Hardware-assisted solutions to secure embedded systems on logic devices

Dr. Piedad Brox Jiménez

p.brox@csic.es

International Workshop on

Cryptographic architectures embedded in logic devices 2023

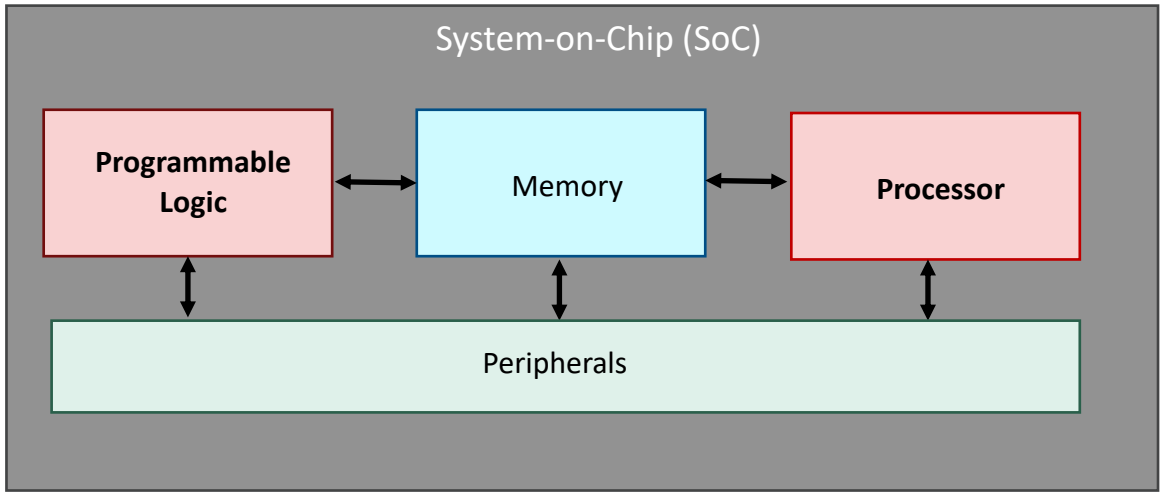
June 12-13, 2023

Outline

1. Introduction to **embedded systems on System-on-Chips** (SoCs)
2. SoC **security features**
3. Ad-hoc **HW RoT**
4. **Use** of a ad-hoc HW RoT
5. HW RoT in the **quantum** era
6. **Concluding remarks**

System-on-Chip (SoC)

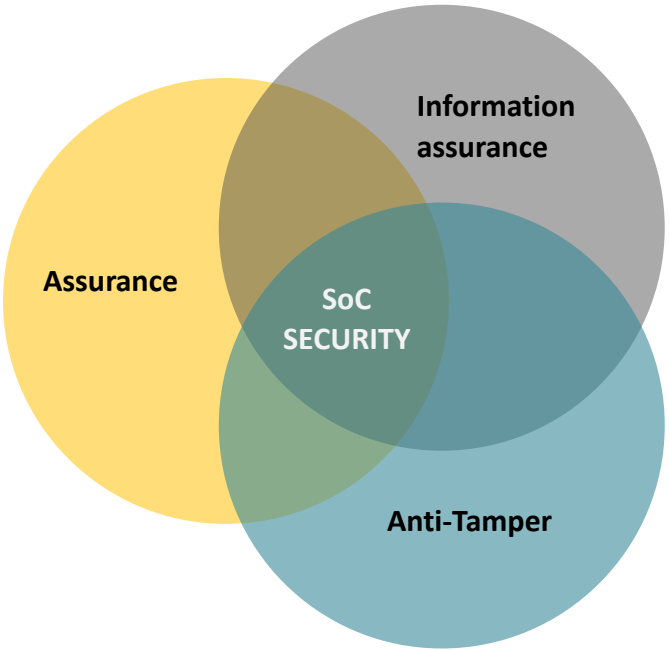
- Essential components of embedded systems implemented on SoCs
- **Hardware components**: processor, programmable logic, memory, and peripherals into complete SoC designs



- Is this embedded system immune to attacks?

SoC security

1. **Assurance**: software, firmware, and IPs must be "Trojan-free"
2. **Information assurance**: the device is handling or processing data that should be protected
3. **Anti-Tamper**: techniques to avoid cloning, reverse engineering or other types of attacks that can extract the IP



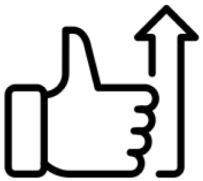
Security Throughout the SoC Lifecycle

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

Analysis of SoC security

- Layered SoC architecture:

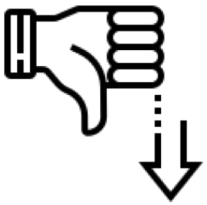
- Commercial solutions: Xilinx (ARM Cortex), Intel (Nios II, ARM HPC)



