

TRUSTED EMBEDDED SYSTEMS BASED ON RISC-V PROCESSORS

IMSE
-cnm



Instituto de
Microelectrónica
de Sevilla

PIEDAD BROX JIMÉNEZ

brox@imse-cnm.csic.es



OUTLINE

1. Motivation
2. Chains of Trust
3. Root of Trust (RoT) for Embedded Systems
4. Building blocks of a hardware RoT
5. Available solutions for Trusted Embedded Systems using RISC-V
6. Conclusions

1. MOTIVATION

- Open hardware revolution
- Attractive solution:
 - ✓ Open-source, royalty-free Instruction Set Architecture (ISA)
 - ✓ Features to increase computer speed, yet reduce cost and power use
 - ✓ Optional extensions → customized designs
- Processor innovation:
 - ✓ Attractive solution for industry → start-ups
 - ✓ Companies that belongs to RISC-V foundation
- Hardware manufacturer → solution for IoT embedded devise



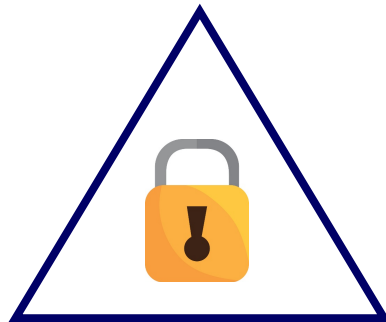
1. MOTIVATION

- Security and Privacy for electronic devices
 - ✓ Digital societies
- The core of cybersecurity → CIA triad:
 - ✓ **C**onfidentiality: control access to information
 - ✓ **I**ntegrity: data should be trustworthy and accurate over its lifetime
 - ✓ **A**vailability: reliable and constant access to data
- Privacy respectful solutions



1. MOTIVATION

- RISC-V vulnerability
 - ✓ Well-known architecture
 - ✓ SCARV: a side-channel hardened RISC-V platform (research project)
- Trusted embedded systems based on RISC-V processors
 - ✓ Hardware dedicated modules
- Multidisciplinary teams



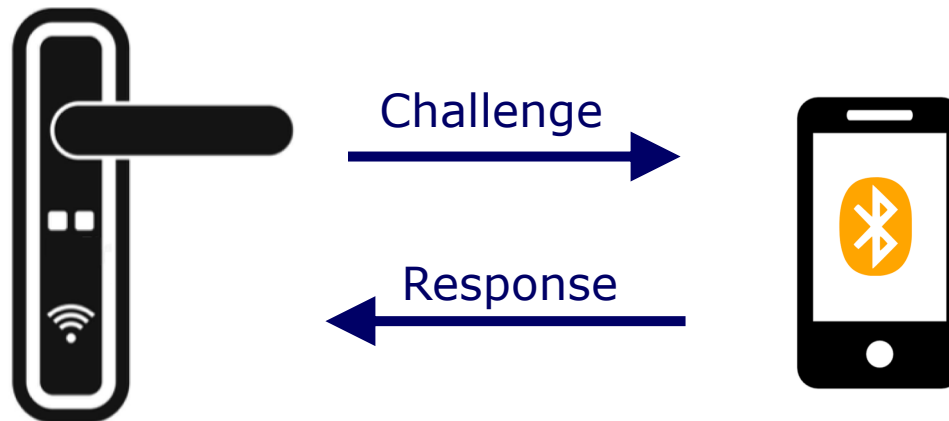
2. CHAINS OF TRUST

- Hybrid (hardware/software) nature of an embedded system
- A trusted chain is required:
 - ✓ **Hardware** → device identity
 - ✓ **Software** → bootloader and operating system
 - ✓ **Applications**
 - ✓ **Network**
- Authentication at every level



