Exploring Open Hardware Solutions for Ensuring the Security of RISC-V Processors

Pablo Navarro Torrero

navarro@imse-cnm.csic.es

FSiC 2023

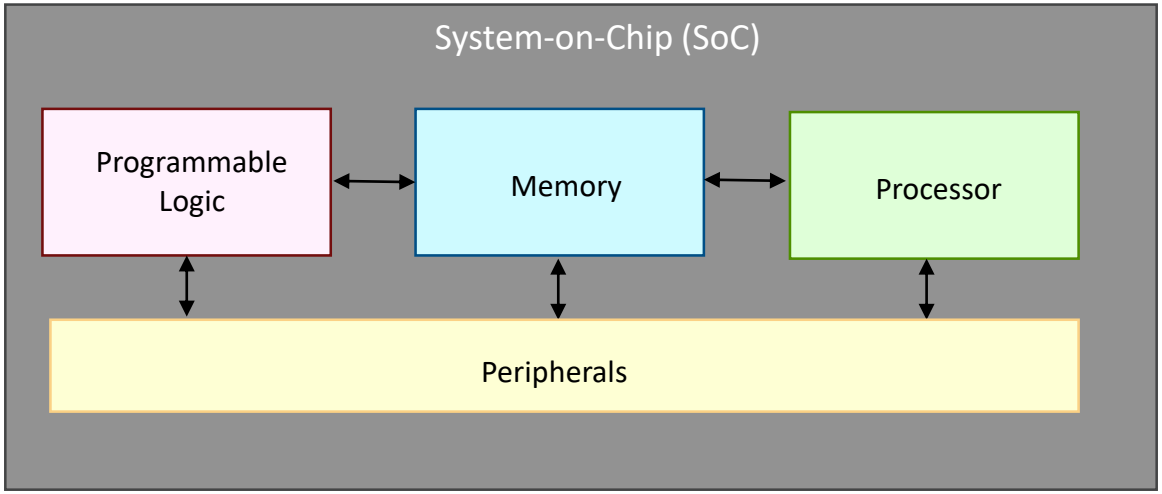
July 11, 2023

Outline

1. Introduction to embedded systems on System-on-Chips (SoCs)
2. Secure features for SoCs
3. Ad-hoc HW Root-of-Trust (RoT)
4. Future roadmap to foster European trusted chips
5. Open source hardware to build ad-hoc RoTs
6. Concluding remarks

System-on-Chip (SoC)

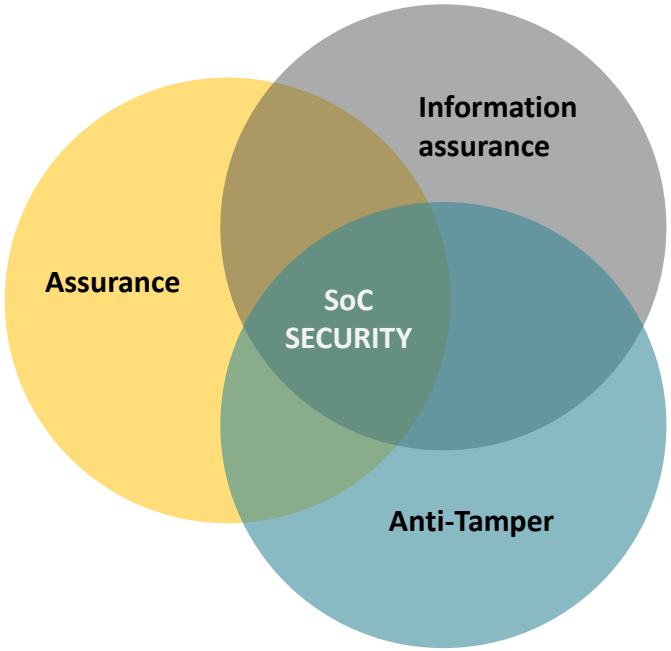
- Integrated circuit with all components of a computer
- Essential components of a SoC to implement embedded systems
- Hardware components: processor, programmable logic, memory, and peripherals into complete SoC designs



- Is this embedded system immune to attacks?