Variety

Design tools

Upgrade facilities

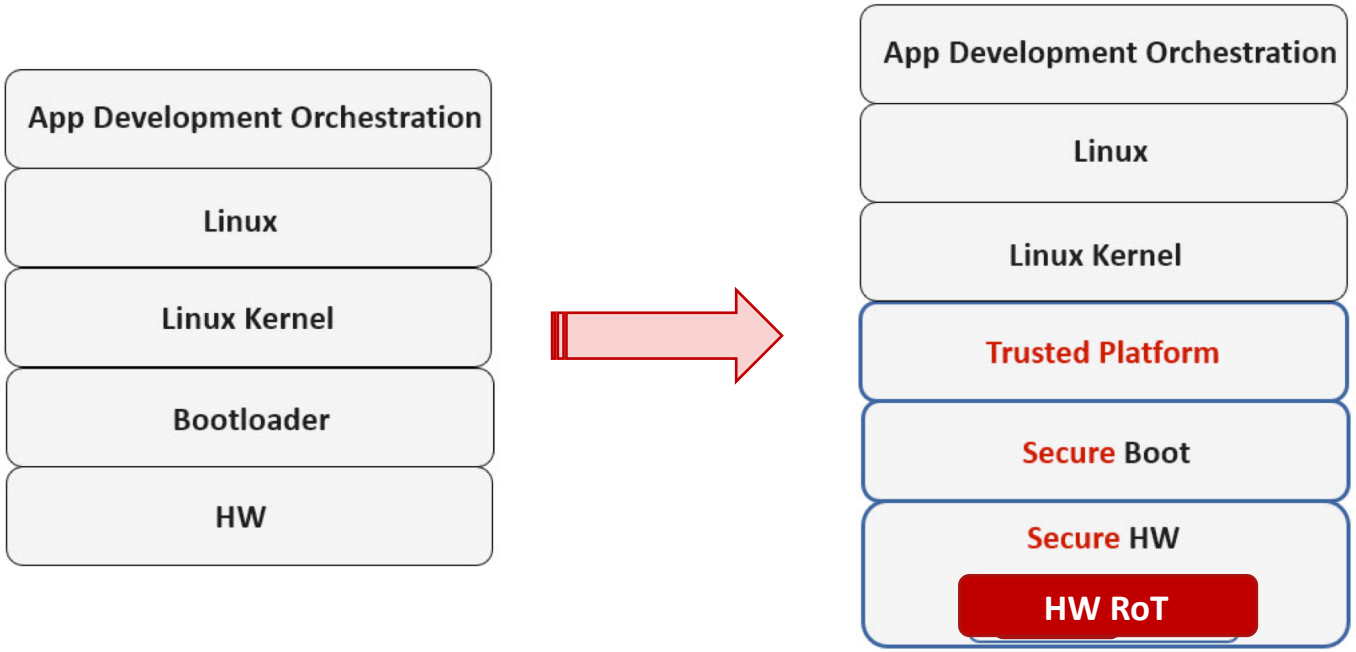


Lack of flexibility

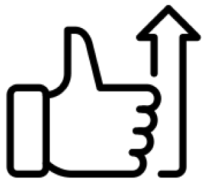
Security features

Security features for SoC

- **Secure** layered SoC architecture:

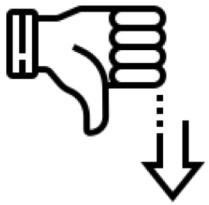


- Secure commercial solutions: high-end SoC families (Xilinx, Intel, Microchip)



Secure initialization

Crypto keys



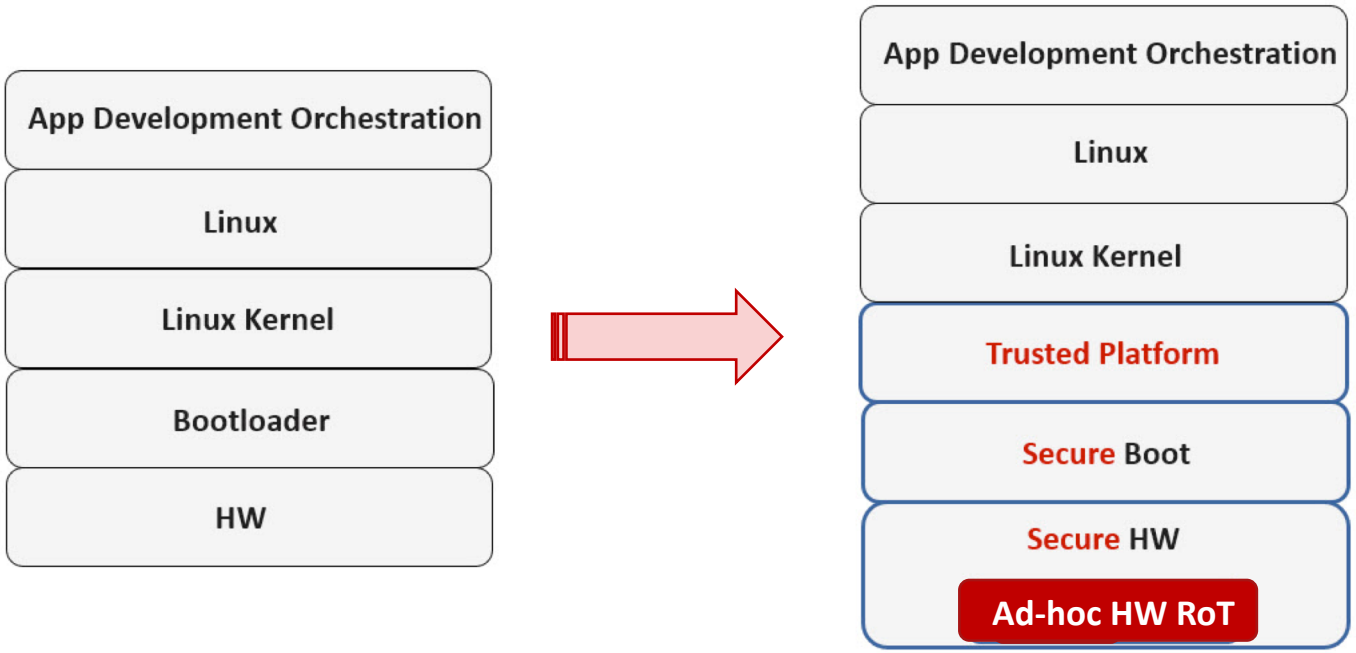
High cost

Technological dependency

Lack of flexibility

Dependency on 3rd vendors

Our approach

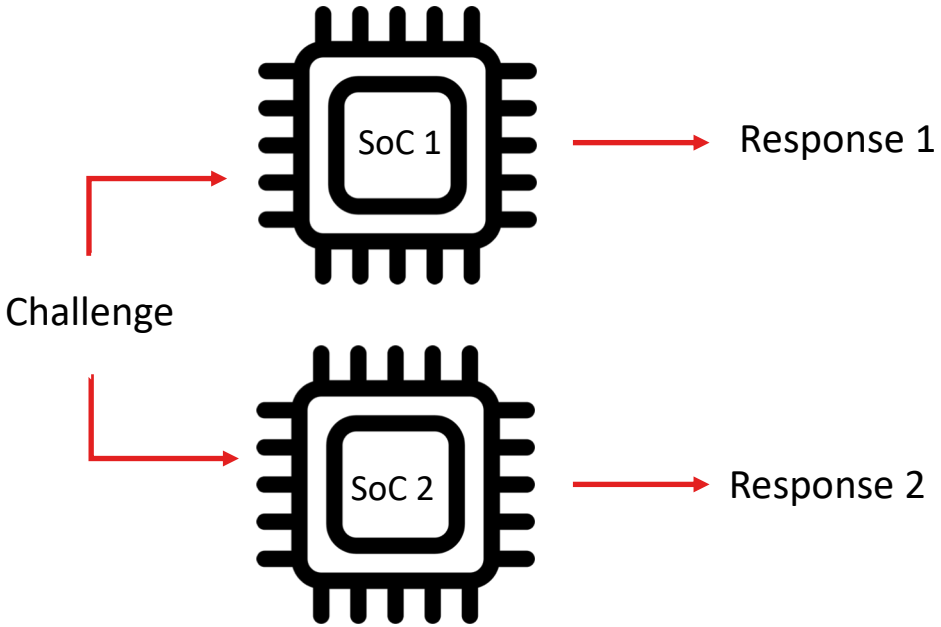


- **Building ad-hoc HW RoT**
  - ✓ Modular
  - ✓ Evolves over time
  - ✓ Technological independency
  - ✓ Migration to ASIC implementations