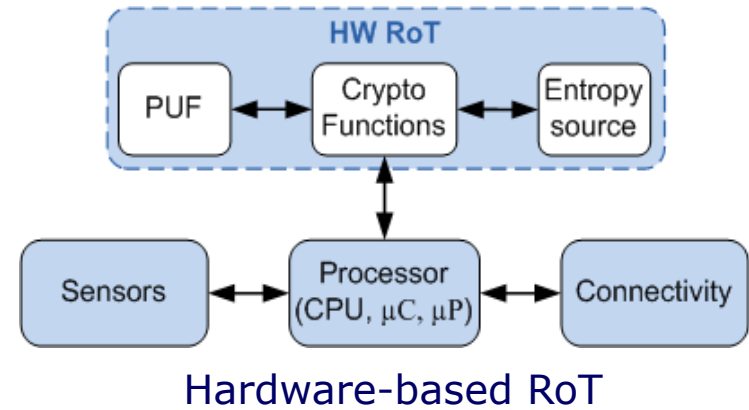
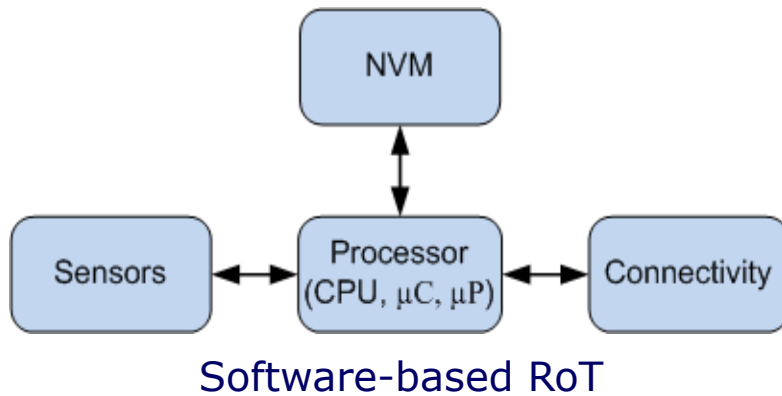
3. RoT ON EMBEDDED SYSTEMS

- Root-of-Trust (**RoT**) → always be trusted
- Alternatives:
 - ✓ Software
 - ✓ Hardware
 - ✓ Hybrid
- Device Authentication → Challenge-response protocol



4. BUILDING BLOCKS OF A HARDWARE RoT

- Building blocks [1]:
 - ✓ Device identity → Physical Unclonable Functions (**PUF**)
 - ✓ Entropy source
 - ✓ Crypto functions



4. BUILDING BLOCKS OF A HARDWARE RoT

- PUF definition: Challenge-Response Pair (CPR)

- PUF characteristics:

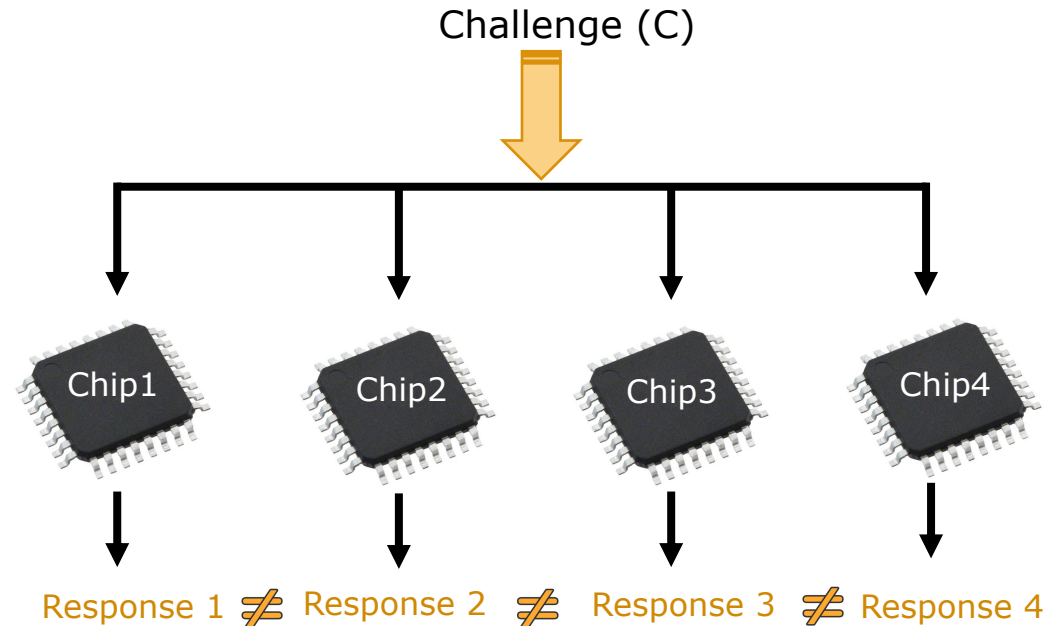
- ✓ Unclonable
- ✓ Uniqueness
- ✓ Reproducibility
- ✓ Unpredictable

