# Eros Camacho Ruiz

**PhD., Hardware Cryptography Researcher**

eroscamaru@gmail.com
camacho@imse-cnm.csic.es
Research Gate: Eros Camacho-Ruiz
Google Scholar: Eros Camacho-Ruiz
ErosCamacho
Eros Camacho Ruiz
https://eroscamacho.github.io/

## About Me

I am focusing on the research of hardware implementations of cryptographic deployments. Extensive experience in the study and use of cryptography developed to date (symmetric key, asymmetric key and digital signatures), as well as post-quantum cryptographic algorithms. I have developed accelerations of these algorithms at both SW and HW levels, evaluating countermeasures against side-channel attacks and including these solutions into embedded platforms for IoT. On my own, I have studied hacking techniques in order to detect and exploit vulnerabilities in web and communication environments.

## Education

**Doctoral Program in Physics Science and Technology** | ***Cum-Laude*** Sep. 2020 – Mar. 2024
*PhD Title: "Design of a hardware Root-of-Trust on embedded systems"* Univ. of Seville, Spain

**MsC on Microelectronics** Sep. 2018 – Jul. 2020
*Thesis: "Acceleration of Post-Quantum Cryptographic Algorithms Using HW/SW Co-Design Techniques"* Univ. of Seville, Spain

**BsC on Physics** Sep. 2013 – Jul. 2017
*Thesis: "Implementation of Quantum Monte Carlo Methods in GPU Architectures"* Univ. of Córdoba, Spain

## Work Experience

**Postdoctoral visiting researcher** Jun. 2024 – Sep. 2024
*Tampere University* Finland

- Hardware developing of ML-KEM.
- Side-channel attacks evaluation of the ML-KEM implementation.

**Cryptography Researcher in European project - QUBIP** Sep. 2023 – Present
*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC* Spain

- Leader of the technical aspects carried out by CSIC-IMSE.
- Leader of Task 2.2 of the WP2.
- Developing and implementation of PQC algorithm in HW in order to secure IoT devices based on Secure Elements.

**PhD visiting researcher** Jun. 2023 – Sep. 2023
*Tampere University* Finland

- Hardware implementation of post-quantum algorithms.
- Kyber768 implementations including countermeasures against side-channel attacks.

**FPU Grant** Dic. 2021 – Jun. 2023
*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC* Spain

- Contract obtained in competitive concurrence at national level.

- Design and implementation of a Root-of-Trust (RoT), including device identification solutions using analog PUFs and PQC algorithm acceleration based on digital modules, as well as other crypto modules.

**Research Assistant in National project** Sep. 2020 – Nov. 2021
*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC* Spain

- Study of SRAMs as PUFs.
- Simulation Analysis where the behavior of SRAMs as PUFs has been evaluated in thermal and aging variability.
- Study of RTN as a stochastic variable in PMOS transistors in order to study its stability to allow the development of PUFs. Its stability with temperature has also been evaluated.

**JAE-Intro Internship** Sep. 2019 – Jan. 2020
*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC* Spain

- Acceleration of PQC algorithms (NTRU) by means of HW/SW co-design techniques on ARM + FPGA-based SoCs of the Xilinx Zynq 7000 family (PYNQ-Z2).
- Realization of dedicated HW modules (Verilog / VHDL) for the implementation of polynomial multiplication.

## Patents

1. ***E. Camacho-Ruiz**, R. Castro-Lopez, E. Roca, P. Brox, and F. V. Fernandez,* "**Method and device for physical unclonable function (PUF) based on random telegraph noise (RTN),**" Univesity of Seville (40 %), CSIC (60 %). PCT Patent PCT/EP2023/057 799, 2023.

## Journal Publications

1. *L.F. Rojas-Muñoz, S. Sánchez-Solano, M. C. Martínez-Rodríguez, **E. Camacho-Ruiz**, P. Navarro-Torrero, P. Brox,* "**HW Root-of-Trust for Key Reconstruction, Message Authentication and Digital Signature,**" Journal of Cryptographic Engineering, *Peer-review pending*

2. ***E. Camacho-Ruiz**, M. C. Martínez-Rodríguez, S. Sánchez-Solano, and P. Brox,* "**Timing-Attack-Resistant Acceleration of NTRU Round 3 Encryption on Resource-Constrained Embedded Systems,**" Cryptography, vol. 7, no. 2, p. 29, Jun. 2023.