SoC security

1. **Assurance**: software, firmware, and IPs must be "Trojan-free". Also supply chain security must be trusted
2. **Information assurance**: the device is handling or processing data that should be protected, e.g. with cryptography and fault tolerant designs
3. **Anti-Tamper**: techniques to avoid cloning, reverse engineering or other types of attacks that can extract the IP



Security Throughout the SoC Lifecycle

- Is this system completely immune to attacks?

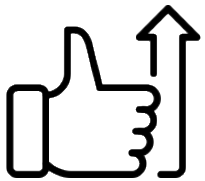
https://www.xilinx.com/products/technology/design-security.html

Analysis of SoC security

- Layered SoC architecture:

Embedded processor security

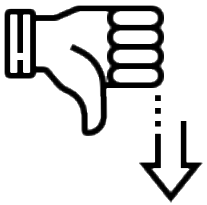
- Commercial solutions: Xilinx (ARM Cortex), Intel (Nios II)



Variety

Design tools

Upgrade facilities

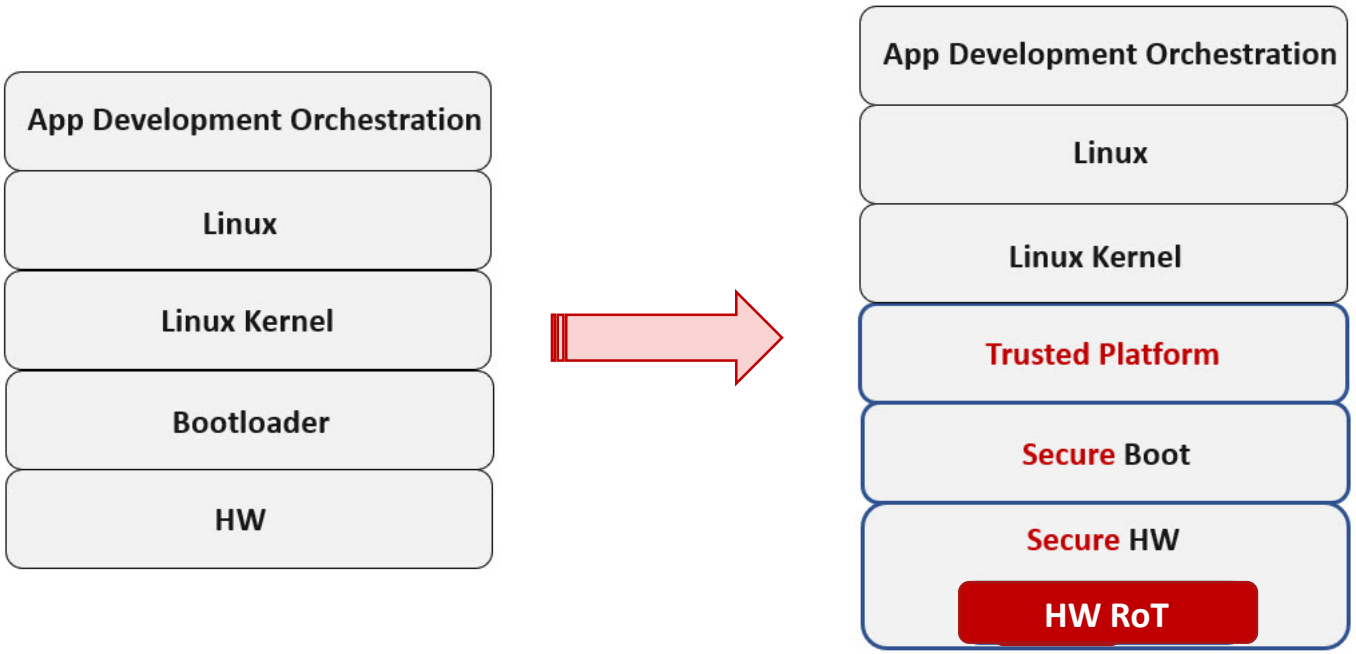


Lack of flexibility

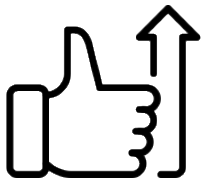
Security features

Secure features for SoC

- **Secure** layered SoC architecture:

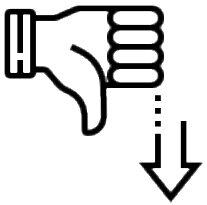


- Secure commercial solutions: high-end SoC families (Xilinx, Intel, Microsemi)



