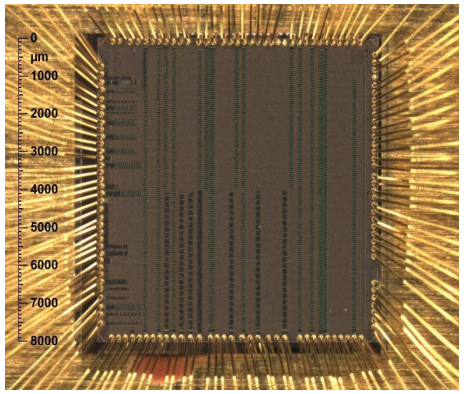
VASCO: ASIC Test Platform for CYBERSECURITY on FD-SOI

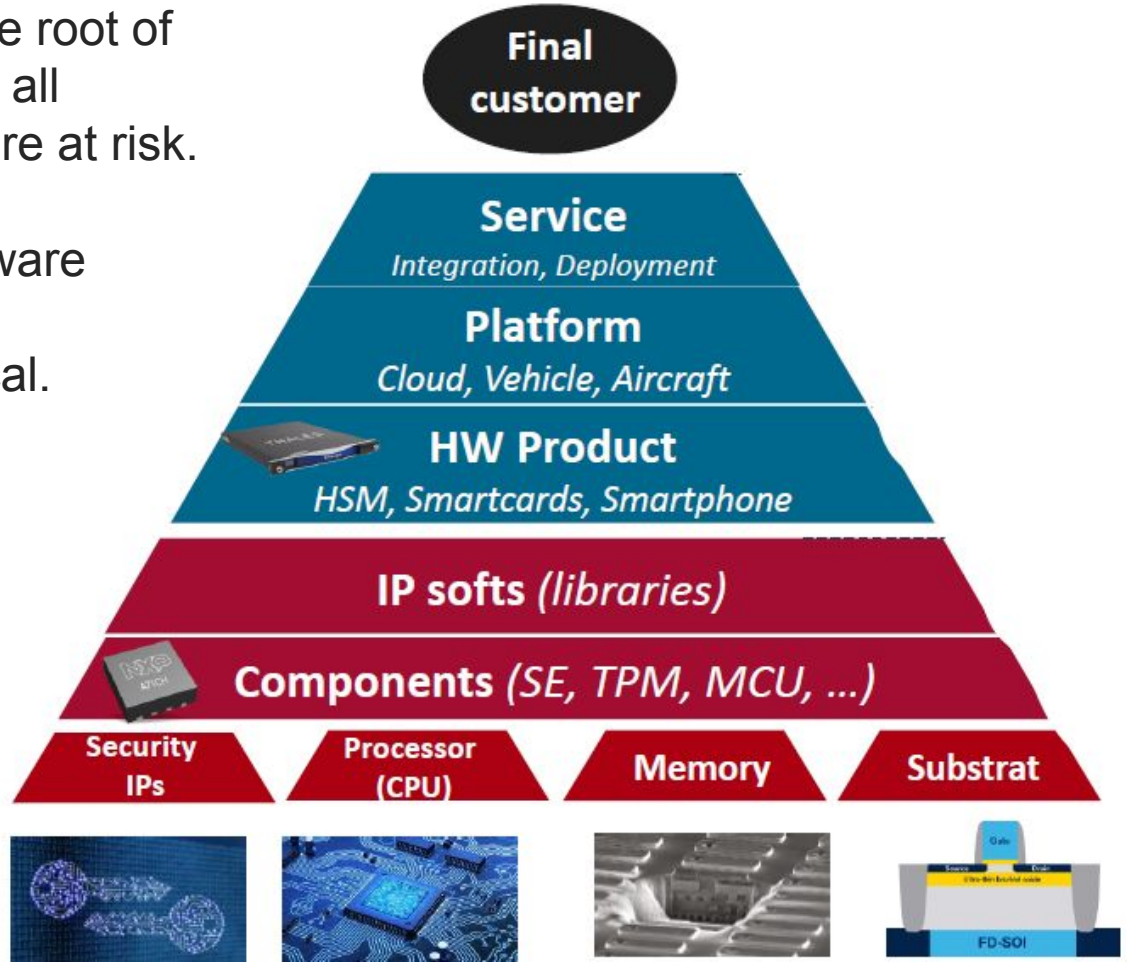
S. Di Matteo[1, 2], R. Alidori[2], L. Benea[1], M. Carmona[1], M. El Majihi[1] , F. Lepin[2], F. Pebay-Peyroula[1], M. Pezzin[2], S. Pontié[1,3], M. Ramirez-Corrales[2], O. Savry[1], E. Valea[2], R. Wacquez[1, 3]