3. *M. C. Martínez-Rodríguez, L. F. Rojas-Muñoz, **E. Camacho-Ruiz**, S. Sánchez-Solano, and P. Brox,* "**Efficient RO-PUF for Generation of Identifiers and Keys in Resource- Constrained Embedded Systems,**" Cryptography, vol. 6, no. 4, p. 51, Oct. 2022.

4. *S. Sánchez-Solano, **E. Camacho-Ruiz**, M. C. Martínez-Rodríguez, and P. Brox,* "**Multi-Unit Serial Polynomial Multiplier to Accelerate NTRU-Based Cryptographic Schemes in IoT Embedded Systems,**" Sensors, vol. 22, no. 5, p. 2057, Mar. 2022.

5. *M. C. Martínez-Rodríguez, **E. Camacho-Ruiz**, P. Brox, and S. Sánchez-Solano,* "**A Configurable RO-PUF for Securing Embedded Systems Implemented on Programmable Devices,**" Electronics, vol. 10, no. 16, p. 1957, Aug. 2021.

6. ***E. Camacho-Ruiz**, S. Sánchez-Solano, P. Brox, and M. C. Martínez-Rodríguez,* "**Timing-Optimized Hardware Implementation to Accelerate Polynomial Multiplication in the NTRU Algorithm,**" J. Emerg. Technol. Comput. Syst. 17, 3, Article 35, 2021.

## Conference Publications

1. ***E. Camacho-Ruiz***, *A. Cabrera-Aldaya*, "**A Secure Hardware Implementation of ML-KEM,**" CHES 2025, *Peer-review pending*

2. ***E. Camacho-Ruiz***, *P. Navarro Torrero, M.C. Martínez-Rodríguez, P. Brox*, "**A compact hardware implementation of SHA2 and SHA3 for PQ Transition,**" CHES 2025, *Peer-review pending*

3. *P. Navarro Torrero*, ***E. Camacho-Ruiz***, *M.C. Martínez-Rodríguez, P. Brox*, "**RSA vs EdDSA: Comparative Study of Hardware Accelerators for Digital Signature Implementations on Embedded Systems,**" 2024 IEEE Nordic Circuits and Systems Conference (NorCAS), Luhn, Sweden, 2024, pp. 1-7.

4. ***E. Camacho-Ruiz***, *L. F. Rojas-Muñoz, A. Karmarkar, P. Navarro-Torrero, P. Brox, M. C. Martínez-Rodríguez*, "**Open Source API for a Hardware Root-of-Trust,**" RECSI 2024

5. *L. Rojas-Muñoz, S. Sánchez-Solano, M. C. Martínez-Rodríguez*, ***E. Camacho-Ruiz***, *P. Navarro-Torrero, A. Karmakar, C. Fernández-García, E. Tena-Sánchez, F. Potestad-Ordóñez, A. Casado-Galán, P. Ortega-Castro, A. Acosta-Jiménez, C. Jiménez-Fernández, and P. Brox*, "**Cryptographic Security Through a Hardware Root of Trust,**" ARC 2024. Lecture Notes in Computer Science, vol 14553. Springer, Cham.

6. ***E. Camacho-Ruiz***, *S. Sánchez-Solano, M. C. Martínez-Rodríguez, E. Tena-Sanchez and P. Brox* "**Simple Power Analysis of an FPGA implementation of a polynomial multiplier for the NTRU cryptosystem,**" 2023 38th Conference on Design of Circuits and Integrated Systems (DCIS), Málaga, Spain, 2023, pp. 1-6.

7. ***E. Camacho-Ruiz***, *S. Sánchez-Solano, M. C. Martínez-Rodríguez and P. Brox*, "**A complete SHA-3 hardware library based on a high efficiency Keccak design,**" 2023 IEEE Nordic Circuits and Systems Conference (NorCAS), Aalborg, Denmark, 2023, pp. 1-7.

8. ***E. Camacho-Ruiz***, *F. J. Rubio-Barbero, R. Castro-Lopez, E. Roca and F. V. Fernandez*, "**Design considerations for a CMOS 65-nm RTN-based PUF,**" 2023 19th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), Funchal, Portugal, 2023, pp. 1-4.

9. *F. J. Rubio-Barbero*, ***E. Camacho-Ruiz***, *R. Castro-Lopez, E. Roca and F. V. Fernandez*, "**A Peak Detect & Hold circuit to measure and exploit RTN in a 65-nm CMOS PUF,**" 2023 19th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), Funchal, Portugal, 2023, pp. 1-4.