Ad-hoc HW RoT: PUF

- **Physical Unclonable Function (PUF)**

  - ✓ CR mechanism (random variations during manufacturing process)
  - ✓ Properties (unique, reliable, unpredictable)
  - ✓ Anti-counterfeit (physical unclonability)
  - ✓ Easy implementation (low-power consumption)
  - ✓ On-line generation



Device digital identity

Entropy source

Ad-hoc HW RoT: PUF

- **A PUF architecture on programmable logic devices**
  - ✓ Delay-based silicon PUF
  - ✓ Competition among identical ROs
  - ✓ Integration of the PUF design as an IP using memory-mapped AXI bus interfaces
  - ✓ Several updates of the architecture

  - ✓ The processor eases the extensive characterizations of the PUF response to evaluate:
    - ➢ Generation of reliable digital identifiers
    - ➢ Generation of random numbers

On-Line Evaluation and Monitoring of Security Features of an RO-Based PUF/TRNG for IoT Devices, L.F. Rojas-Muñoz et al. Sensors, vol. 23, no. 8, article 4070, 2023

Ad-hoc HW RoT: PUF

- **A PUF architecture on programmable logic devices**

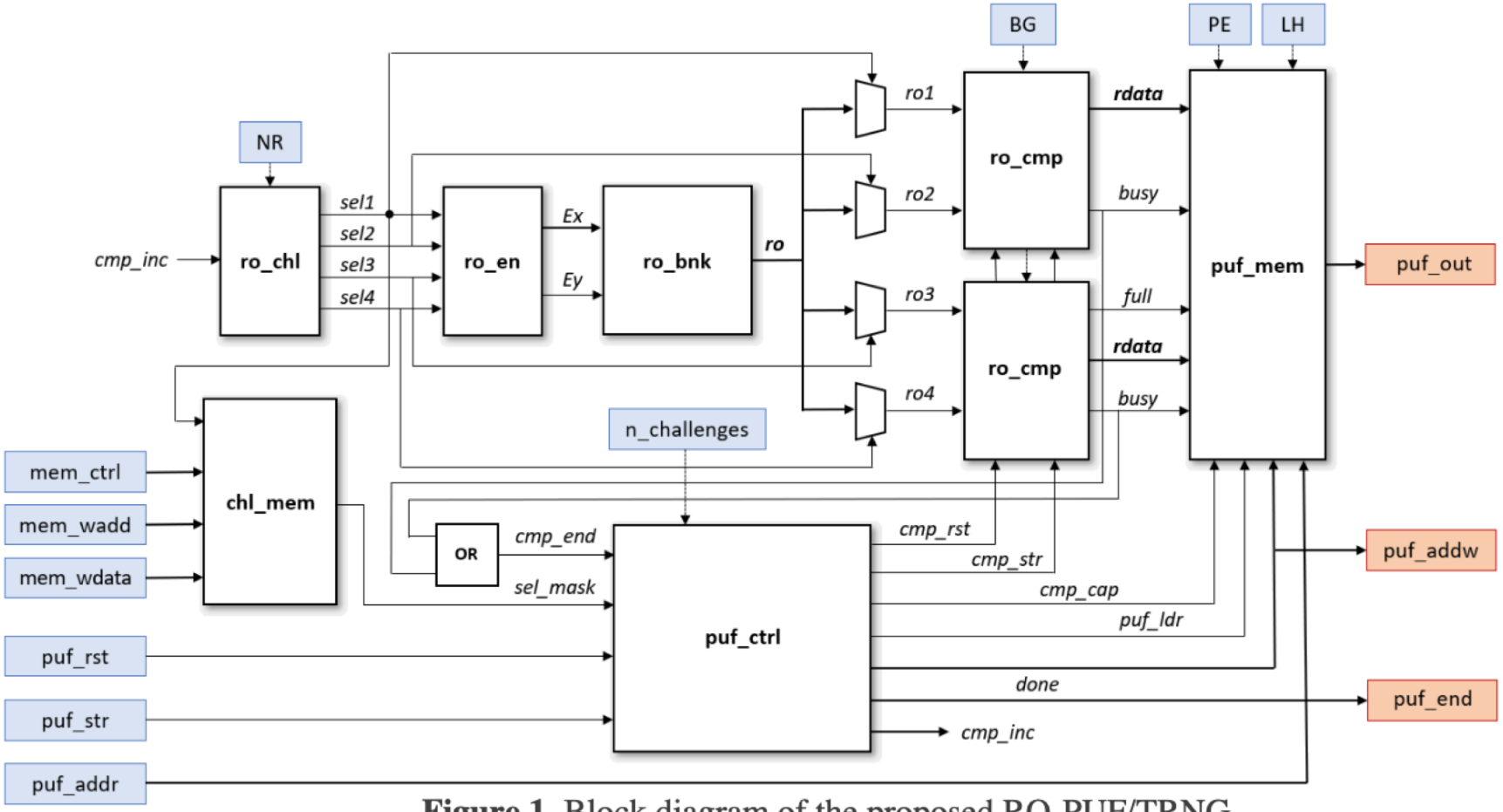
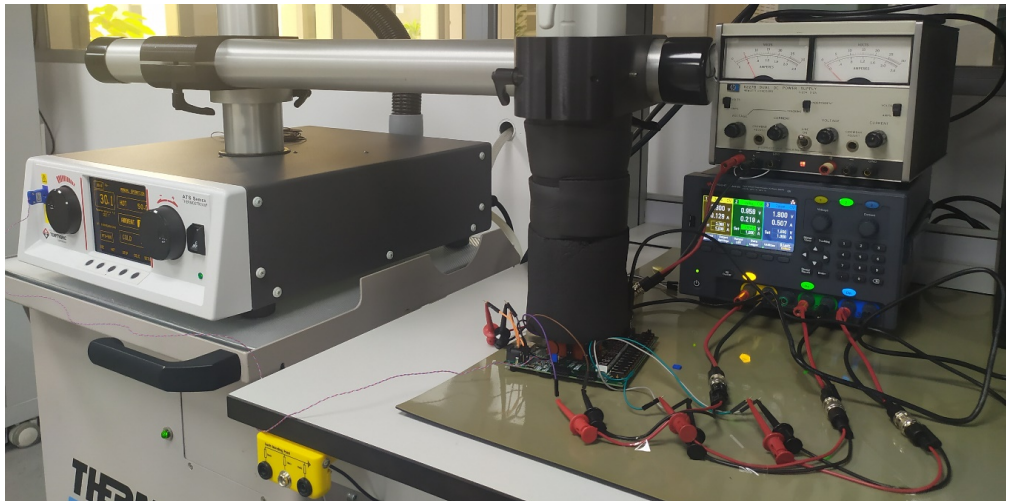