- Silicon PUFs [2]:

- ✓ SRAM
- ✓ Ring Oscillators

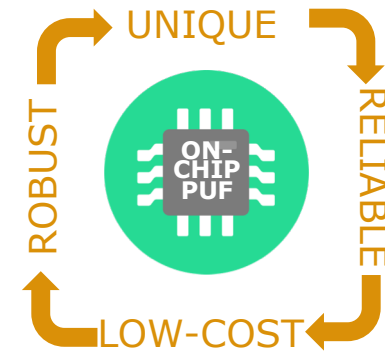
- PUF assumptions:

- ✓ A Response (R_i) gives negligible info on another Response (R_j)
- ✓ Infeasible to model PUF (accurately)
- ✓ Physical tampering will destroy it or will modify radically



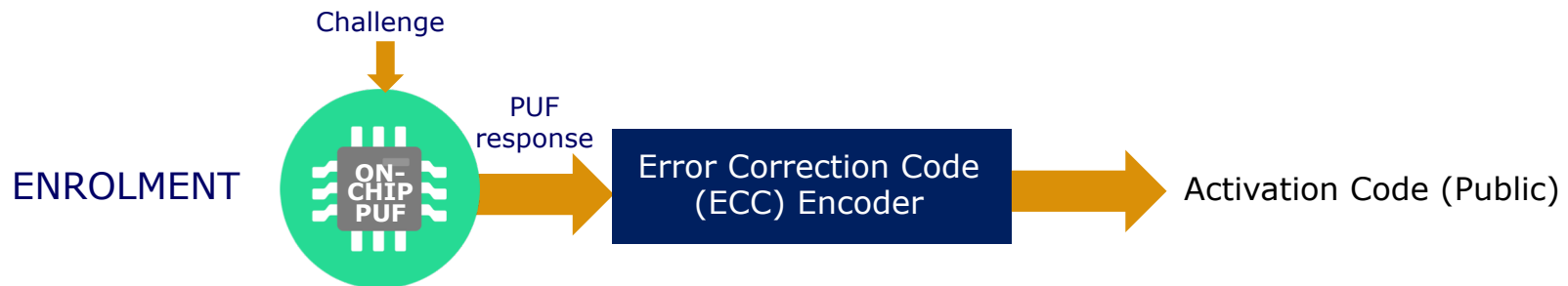
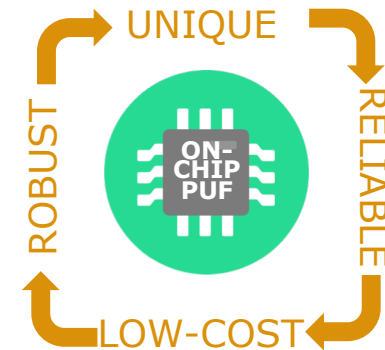
4. BUILDING BLOCKS OF A HARDWARE RoT