10. ***E. Camacho-Ruiz***, *R. Castro-Lopez, E. Roca and F. V. Fernandez*, "**High-level design of a novel PUF based on RTN,**" 2022 18th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), Villasimius, Italy, 2022, pp. 1-4.

11. ***E. Camacho-Ruiz***, *A. Santana-Andreo, R. Castro-Lopez, E. Roca and F. V. Fernandez*, "**On the use of an RTN simulator to explore the quality trade-offs of a novel RTN-based PUF,**" 2022 18th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), Villasimius, Italy, 2022, pp. 1-4.

12. ***E. Camacho-Ruiz***, *R. Castro-Lopez, E. Roca, P. Brox and F. V. Fernandez*, "**A novel Physical Unclonable Function using RTN,**" 2022 IEEE International Symposium on Circuits and Systems (ISCAS), Austin, TX, USA, 2022, pp. 160-164.

13. *M. C. Martínez-Rodríguez*, ***E. Camacho-Ruiz***, *S. Sánchez-Solano and P. Brox*, "**Design Flow to Evaluate the Performance of Ring Oscillator PUFs on FPGAs,**" 2021 XXXVI Conference on Design of Circuits and Integrated Systems (DCIS), Vila do Conde, Portugal, 2021, pp. 1-6.

14. *P. Saraza-Canflanca, **E. Camacho-Ruiz**, R. Castro-Lopez, E. Roca, J. Martin-Martinez, R. Rodriguez, M. Nafria, and F. V. Fernandez*, "**Simulating the impact of Random Telegraph Noise on integrated circuits,**" SMACD / PRIME 2021; International Conference on SMACD and 16th Conference on PRIME, online, 2021, pp. 1-4.

15. ***E. Camacho-Ruiz**, P. Saraza-Canflanca, R. Castro-Lopez, E. Roca, P. Brox and F. V. Fernandez*, "**Study of SRAM PUFs reliability using the Static Noise Margin,**" SMACD / PRIME 2021; International Conference on SMACD and 16th Conference on PRIME, online, 2021, pp. 1-4.

16. ***E. Camacho-Ruiz**, M. C. Martínez-Rodríguez, S. Sánchez-Solano and P. Brox*, "**Accelerating the Development of NTRU Algorithm on Embedded Systems,**" 2020 XXXV Conference on Design of Circuits and Integrated Systems (DCIS), Segovia, Spain, 2020, pp. 1-6.

## Technical Reports

1. "**Specifications of pilot demonstrators,**" Horizon Europe, QUBIP, Deliverable D2.1, Oct. 2024
2. "**Final VLSI integration of a lightweight RoT,**" Horizon 2020, SPIRS, Deliverable D5.4, Sep. 2024
3. "**Analysis and design of PQ building blocks,**" Horizon Europe, QUBIP, Deliverable D1.4, Aug. 2024
4. "**Dissemination, exploitation and communication plan and activities (initial version),**" Horizon Europe, QUBIP, Deliverable D4.1, Feb. 2024
5. "**Final design of RoT,**" Horizon 2020, SPIRS, Deliverable D2.2, Sep. 2023
6. "**First VLSI integration of a lightweight RoT,**" Horizon 2020, SPIRS, Deliverable D5.2, Mar. 2023
7. "**Initial Design of RoT Components,**" Horizon 2020, SPIRS, Deliverable D2.1, Dic. 2022

## Open-Source Projects

1. "**Public repository: QuantumSakura**" Link
2. "**Public repository: Lib-RoT-SPIRS**" Link
3. "**Public repository: NTRU-Round3 HW**" Link
4. "**Public repository: Demo Kyber**" Link
5. "**Public repository: SHA3+SHAKE HW**" Link
6. "**Public repository: SHA2 HW**" Link
7. "**Public repository: HMAC HW**" Link

## Projects

**Transition to Post-Quantum Cryptography (QUBIP)** Sep. 2023 – Present
*GA NO. 101119746, PC: PhD. Andrea Vesco*
HORIZON EUROPE, EUROPEAN UNION

**Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process (SPIRS)** Sep. 2021 - Sep. 2023
*GA NO. 952622, PC: PhD. Piedad Brox*
H2020, EUROPEAN UNION

**The Variability Challenge in Nano-CMOS: from Device Modeling to IC Design for Mitigation ADN Exploitation (VIGILANT)** Sep. 2020 - Sep. 2023
*PID2019-103869RB-C31, PC: PhD. Rafael Castro*
MINISTRY OF SCIENCE, SPAIN