Figure 1. Block diagram of the proposed RO-PUF/TRNG

ro_bnk → Matrix of ROs (4 stage ROs per CLB)
ro_cmp → 2 block for simultaneous RO-pair comparisons
ro_chl → Challenge generation mechanism
chl_mem → Optimal challenge selector
puf_mem → Store and retrieve the output2
puf_ctrl → Contrl of system operation

Ad-hoc HW RoT: PUF

- **A PUF architecture on programmable logic devices**
  - Generation of an SDK (Software Development Kit) with functions and applications to process the quality of the PUF response.
    - Software online characterization
  - Evaluation of the PUF performance under variations:
    - power supply
    - temperature



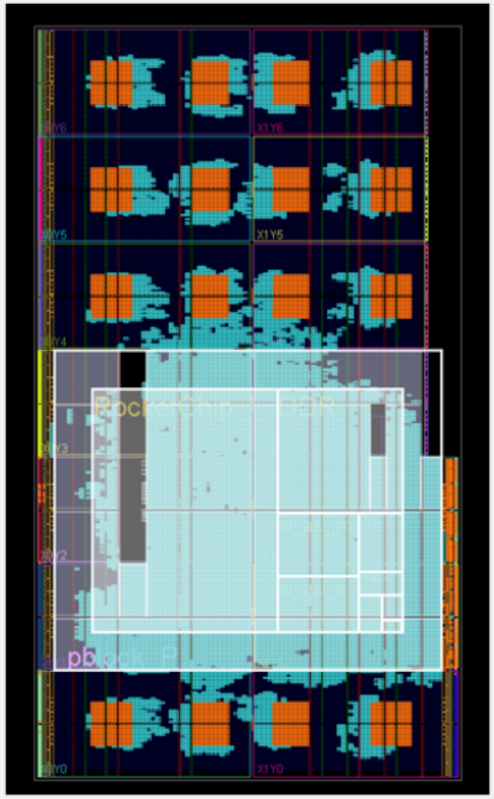
Entropy source:

- ✓ Randomness Assessment (15 tests, NIST 800-22 recommendation)
- ✓ Validation (10 tests, NIST 800-90b recommendation)
- ✓ Avaliable in the GitLab repository IMSE.HwSec

On-Line Evaluation and Monitoring of Security Features of an RO-Based PUF/TRNG for IoT Devices, L.F. Rojas-Muñoz et al. Sensors, vol. 23, no. 8, article 4070, 2023

Ad-hoc HW RoT: PUF

- **A PUF architecture on programmable logic devices**
  - ✓ Different programmable devices
  - ✓ Hard and soft processor cores (32 and 64 bits)