Secure initialization

Crypto keys in NVM



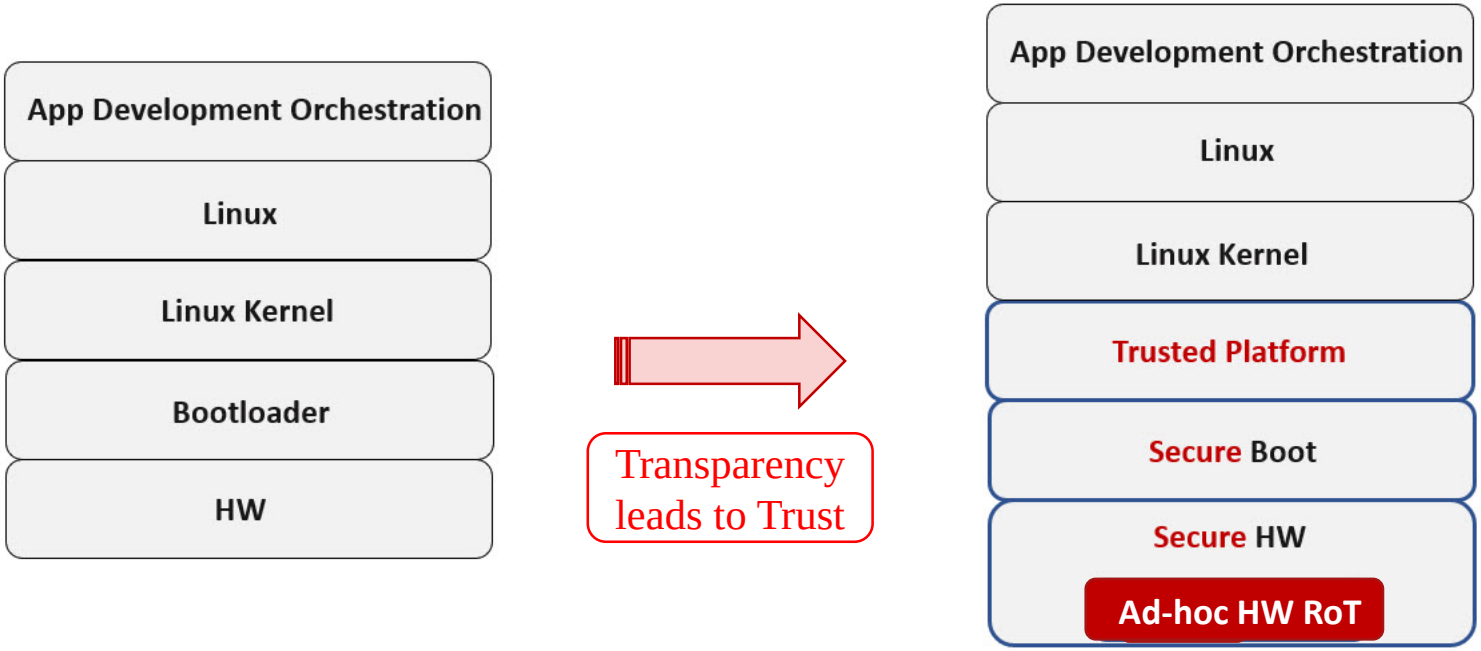
High cost

Technological dependency

Lack of flexibility

Dependency on 3rd vendors

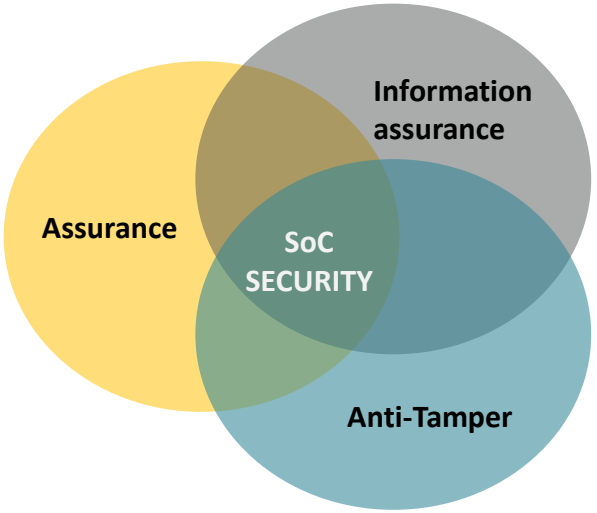
Our approach

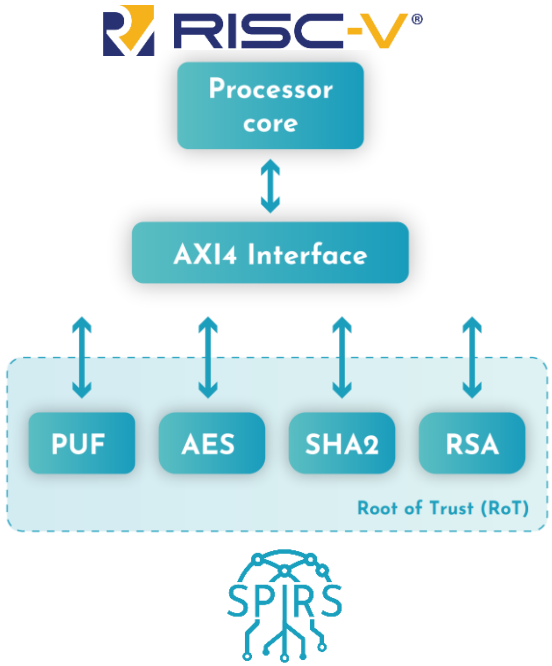


- **Building ad-hoc HW RoT**
  - ✓ Modular ➔ Flexibility
  - ✓ Technological independency ➔ ASIC and FPGA
  - ✓ Evolves over time ➔ Safety and Reliability
  - ✓ Open distribution of IP modules ➔ Trust

Ad-hoc HW RoT: crypto accelerators

- **Authenticity ➔ Anti-Tamper**
  - ✓ PUF (Physical Unclonable Function)
  - ✓ Unique identifier and random keys
  - ✓ Full hardware implementations (NIST validation)
- **Symmetric ciphers ➔ Information Assurance**
  - ✓ AES, 3DES, ASCON