- Design of a silicon PUF



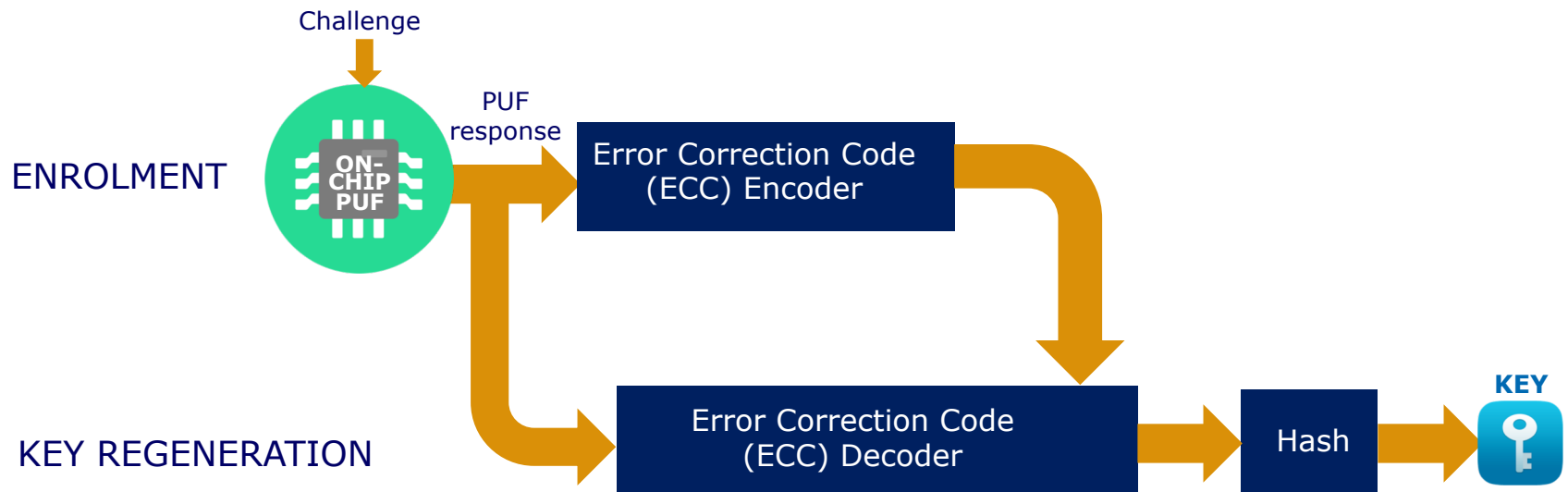
4. BUILDING BLOCKS OF A HARDWARE RoT

- Design of a silicon PUF
- PUF → cryptographic keys:
 - ✓ Key Enrolment Phase



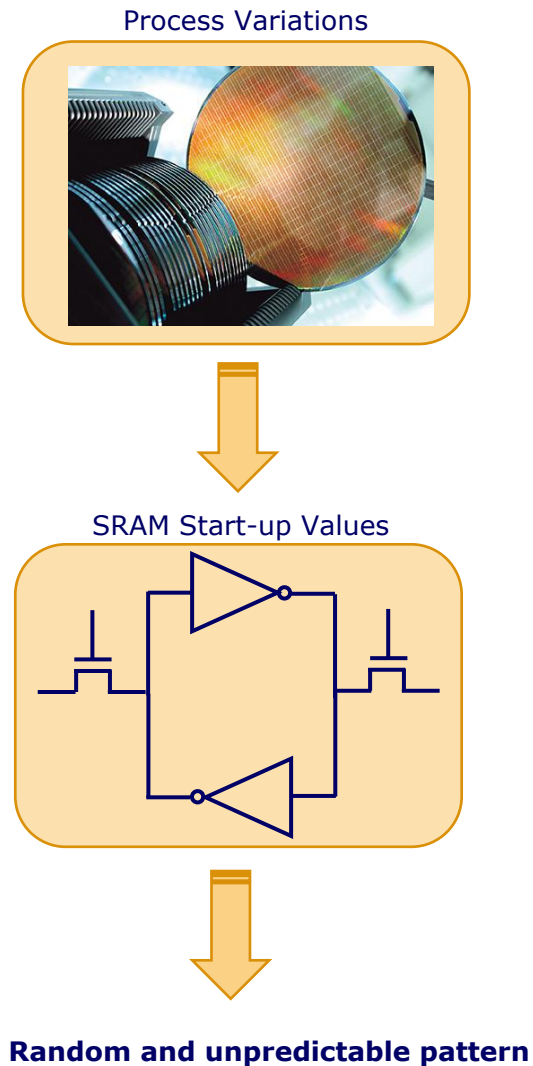
4. BUILDING BLOCKS OF A HARDWARE RoT

- Design of a silicon PUF
- PUF → cryptographic keys:
 - ✓ Key Enrolment Phase
 - ✓ Key Regeneration Phase