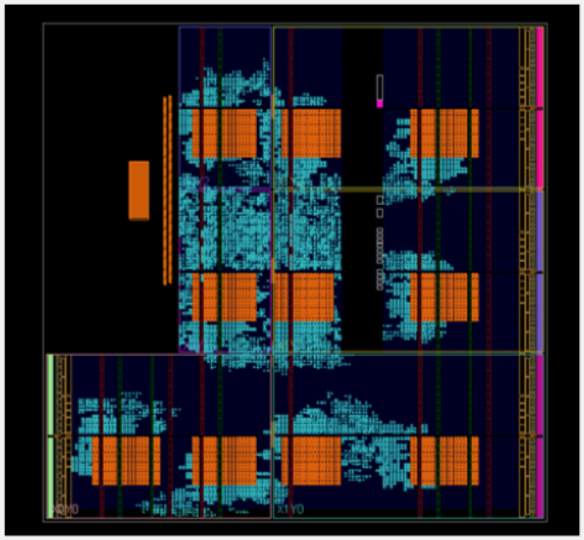


Genesys 2 board
Kintex XC7K325T FPGA

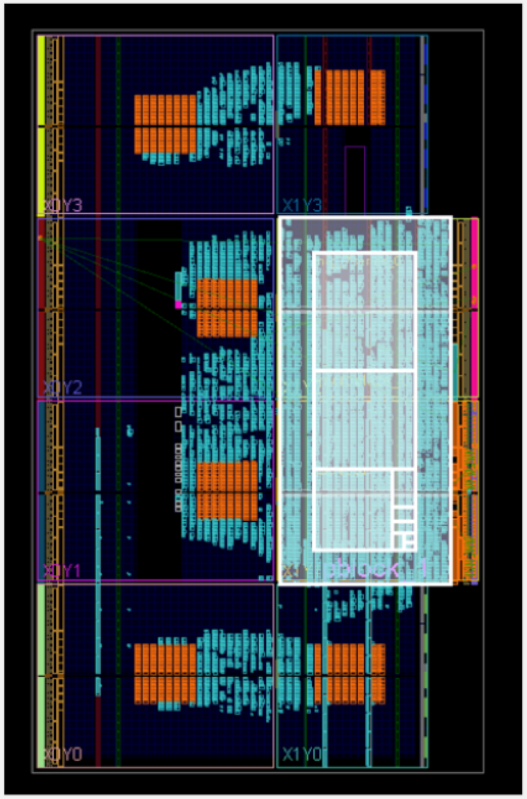
Rocket64B1 - RISC-V
Linux

Nexys- A7 board
Artix XC7A100T FPGA

Pynq-Z2 board
Zynq XC7Z020 SoC



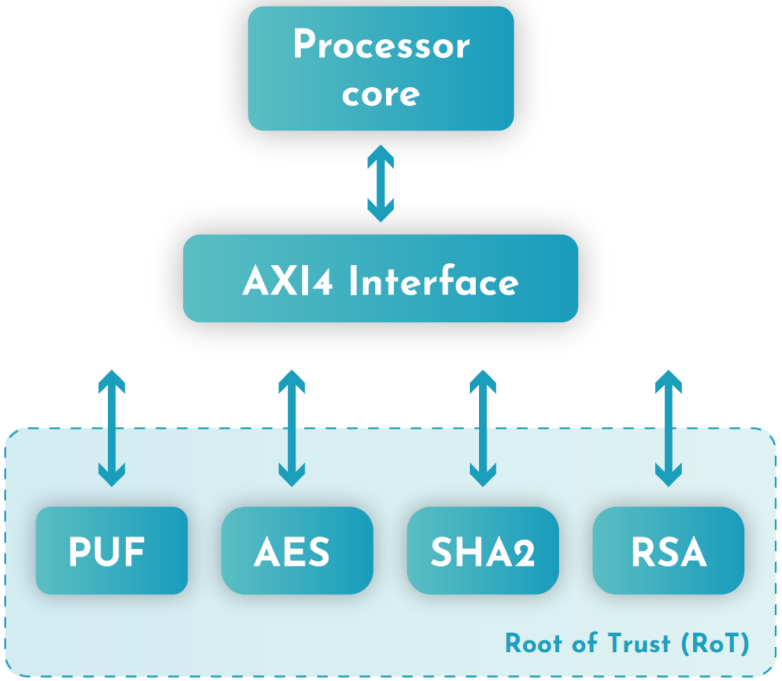
ARM dual-core Cortex-A9
Pynq - Petalinux



MicroBlaze 32-bit soft-core
Standalone

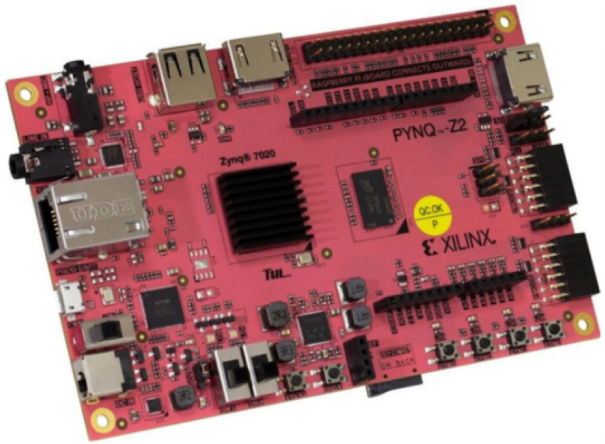
Ad-hoc HW RoT: crypto accelerators

- **Symmetric ciphers**
  - ✓ AES
  - ✓ Full hardware implementation (standard compliance, NIST validation)
- **Hashing**
  - ✓ SHA2
  - ✓ Full hardware implementations (standard compliance, NIST validation)
- **Digital signatures**
  - ✓ RSA (standard compliance, NIST validation)
  - ✓ Hardware accelerator



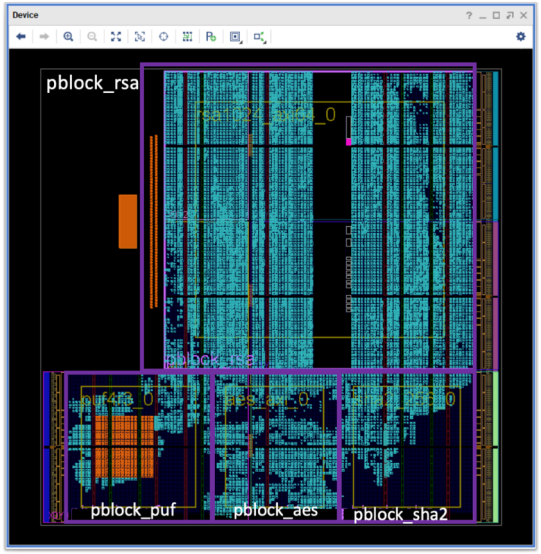
Ad-hoc HW RoT: example 1

- Development board



Xilinx Zynq7020 SoC Specifications
2 x Cortex-A9 cores running @ 650Mhz
Programmable logic (Artix-7 FPGA equivalent) with: • 13.3K logic slices, each with four 6-input LUTs and 8 flip-flops • 630 KB of fast block RAM • 4 clock management tiles • 220 DSP slices • On-chip analog-to-digital converter (XADC)
1 Gbps Ethernet, USB 2.0, SDIO
SPI, UART, CAN, I2C

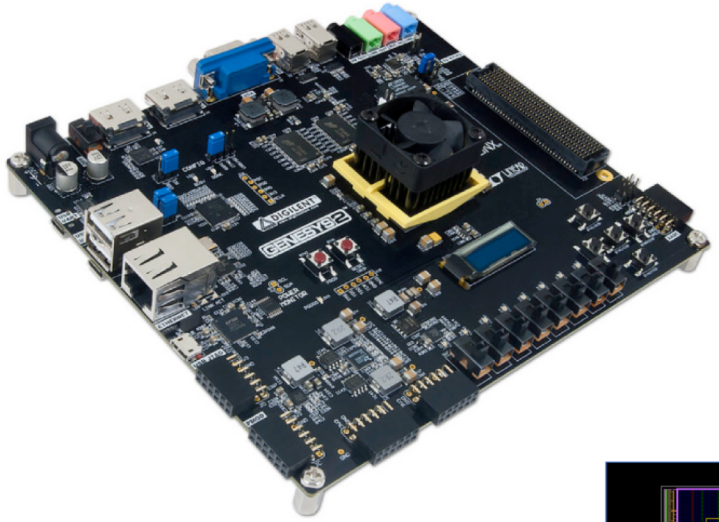
- Floor planning and resource distribution



