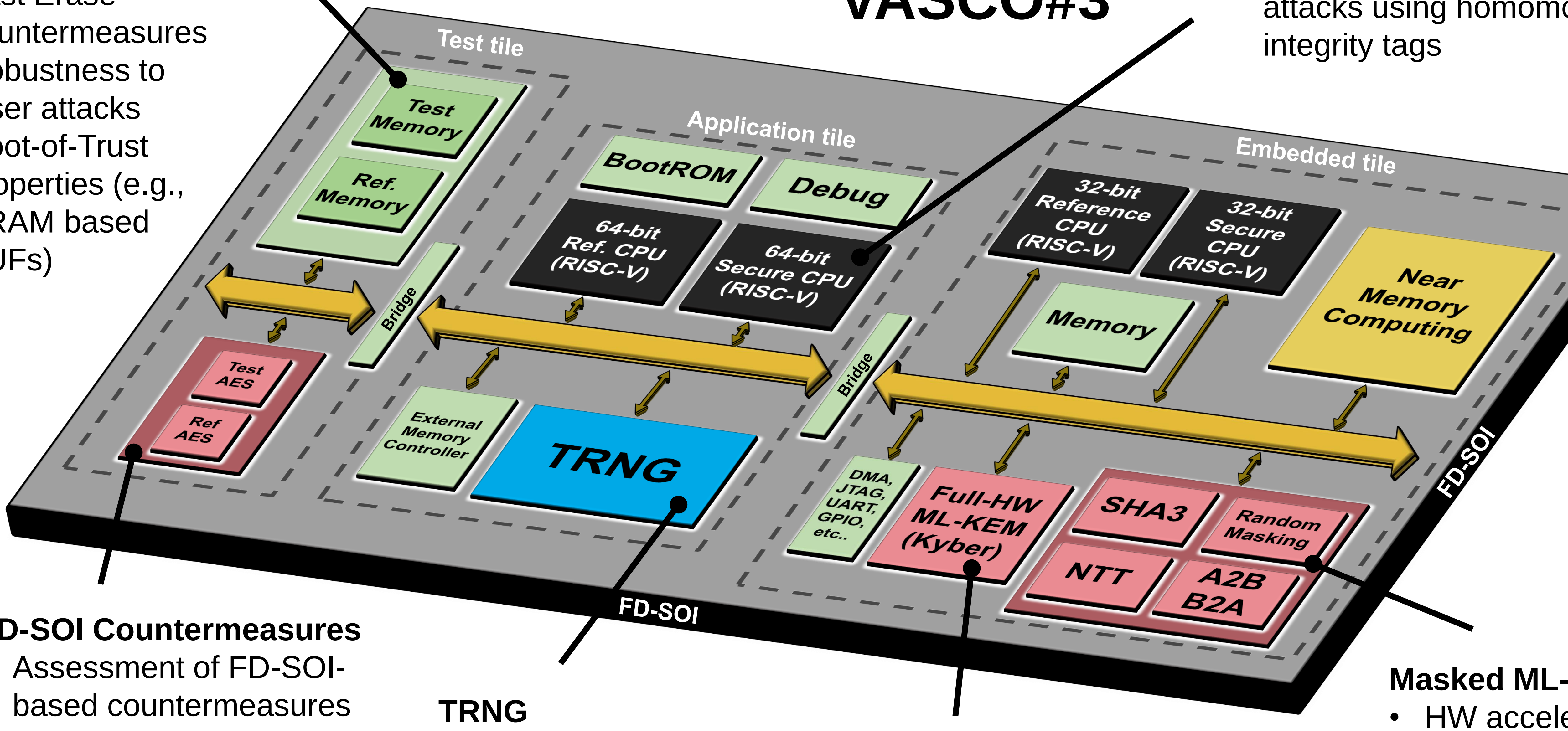
Secure 32-bit RISC-V
- Pipeline is hardened versus fault injection attacks: *Homomorphic integrity tags, dummy instructions, masking of the decoding stage*

Random Generator
- First Ring Oscillator based TRNG characterized on FD-SOI

Post-Quantum Cryptography
- Hybrid-pre-post-quantum cryptoprocessor
- Resistant to Side-Channel and Fault Injection attacks

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

VASCO#3



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)

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

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)

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