  - ✓ Confidentiality: encryption
  - ✓ Full hardware implementations (NIST validation)
- **Hashing ➔ Information Assurance**
  - ✓ SHA2
  - ✓ Integrity
  - ✓ Full hardware implementations (NIST validation)
- **Digital signatures ➔ Information Assurance**
  - ✓ RSA
  - ✓ Hardware accelerator (NIST validation)

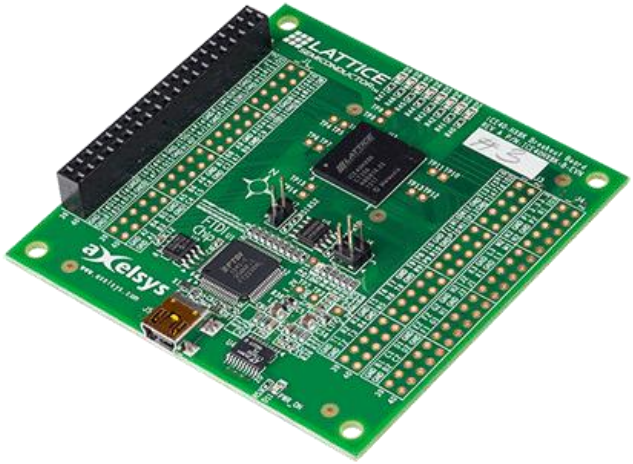




The SPIRS Project has received funding from the European Union's 2020 research and innnovation programme under the Grant Agreement Nº952622

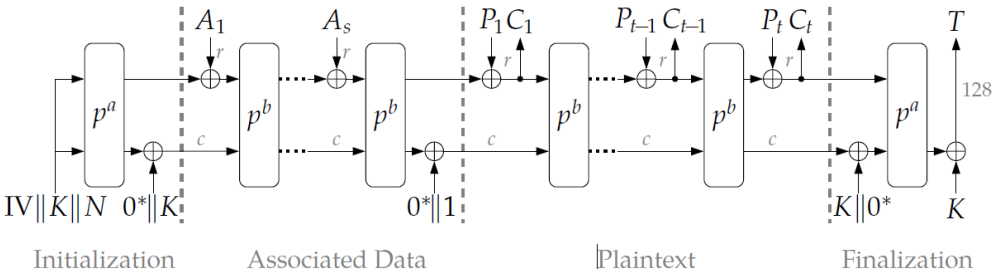
Ad-hoc HW RoT: symmetric cipher example

- Development board



Feature	*iCE40-HX8K*
Manufacturer	Lattice Semiconductor
Technology	40nm
Logic Cell	7,680
LUT	7,680 (4-input)
FF	7,680
BRAM	32
RAM	128Kb
DSP	–
PLL	2
Package	256-ball caBGA