Hard-core

Ad-hoc HW RoT: example 2

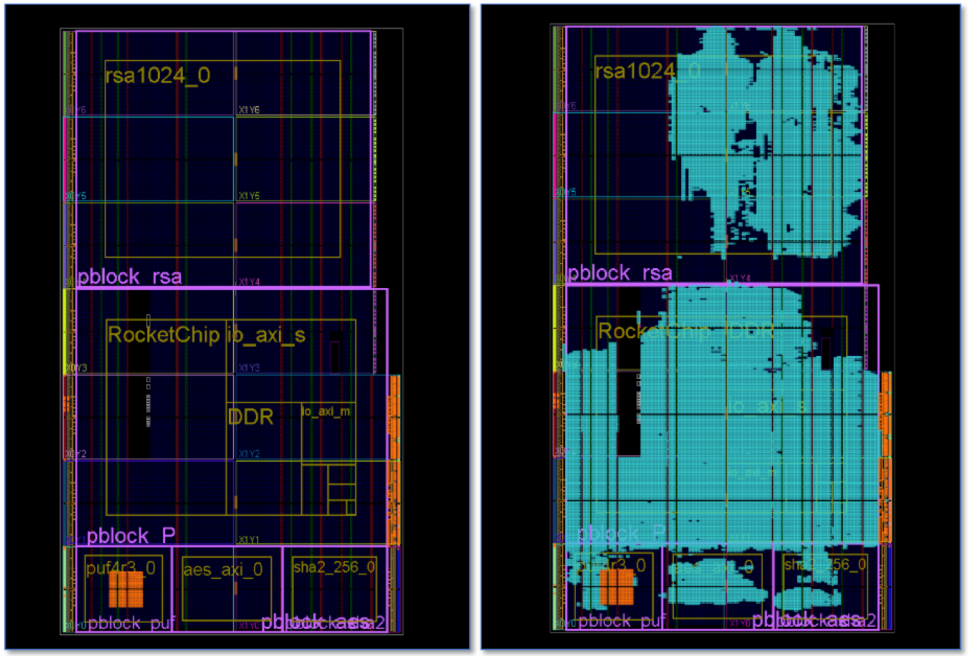
- Development board



Xilinx Kintex-7 XC7K325T-2FFG900C FPGA Specifications
Logic cells: • 50.9K logic slices, each with four 6-input LUTs and 8 flip-flops • 16Mbits of fast block RAM • 10 clock management tiles • 840 DSP slices • On-chip analog-to-digital converter (XADC)
Ethernet RJ-45 10/100/1000
USB-UART Bridge, USB-JTAG bridge

- Floor planning and resource distribution

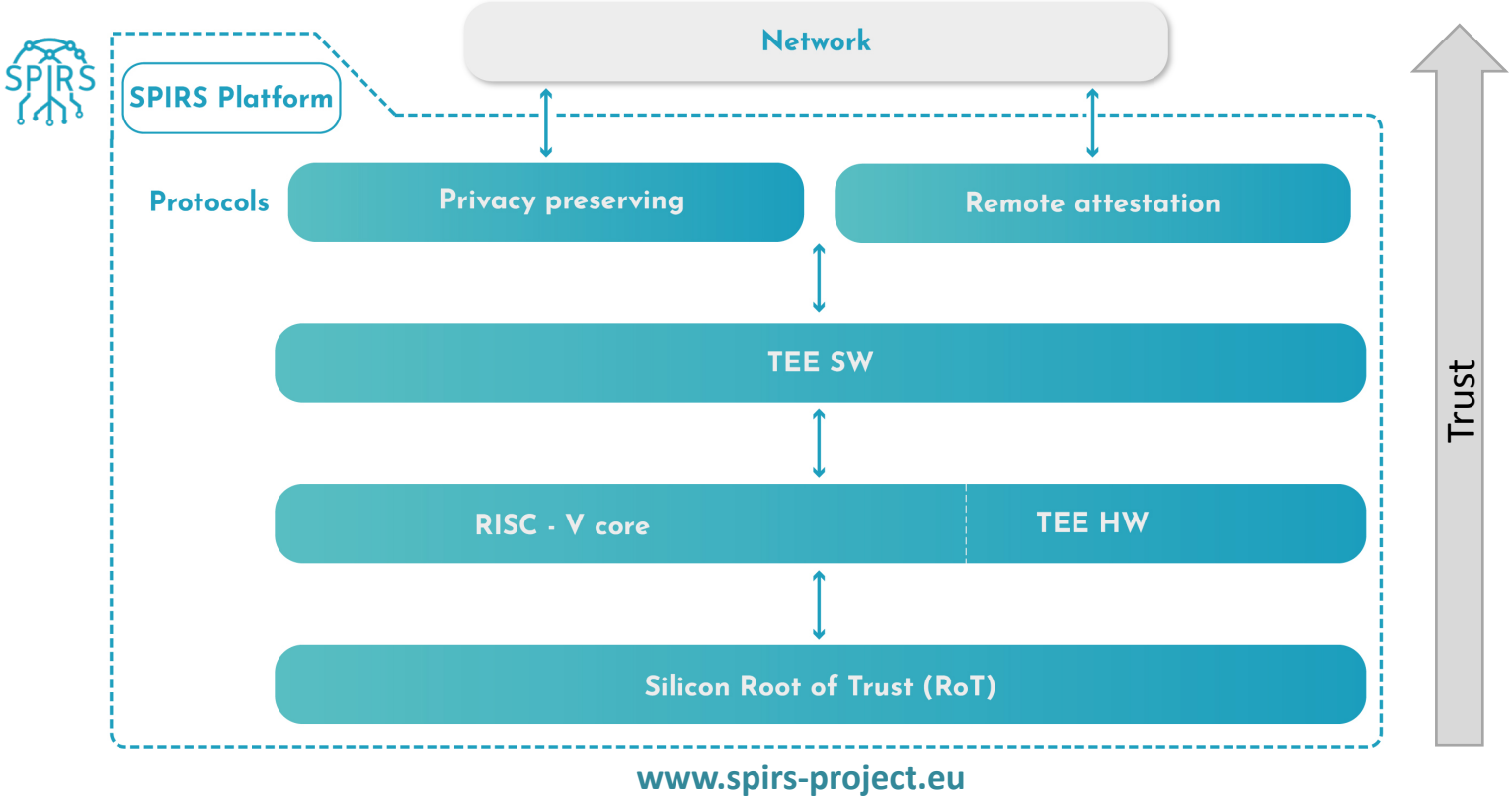
RISC-V soft-core



How do you use a HW RoT?

- **SPIRS project**

  To establish **chains of trust** rooted in the silicon manufacturing process for ICT systems, and apply them in improving the supply chain for networked infrastructures



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

How do you use a HW RoT?

- **SPIRS project**

HARDWARE ROOT OF TRUST

- Device-Unique Hardware ID
- Hardware entropy source
- Crypto accelerators
- Hardware countermeasures

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

How do you use a HW RoT?

- **SPIRS project**

HARDWARE ROOT OF TRUST

- Device-Unique Hardware ID
- Hardware entropy source
- Crypto accelerators
- Hardware countermeasures

BUILD TRUST

- Customized TEE based on Keystone
- Measured Secure Boot (DICE specifications)

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

How do you use a HW RoT?

- **SPIRS project**



HARDWARE ROOT OF TRUST	BUILD TRUST	MAINTAIN TRUST
• Device-Unique Hardware ID • Hardware entropy source • Crypto accelerators • Hardware countermeasures	• Customized TEE based on Keystone • Measured Secure Boot (DICE specifications)	• Privacy protection measures • Privacy respectful audit trails for identifying security threats and monitor performance

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

How do you use a HW RoT?