(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



Secure HW: the basis of the Security Chain

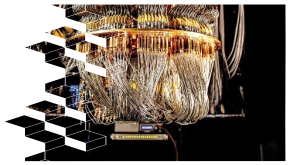
- **Foundation of Security**: Hardware is the root of trust for secure systems if compromised, all software and cryptographic protections are at risk.
- **Rising Threats**: Increasing attacks on hardware (side-channel attacks, trojans, supply chain vulnerabilities) make hardware security critical.
- **Essential for Critical Systems**: Industries like finance, healthcare, defense, and IoT rely on trusted hardware to protect sensitive data.
- **Secure Hardware Enables Trusted Computing**: Secure boot, authentication, and encryption all depend on trusted hardware components.



Challanges of Modern HW components

Growing Security Threats and advanced Attacks:

- **Quantum Computing**: Future quantum attacks could break today's encryption.
- **Side-Channel & Fault Injection Attacks**: Exploit power consumption, timing, EM emissions, and hardware faults to extract secrets. AI enhances side-channel analysis.



Evolution of Security Standard and Certifications:

- Regulations (e.g., **CRA**) evolve constantly, increasing compliance complexity.
- Specific Standards emitted by national agencies (e.g. NIST, ANSSI, BSI, etc.)
- New threats demand continuous updates to security frameworks.

NIST

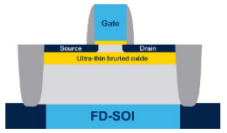
BSI

Common Criteria

Technological Advancement:

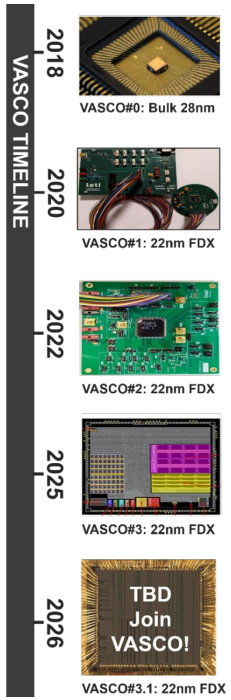
- **Post-Quantum Cryptography**: New algorithms to resist quantum attacks.
- **RISC-V & Open Hardware**: Brings flexibility but increases security risks.
- **FD-SOI Technology**: Can enhances power efficiency and resilience against fault attacks -> migration of Embedded systems.