- LWC ASCON interfaced with UART: resource utilisation

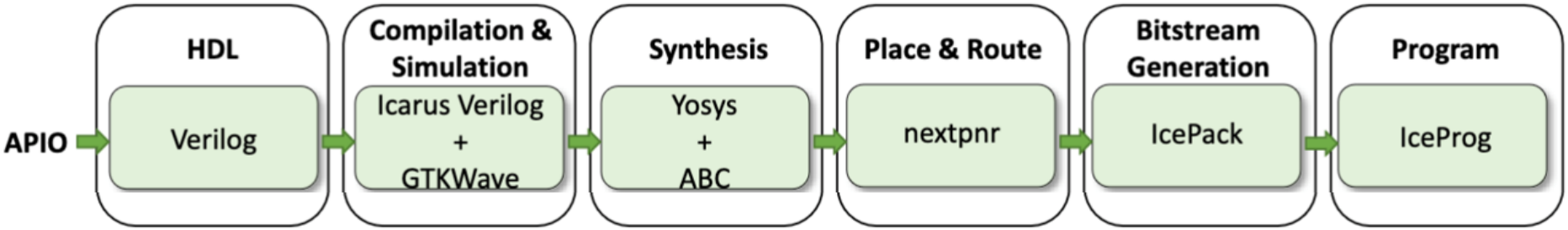



```
Info: Device utilisation:
Info:            ICESTORM_LC:  3566/ 7680    46%
Info:           ICESTORM_RAM:     8/   32    25%
Info:                  SB_IO:     4/  256     1%
Info:                  SB_GB:     7/    8    87%
Info:           ICESTORM_PLL:     0/    2     0%
Info:            SB_WARMBOOT:     0/    1     0%
```

https://ascon.iaik.tugraz.at/specification.html

GitLab Repository: https://gitlab.com/hwsec

Ad-hoc HW RoT: design flow

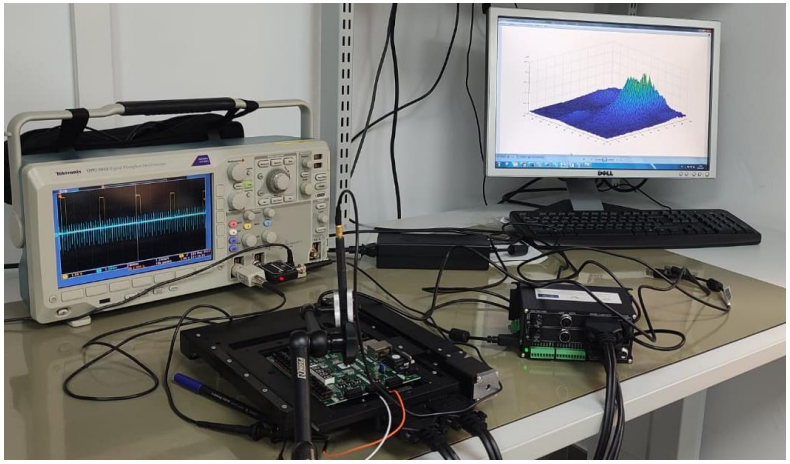


APIO

https://github.com/FPGAwars/apio

RoT protection against attacks

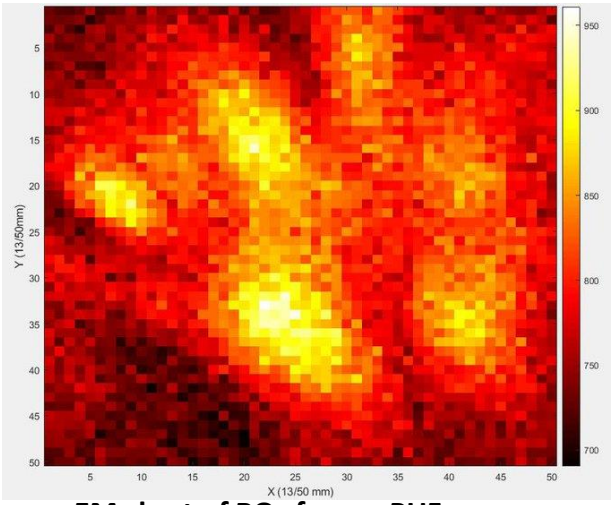
- Security evaluation: side-channel and fault-injection attacks