- **SPIRS project**

HARDWARE ROOT OF TRUST

- Device-Unique Hardware ID
- Hardware entropy source
- Crypto accelerators
- Hardware countermeasures

BUILD TRUST

- Customized TEE based on Keystone
- Measured Secure Boot (DICE specifications)

MAINTAIN TRUST

- Privacy protection measures
- Privacy respectful audit trails for identifying security threats and monitor performance

PROVE TRUST

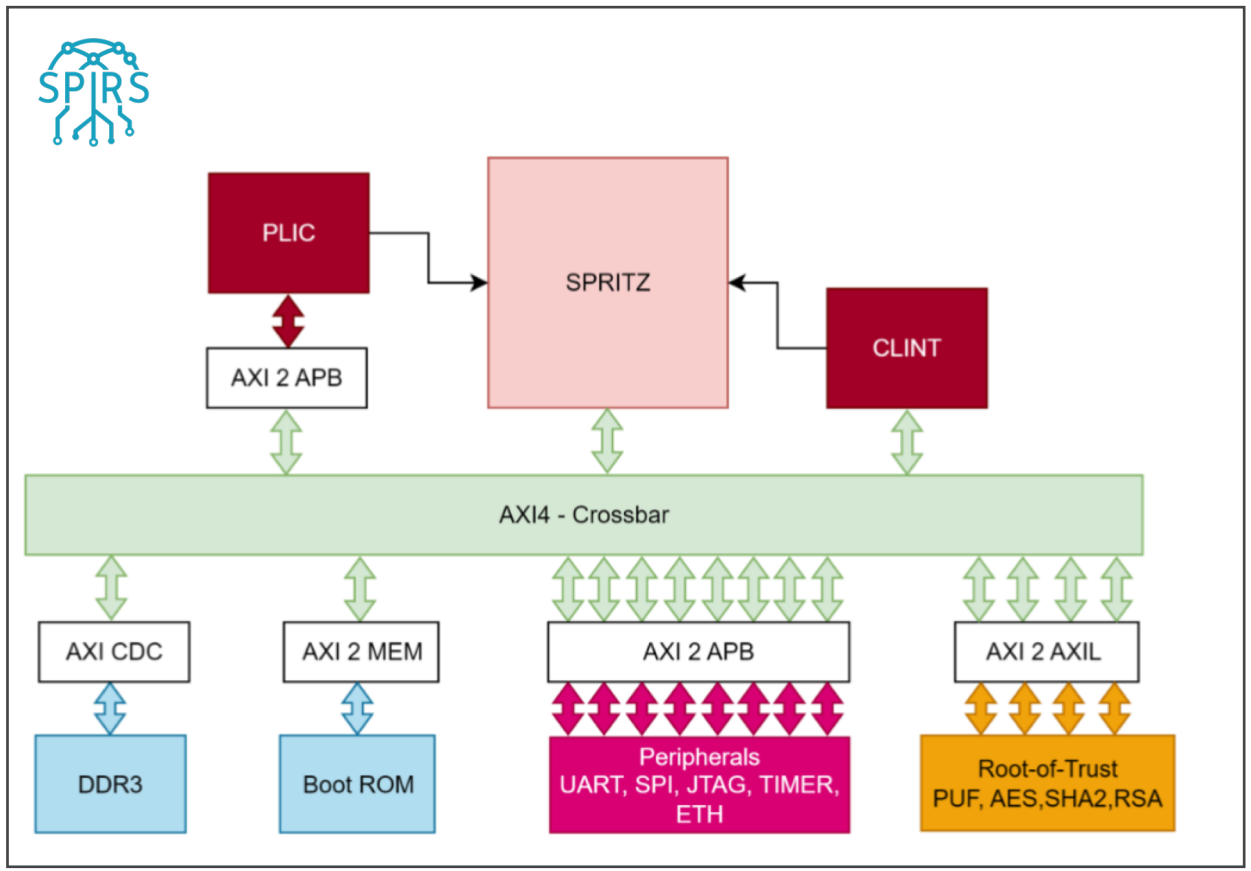
- Attestation mechanisms
- Integration into network infrastructures
- Validation in real use cases

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

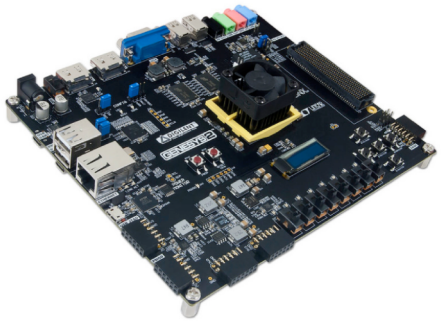
How do you use a HW RoT?

- **SPIRS project**

  Block diagram of hardware components



- SPRITZ: secure version of the CVA6 core (OpenHW group)
- Implementation on Genesys2 board

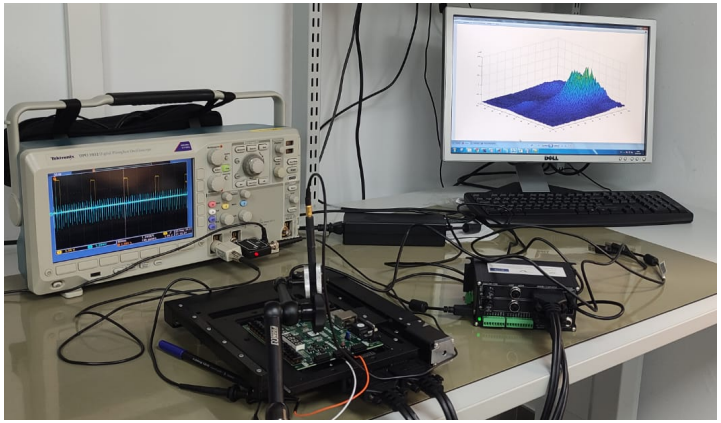


Secure Platform for ICT systems rooted at the silicon manufacturing process. C.Andriamisaina et al. RISC-V Summit Europe 2023

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

RoT protection against attacks

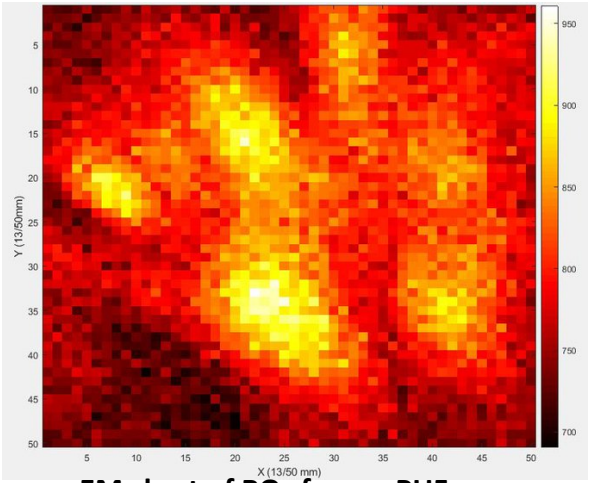
- Security evaluation: side-channel and fault-injection attacks