**Dispositivos Circuitos y Arquitecturas Fiables y de Bajo Consumo para IoT (TOGETHER)** Jun. 2021 - Dic. 2021
*TEC2016-75151-C3-3-R, PC: PhD. Rafael Castro*
MINISTRY OF SCIENCE, SPAIN

**Design of hardware solutions to manage people and things identities with trust, security, and privacy in IoT ecosystem (HW-IDENTIoTY)** Oct. 2019 - Nov. 2019
*TEC2017-83557-R, PC: PhD. Piedad Brox*
MINISTRY OF SCIENCE, SPAIN

**Advancing in cybersecurity technologies (LINKA20216)** Jan. 2020 - Sep. 2020
*CSIC, PC: PhD. Piedad Brox*
CSIC

**Diseño hardware de módulos criptográficos integrables en dispositivos IoT (HW-Crypto Cores)** Sep. 2019 - Nov. 2020
*CSIC, PC: PhD. Piedad Brox*
CSIC

## Supervision Experience

**Leader and Coordinator of Technical Team in the Research Center (IMSE-CSIC)** 2024 - Present
*Instituto de Microelectrónica de Sevilla (IMSE)*

**Leader and Coordinator of Task 2.2 of QUBIP Project** 2023 - Present
*Horizon Europe, QUBIP*

**MsC Thesis: “Security Assessment in the Hardware Implementation of Elliptic Curve Digital Signature Algorithms” – Author: Pablo Navarro Torrero** 2023/2024
*MsC on Microelectronics, Univ. of Seville*

**BsC Thesis: “Diseño de un comparador en tensión para nuevos módulos criptográficos hardware” – Author: Pedro Sánchez Fernández** 2021/2022
*BsC on Physics, Univ. of Seville*

## Reviewer Experience

**Member of the “Technical Program Committee” of ARC 2025** 2025
*ARC 2025, TBD* Seville, Spain

**Technical Consultant of Centro Criptológico Nacional (CCN)** 2024 - Present
*Centro Criptológico Nacional (CCN)* Seville, Spain

**Technical reviewer of ”CHES-2024 Artifact”** 2024
*CHES 2024, 4-7th Sep. 2024* Halifax, Canada

**Journal reviewer of ”Sensors” from MDPI** 2024 - Present

**Member of the “Technical Program Committee” of QSNS 2024** 2024
*QSNS 2024, 26-27th Jun. 2024* Paris, France

**Member of the Working Group Post-Quantum Use In Protocols (PQUIP) of IETF** 2023 - Present
*Internet Engineering Task Force (IETF)*

**Member of the Working Group Limited Additional Mechanisms for PKIX and SMIME (LAMPS) of IETF** 2023 - Present
*Internet Engineering Task Force (IETF)*

## LANGUAGES

**Spanish:** Native

**English:** B2 (certified), C1 (in practice)

**Finnish:** A1 (in practice)

## SKILLS

**Digital HW description languages** : VHDL, Verilog, SystemVerilog
**Analog HW description languages** : Spice, Verilog-A, Verilog-AMS
**SW programming languages** : C, C++, Python, Java
**GPU-Parallelization languages** : CUDA
**Mathematical languages** : Matlab

**Design skills**

- Knowledge of analog, digital and mixed design flows.
- Design and implementation of analog, digital and mixed integrated circuits (ICs).
- Implementation of HW designs in embedded systems (SoCs). Development environment used: Vivado Design Suite, Vitis HLS and ISE.
- Integrated circuit design tools: Cadence and Spectre (simulator).
- Implementation of designs on platforms such as: Arduino and Raspberry Pi.

**Cryptographic skills**

- High degree of knowledge of current symmetric, asymmetric and digital signature cryptographic algorithms.
- High degree of knowledge of post-quantum cryptographic algorithms.
- Knowledge of HW implementation techniques for the acceleration of these algorithms.
- Knowledge of Side-Channel Attacks evaluation and countermeasure design.
- Mastery of the most common HW implementation techniques for PUFs.
- Knowledge of the use of PUFs both key obfuscators and identity generators in cryptographic environments.
- Vulnerability assessment and exploitation environments for host, web and network systems: KaliLinux (and all its tools) and Parrot.

**Other skills**

- Writing scientific articles.
- Technical project writing.
- Strong ability to present scientific content orally.
- Ability to organize and be responsible for the work.
- Motivation for problem solving.
- Great capacity for learning and adaptation.
- High degree of commitment to the work to be performed.
- Office tools: Word, Excel, Powerpoint.