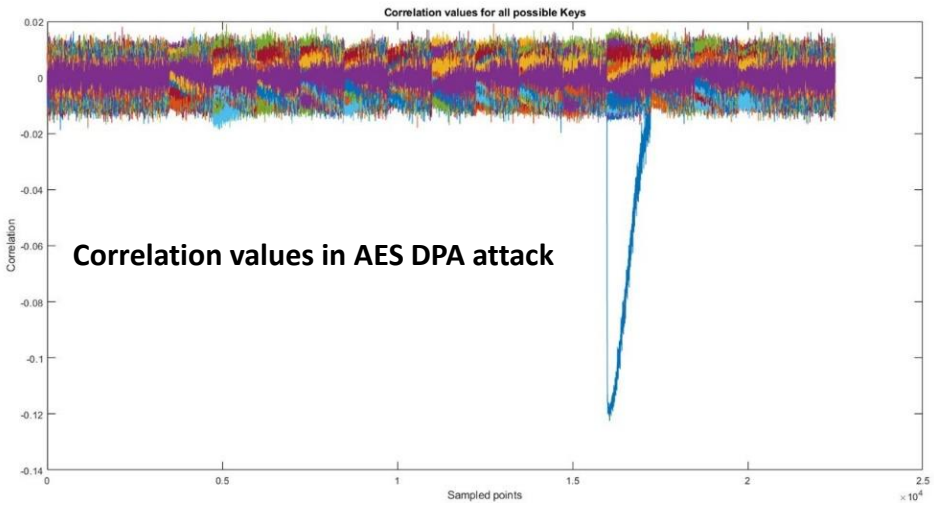
EM emanation experimental set-up

- ✓ EM attacks
- ✓ Power attacks
- ✓ T-test evaluation
- ✓ Fault-injection attacks (clock signal, control signal, EM injection)

- **Design of countermeasures** to mitigate the detected leakage



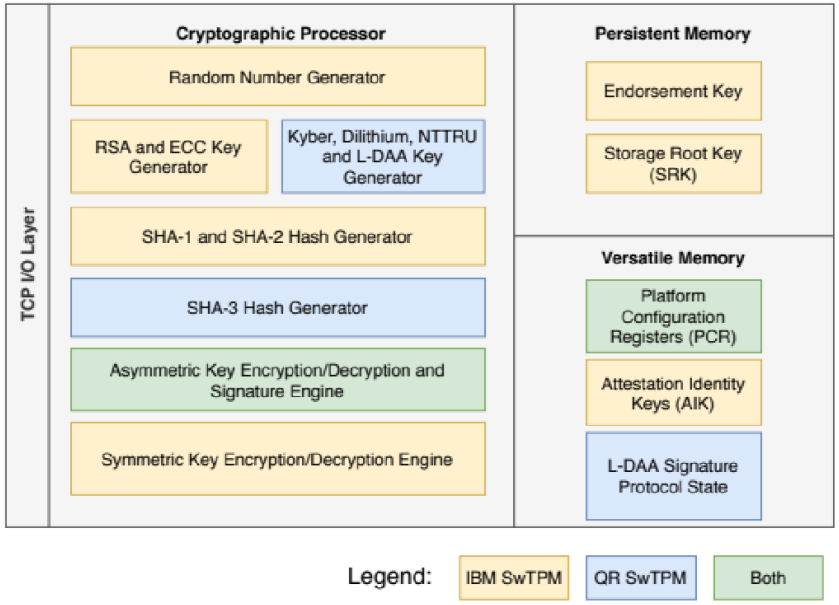
EM chart of ROs from a PUF



HW RoT in the quantum era

- **Future paradigm → Quantum computers**
- **Shor's algorithm** (current asymmetric cryptography)
  - ✓ Factoring a large biprime number (RSA)
  - ✓ Discrete Logarithm Problem (Diffie-Hellman, DSA, ECC)
- **PQC →** Post-Quantum Cryptography (KEM, digital signature)
- **Future RoT →** SHA-3, hardware accelerators for PQC