RISC-V®

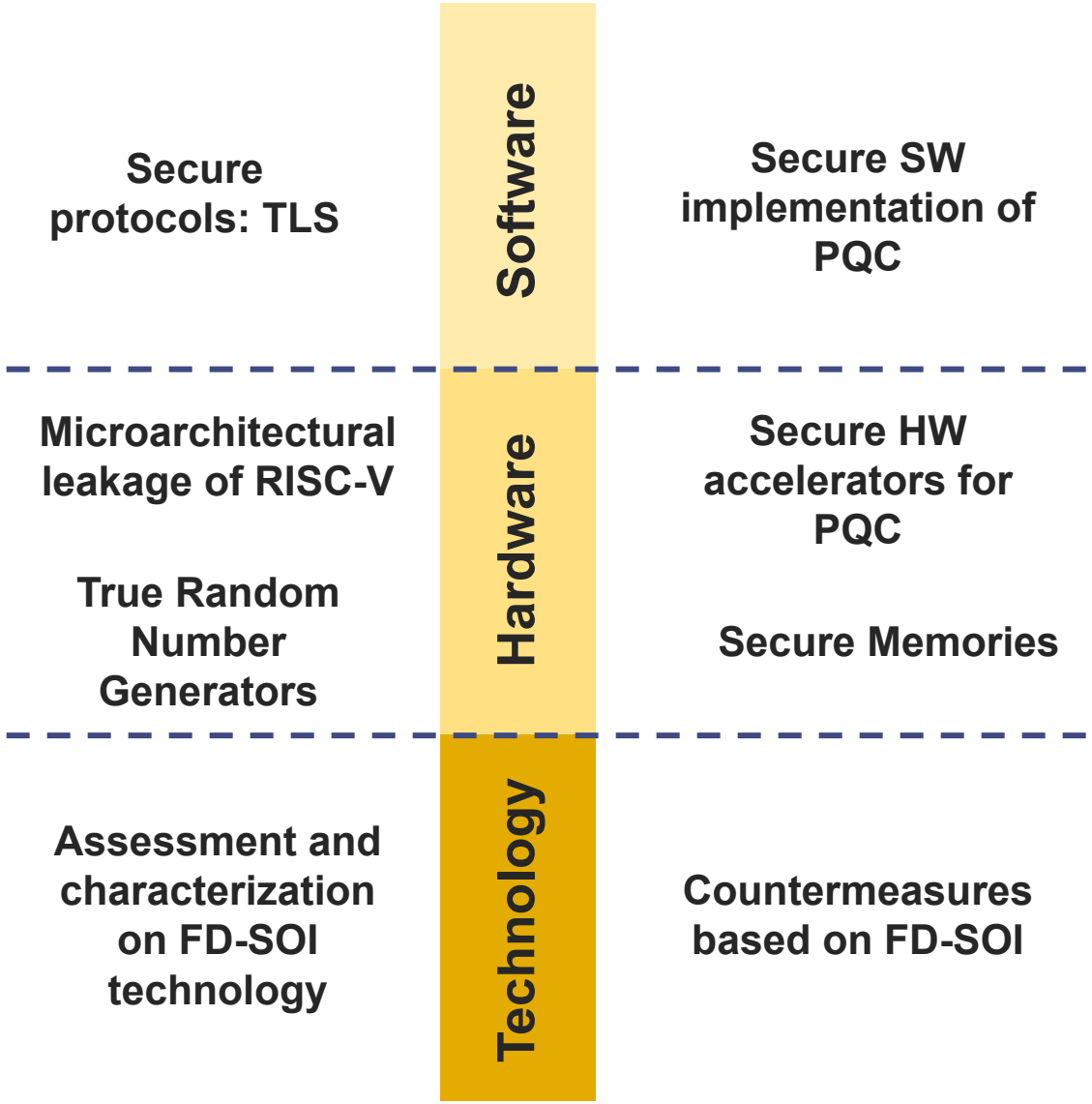


VASCO: an ASIC Platform for Cybersecurity

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

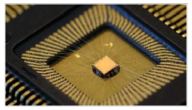


- Test HW and SW innovations
- Test the capabilities of FD-SOI for resilience against SCAs and FI attacks
- Anticipate the migration to FD-SOI for embedded systems
- Digital twin: use hardware to build models (e.g. TRNGs)
- Build security component at different abstraction levels
- Open to **parterships**