4. BUILDING BLOCKS OF A HARDWARE RoT

- Generation of random numbers [2]:
 - ✓ Initialization vectors
 - ✓ Nonces
 - ✓ Challenges
 - ✓ Keys
- Source entropy:
 - ✓ Unpredictable PUF behaviour
- One example:
 - ✓ SRAM PUF: start-up values



4. BUILDING BLOCKS OF A HARDWARE RoT

- Crypto functions: CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) [3]

- ✓ Symmetric Cryptography
- ✓ Authenticated ciphers
- ✓ SW and HW realizations
- ✓ Portfolio of solutions



Cryptographic competitions

| | |
|---|---|
| <p>Introduction Secret-key cryptography Disasters Features</p> <p>Focused competitions: AES eSTREAM SHA-3 PHC CAESAR</p> <p>Broader evaluations: CRYPTREC NESSIE</p> <p>CAESAR details: Submissions Call for submissions Call draft 5 Call draft 4 Call draft 3 Call draft 2 Call draft 1 Committee Frequently asked questions</p> | <p>CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness</p> <p>Timeline</p> <ul style="list-style-type: none"> • M-20, 2012.07.05-06: DIAC: Directions in Authenticated Ciphers. Stockholm. • M-14, 2013.01.15: Competition announced at the <i>Early Symmetric Crypto</i> workshop in Mondorf-les-Bains; also announced online. • M-7, 2013.08.11-13: DIAC 2013: Directions in Authenticated Ciphers 2013. Chicago. • M0, 2014.03.15: Deadline for first-round submissions. • M2, 2014.05.15: Deadline for first-round software. • M5, 2014.08.23-24: DIAC 2014: Directions in Authenticated Ciphers 2014. Santa Barbara. • M16, 2015.07.07: Announcement of second-round candidates. • M17, 2015.08.29: Deadline for second-round tweaks. • M18, 2015.09.15: Deadline for second-round software. • M18, 2015.09.28-29: DIAC 2015: Directions in Authenticated Ciphers 2015. Singapore. • M27, 2016.06.30: Deadline for Verilog/VHDL. • M29, 2016.08.15: Announcement of third-round candidates. • M30, 2016.09.15: Deadline for third-round tweaks. • M30, 2016.09.26-27: DIAC 2016. Nagoya, Japan. • M31, 2016.10.15: Deadline for third-round software. • M40, 2017.07.15: Deadline for third-round Verilog/VHDL. • M40, 2017.07.15: Deadline for optimized third-round software. • M48, 2018.03.05: Announcement of finalists. • M59: 2019.02.20: Announcement of final portfolio. |
|---|---|

- 1) Lightweight applications (resource constrained environments)
- 2) High-performance applications
- 3) Defense in depth

4. BUILDING BLOCKS OF A HARDWARE RoT

- Crypto functions: NIST Post-Quantum Competition [4]
 - ✓ Second round (26 candidates)
 - ✓ Two categories
 - 1) Public-key Encryption and Key-establishment Algorithms
 - 2) Digital Signatures Algorithms



NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography

f G+ t

Project Overview

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. [Full details can be found in the Post-Quantum Cryptography Standardization page.](#)

The Round 2 candidates were announced January 30, 2019. NISTIR 8240, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process is now available.