FutureTPM



Other open RoT initiatives

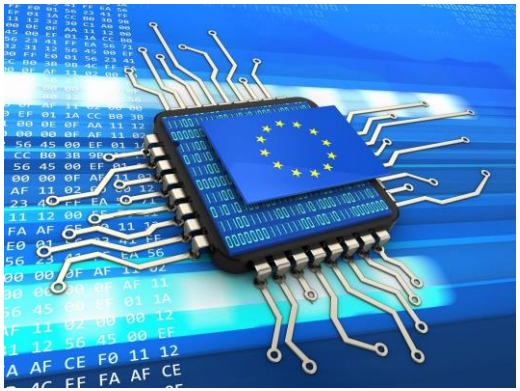
- **OpenTitan: Open source silicon root of trust (RoT)**
  - ✓ OpenTitan is an open source project
  - ✓ **Goal**: build a transparent, high-quality reference design and integration guidelines for silicon root of trust (RoT) chips
  - ✓ **Collaborative work** with leading not-for-profit, academic, and commercial organizations committed to its development and expansion
  - ✓ **Security through transparency** since community can audit, evaluate, and improve the security properties of the design
  - ✓ Main **components**: key manager, entropy source, AES, SHA-2, HMAC

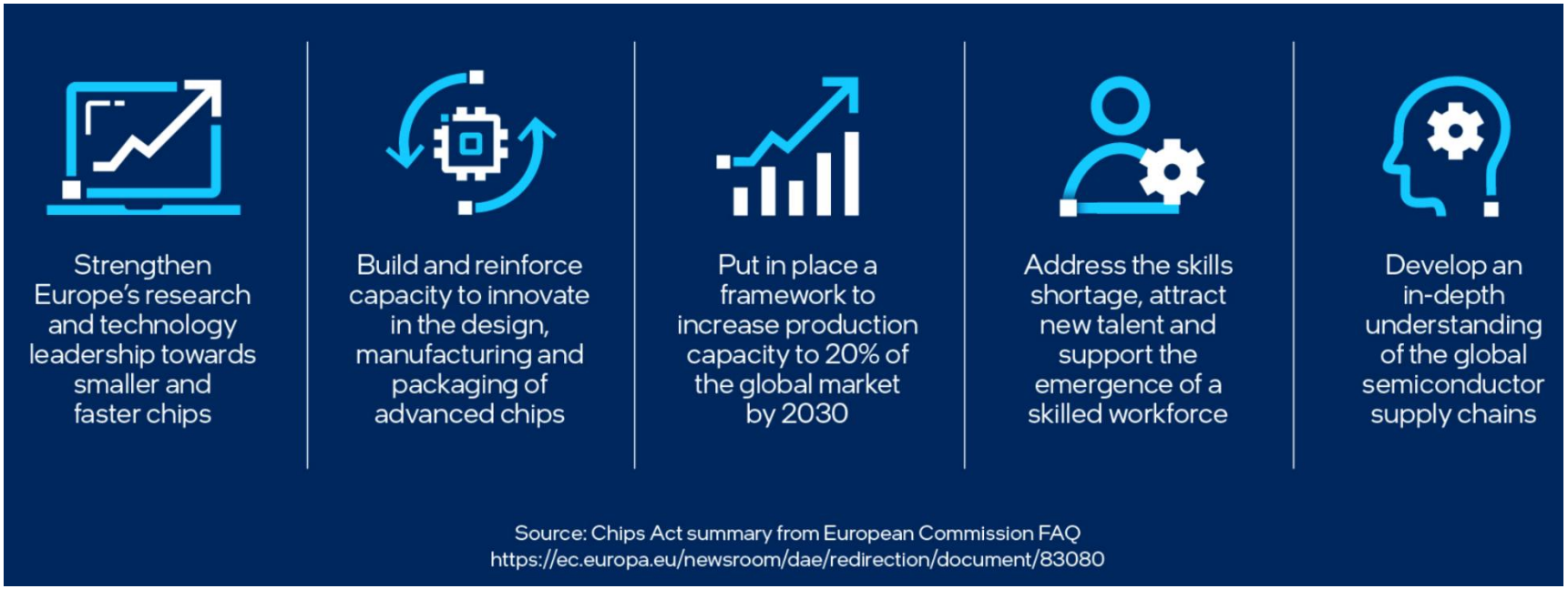
opentitan

https://opentitan.org/

Secure future digitalization in Europe

- **European Chip Act**
  - ✓ EU strengthens its semiconductors ecosystem
  - ✓ Increase resilience
  - ✓ Ensure supply and reduce external dependencies