VASCO#2 Architecture

VASCO TIMELINE

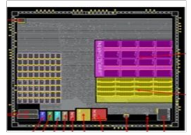
2018

VASCO#0: Bulk 28nm

2020

VASCO#1: 22nm FDX

2022

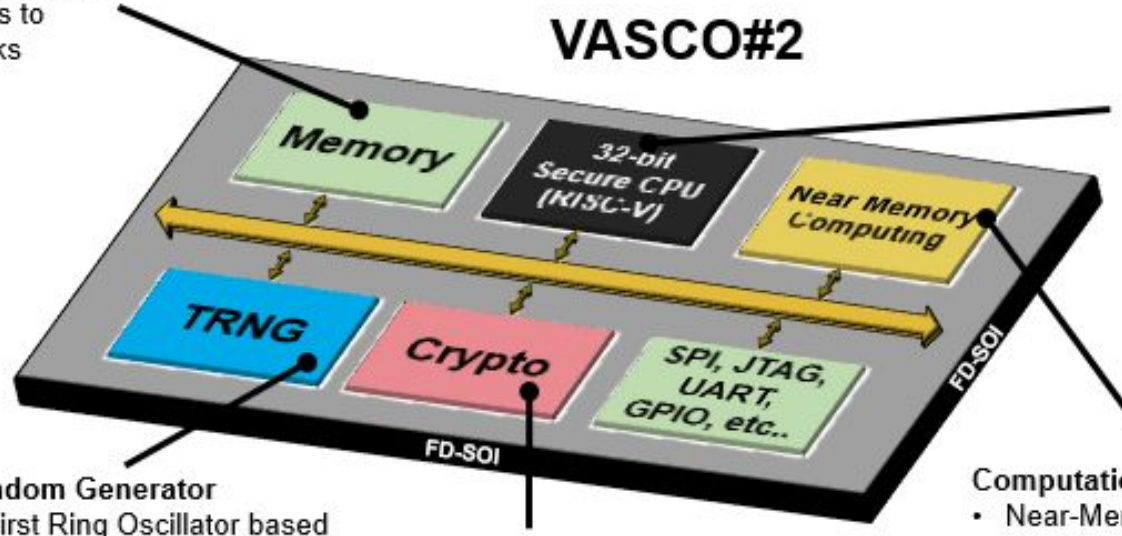
VASCO#2: 22nm FDX

2025

VASCO#3: 22nm FDX

2026


VASCO#3.1: 22nm FDX

Test Memory
- Test platform for assessing security of FD-SOI SRAMs
- Robustness to laser attacks



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

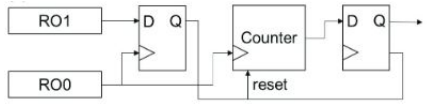
Post-Quantum Cryptography
- Hybrid-pre-post-quantum cryptoprocessor
- Resistant to Side-Channel and Fault Injection attacks

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

VASCO#2 Results

- **Fault injection on CV32E40P**

- **Noise Characterization of ROs**



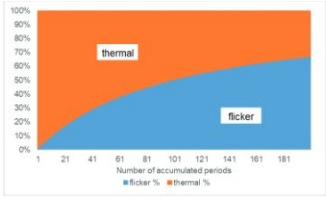
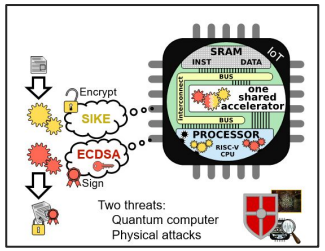
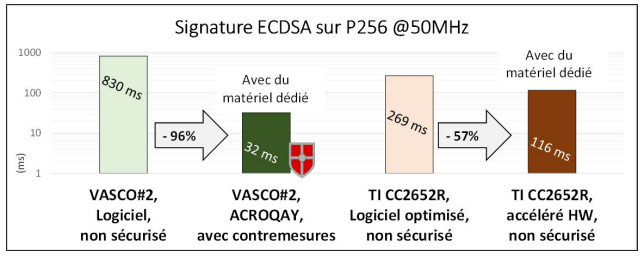


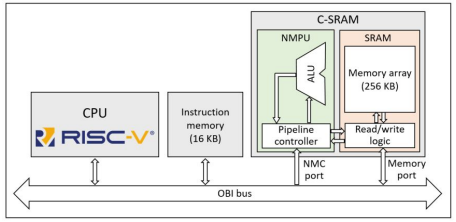
Fig. 13. Noise composition for $V_{BS} = 0.2V$

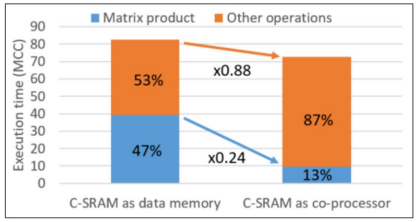
- **Fault Injection on Accelerator for crypto**





- **Near Memory Computing for crypto**





[1] Benea, L., Carmona, M., Pebay-Peyroula, F., & Wacquez, R. (2022, August). On the Characterization of Jitter in Ring Oscillators using Allan variance for True Random Number Generator Applications. In 2022 25th **Euromicro Conference on Digital System Design (DSD)** (pp. 534-538). IEEE.

[2] Benea, L., Carmona, M., Fischer, V., Pebay-Peyroula, F., & Wacquez, R. Impact of the Flicker Noise on the Ring Oscillator-based TRNGs. **IACR Transactions on Cryptographic Hardware and Embedded Systems**, 2024(1).