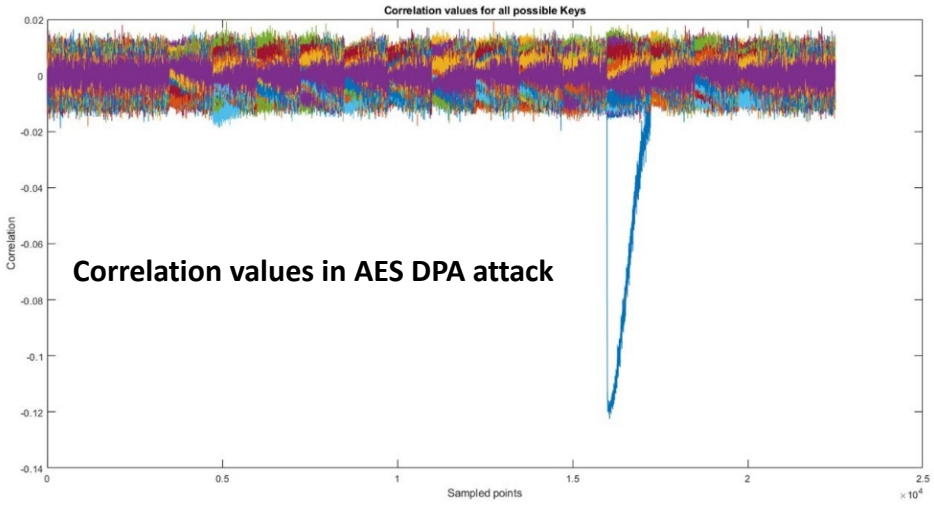
EM emanation experimental set-up

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

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



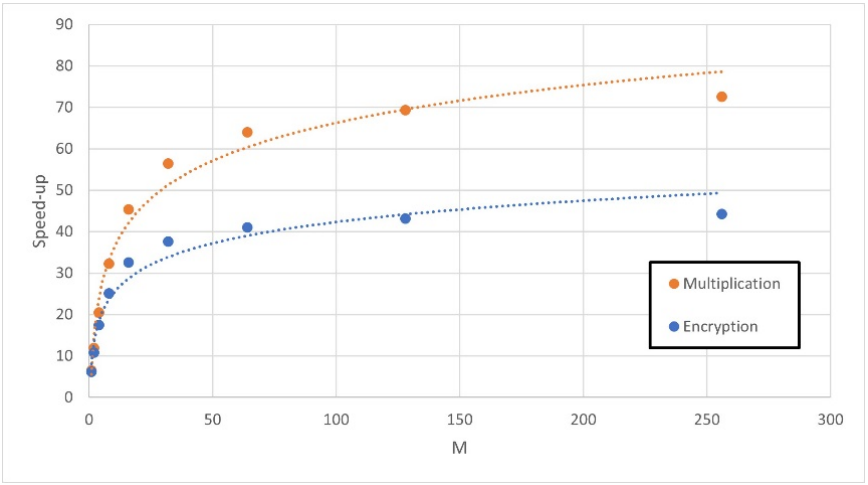
EM chart of ROs from a PUF



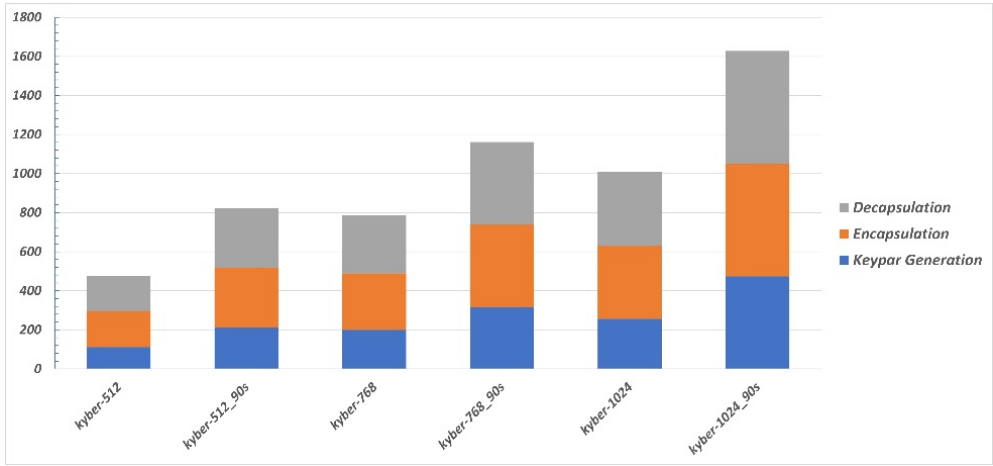
Design and Evaluation of Countermeasures Against Fault Injection Attacks and Power Side-Channel Leakage Exploration for AES Block Cipher
F.E. Potestad-Ordóñez et al., IEEE Access, vol. 10, pp 65548-65561, 2022

HW RoT in the quantum era

- Evaluation of Post-Quantum algorithms for data encryption and digital signatures
- Design of HW accelerators for polynomial truncated multiplication in NTRU algorithms:
  - NTRU standardized version in IEEE Std 1363.1
  - Both NTRU in the third round of the NIST Post-Quantum competition
- Preliminary study about different schemas to accelerate the NTT transformation:
  - KEM through CRYSTALS-Kyber
  - digital signature in CRYSTALS-Dilithium on embedded systems



HW vs SW acceleration of the multiplication and encryption in NTRU-HPS Round-3



SW performance of the CRYSTALS-Kyber cryptosystem (on ARM-v8)

Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems
E. Camacho-Ruiz et al, Cryptography, vol. 7, no.2, article 29, 2023

Concluding remarks

- Security of **embedded processors** → secure digital world
- **Ad-hoc HW RoT**:

1. **Hardware-assisted** solutions to secure embedded systems:
   - Efficient in timing performance and power-consumption
   - Affordable monetary cost
   - Suitable to be implemented on different devices
   - Compliant with security standards
2. **Next steps**:
   - Inclusion of HW countermeasures
   - Inclusion of HW accelerators for PQC