Secure future digitalization in Europe

- **European Chip Act**

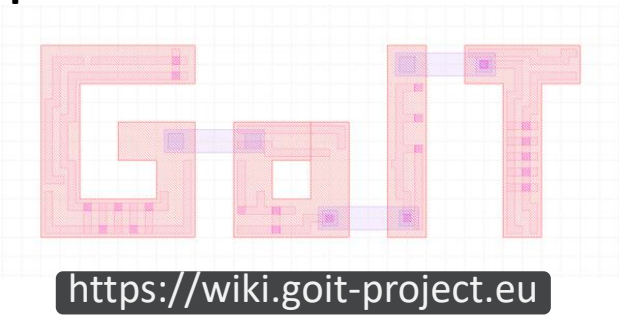
  1. **Pillar 1**: setting up the Chips for Europe Initiative to support technology
  2. **Pillar 2**: creating a framework to ensure security of supply by attracting increased investment and production capacity (semiconductor manufacturing , packaging, advanced testing, assembly)
  3. **Pillar 3**: establishing a mechanism for coordinating and monitoring (supply, demand, shortages, crisis phases)

- **Trusted chips ➔ Certification Committee**

  - ✓ Evaluate risks associated with the chips value chain
  - ✓ Trusted electronics
  - ✓ Standards and security certification in creating trust in the security of microchips
  - ✓ Joint standardization roadmap to inform future standards development to build trusted chips

Open-source hardware

- **Open-source hardware: a step towards Europe's digital independence**



https://wiki.goit-project.eu

✓ EU Coordination and Support Action (CSA)

✓ **Open Source Hardware for ultra-low-power, secure processors**

✓ Goals:

1. Feedback the **policymakers** with technical reports and roadmaps
2. Know-how for open-source chip design across **European universities**
3. Organization the **Free Silicon Conference**
4. Develop a GPL-compatible forever-open (copyleft) **licence** for silicon chips
5. Include the available **open-source PDK** in existing open-source design flows
6. Create a **repository of open-source EDA tools and hardware blocks**
7. Package **open-source tools** into mainstream GNU/Linux distributions
8. **Disseminate** the existing open-source tools and libraries
9. **Promote** the concept of open-source silicon chips
10. Contribute to **standardization / certification** activities for open-source silicon chips

The GoIT Project has received funding from the European Union's Horizon Europe programme under the Grant Agreement Nº 101070660

Open-source hardware

- **Our role in GoIT project**

Prospecting open initiatives in hardware security

- Review of open available RTL descriptions of cryptographic algorithms
- Review of available repositories for hardware benchmarking

Fostering open hardware to build ad-hoc RoT

- Raise awareness of the scientific community
- Standardize design requirements
- Integration of open hardware RoT on RISC-V processors
- Monitor security enhancements in RISC-V-processors

Promoting open source hardware for security in next generations

- Provide open educational resources
- Participation in specialized teaching conferences
- International contest for students

The GoIT Project has received funding from the European Union's Horizon Europe programme under the Grant Agreement Nº 101070660

Concluding remarks

- Security of **embedded systems** → secure digital world
- **Open Source Hardware**:
  1. Creation of repositories with HDL descriptions and IPs for open HW RoTs
  2. Ensure compatibility with open design flows and RISC-V processors
- **Advantages**:
  - ✓ Improve their **performance** by fostering collaborative work
  - ✓ Increase their **resilience** with the detection of vulnerabilities and the development mechanisms to prevent them
  - ✓ Increase **reusability** of IP modules RoT
  - ✓ Encourage progress towards EU **technological independence**

Exploring Open Hardware Solutions for Ensuring the Security of RISC-V Processors

Pablo Navarro Torrero

navarro@imse-cnm.csic.es

FSiC 2023

July 11, 2023