[3] Leplus, G., Savry, O., & Bossuet, L. (2022, June). Insertion of random delay with context-aware dummy instructions generator in a RISC-V processor. In *2022* ***IEEE International Symposium on Hardware Oriented Security and Trust (HOST)***

[4] Leplus, G., Savry, O., & Bossuet, L. (2022, August). SecDec: Secure Decode Stage thanks to masking of instructions with the generated signals. In 2022 25th **Euromicro Conference on Digital System Design (DSD)**

[5] M. Ramirez Corrales E. Valea, JP. Noël, Improving Post-Quantum Cryptography coupling Near-Memory Computing and RISC-V Cores. **RISC V Summit 2023**

VASCO#3 Architecture

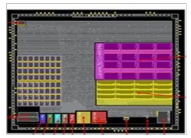
VASCO TIMELINE

2018 — VASCO#0: Bulk 28nm

2020 — VASCO#1: 22nm FDX

2022 — VASCO#2: 22nm FDX

2025 — VASCO#3: 22nm FDX

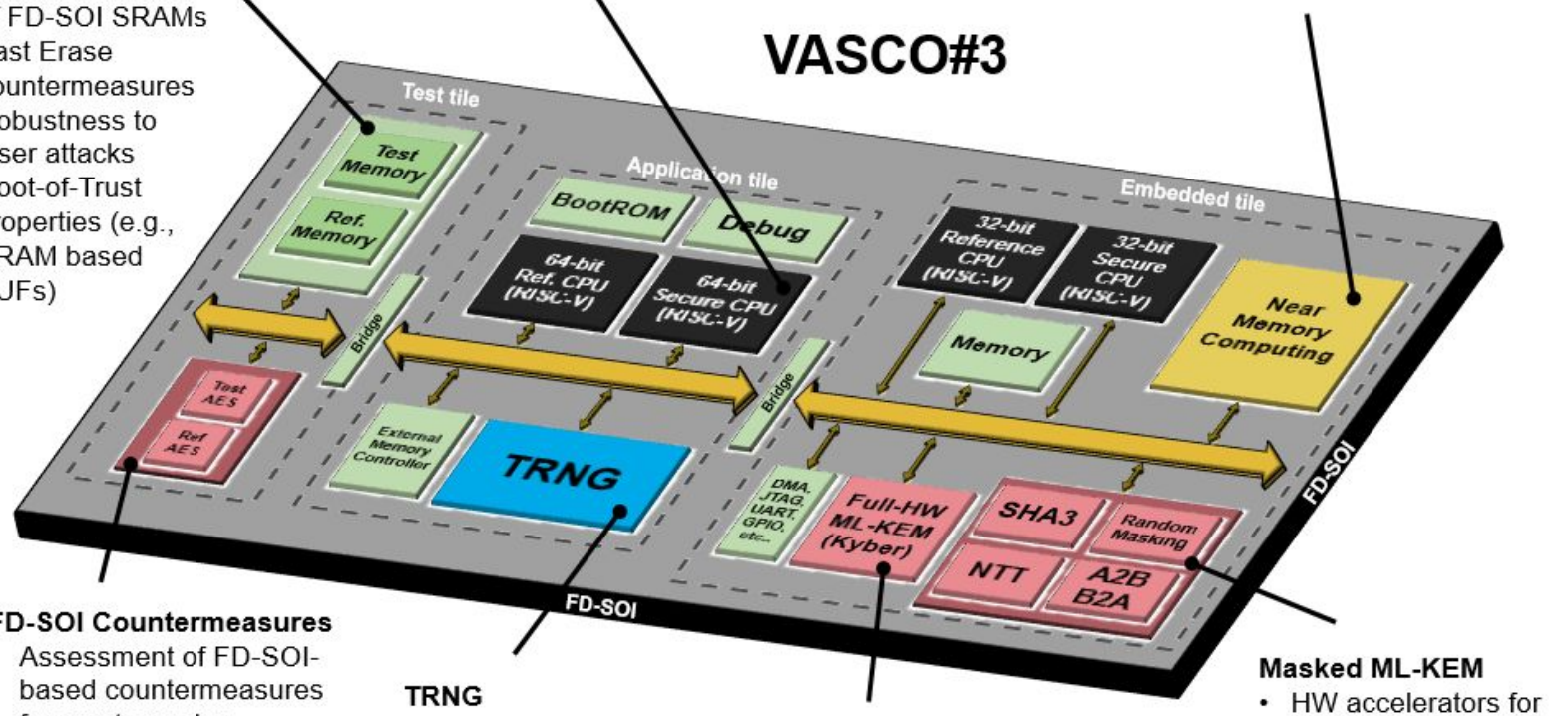


2026 — VASCO#3.1: 22nm FDX

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

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

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)



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

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