European Commission


Horizon 2020
European Union funding
for Research & Innovation


PQCrypto
ICT-645622

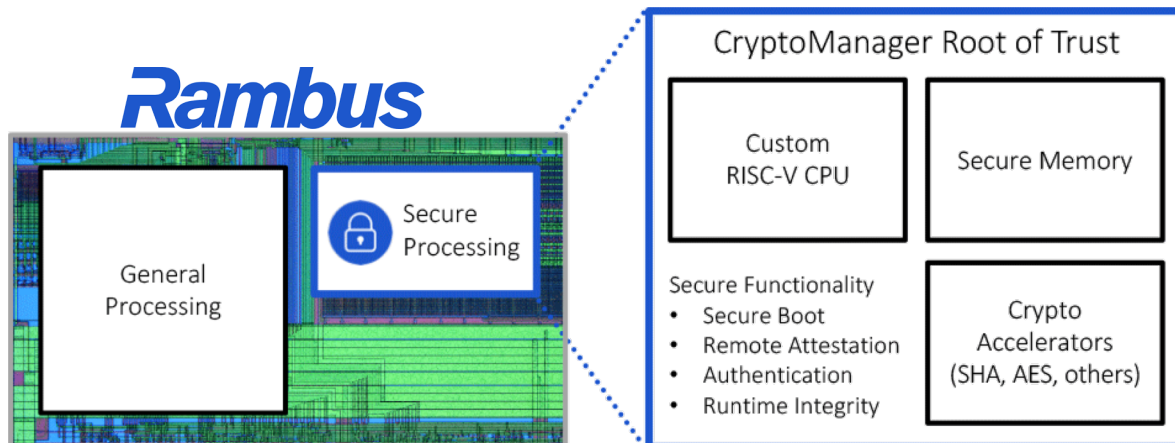



futureTPM


SAFE crypto

5. AVAILABLE SOLUTIONS FOR TRUSTED EMBEDDED SYSTEMS USING RISC-V

- CryptoManager Root of Trust (provided by Rambus) [5]:
 - ✓ Family of fully-programmable hardware security co-processor
 - ✓ Security IP
 - ✓ Custom RISC-V CPU (specifically for security)
 - ✓ Standard applications
- Closed solution:
 - ✓ Not privacy-respectful solution
 - ✓ Lack of flexibility to include new crypto functions



5. AVAILABLE SOLUTIONS FOR TRUSTED EMBEDDED SYSTEMS USING RISC-V

- An attested execution processor (Sanctum Processor) [6]:
 - ✓ Secure boot process and remote attestation
 - ✓ Chain of trust rooted at hardware → PUF
 - ✓ RISC-V Rocket chip architecture
- Keystone [7]:
 - ✓ Open framework for custom Trusted Execution Environments
 - ✓ Use of secure hardware enclaves
 - ✓ Authenticate software and chip itself
- Further improvements:
 - ✓ Not integration of hardware crypto functions
 - ✓ Not conceived for small devices (embedded systems)



Keystone

6. CONCLUSIONS

- RISC-V core + Hardware RoT
- Building blocks of RoT (modular, flexible, extensible solution):
 1. Silicon PUF
 - ✓ Source of entropy
 - ✓ Re-generation of cryptographic keys & device authentication
 2. Software Authenticity
 - ✓ Secure bootloader using PUF response
 - ✓ Trusted Execution Environment (TEE) running on top of RISC-V
 3. Trusted Applications
 - ✓ Privacy Enabling Tools, Remote Attestation
- Open issues:
 - ✓ Integration of hardware crypto functions
 - ✓ Design of hw RoT for small devices (embedded systems)
 - ✓ Inclusion of trusted applications to provide end-to-end solutions

REFERENCES

- [1] M. Alioto, “Trends in Hardware Security: From basics to ASICs,” IEEE Solid-State Circuits Mag., 2019
- [2] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial”, Proc. Of the IEEE, 102 (8), 2014
- [3] <https://competitions.cr.yip.to/caesar.html>
- [4] <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>
- [5] <https://www.rambus.com/security/root-of-trust/cryptomanager-root-of-trust/>
- [6] I. Lebedev, K. Hogan, S. Devadas, “Secure Boot and Remote Attestation in the Sanctum Processor”, IEEE 31st Computer Security Foundations Symposium (CSF), 2018
- [7] D. Lee, D. Kohlbrenner, S. Shinde, D. Song, K. Asanovic, “Keystone: An Open Framework for Architecting TEEs”, arXiv: 1907.10119, 2019

TRUSTED EMBEDDED SYSTEMS BASED ON RISC-V PROCESSORS

IMSE
-cnm



Instituto de
Microelectrónica
de Sevilla

PIEDAD BROX JIMÉNEZ

brox@imse-cnm.csic.es