# Eros Camacho Ruiz

*PhD., Hardware Cryptography Researcher*


**Phone Number: +34 691798638**

**Email: eroscamaru@gmail.com / camacho@imse-cnm.csic.es**

**Languages: Spanish (Native) / English (C1)**

**Website: http://www2.imse-cnm.csic.es/~camacho/**


## About Me

I am focusing on the research of hardware implementations of cryptographic techniques. Extensive experience in the study and use of cryptography developed to date (symmetric key, asymmetric key and digital signatures), as well as the new cryptography whose arrival is imminent: post-quantum cryptographic algorithms. I have developed accelerations of these algorithms at both SW and HW levels, adding certain countermeasures against side-channel attacks. On my own, I have studied ethical hacking techniques in order to detect and exploit vulnerabilities in web and communication environments.

## Work Experience

**SEPTEMBER 2023 - PRESENT**

### Technical Researcher in European project - QUBIP

*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC, Spain*

Developing and implementation of PQC algorithm in HW in order to secure IoT devices.

**JUNE 2023 - SEPTEMBER 2023**

### Visiting Researcher

*Tampere University, Finland*

HW implementation of post-quantum algorithms. Specifically, Kyber768 implementations including countermeasures against side-channel attacks.

**DECEMBER 2021 - JUNE 2023**

### FPU Grant

*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC, Spain*

Contract obtained in competitive concurrence at national level. The goal was the design and implementation of a Root-of-Trust (RoT). This RoT will include device identification solutions using PUFs (Physical Unclonable Functions) and PQC algorithm acceleration modules. The ultimate goal was the design and integration of this RoT in the same ASIC.

**SEPTEMBER 2020 - NOVEMBER 2021**

### Technical Researcher

*Instituto de Microelectrónica de Sevilla (IMSE) – CSIC, Spain*

Study of SRAMs as PUFs. A multitude of simulations 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.

**SEPTEMBER 2019 - JANUARY 2020**

### JAE-Intro Intern

*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.

## Education

**2020 – 2024**

**PhD**

### Doctoral Program in Physics Science and Technology

*University of Seville, Spain*

In relation to the knowledge acquired during the development of the dissertation, it is worth highlighting the global knowledge of cryptographic environments and their current implications; the use of these systems in IoT environments, where resources or area are limited for HW solutions; in-depth knowledge of HW implementation techniques of cryptographic solutions for both acceleration and obfuscation and device identification; as well as knowledge of attack techniques and proposed countermeasures.

**2018 – 2020**

**Master's Degree**

### Master of Science Degreee in Microelectronics

*University of Seville, Spain*

Thesis: "Acceleration of Post-Quantum Cryptographic Algorithms Using HW/SW Co-Design Techniques".

**2013 – 2017**

**Bachelor's Degree**

### Bachelor of Science Degree in Physics

*University of Córdoba, Spain*

Thesis: "Implementation of Quantum Monte Carlo Methods in GPU Architectures".

## Journal Publications

1. *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.
2. *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.
3. *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.
4. *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.
5. *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.

## Conference Publications

1. *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.*
2. *E. Camacho-Ruiz, P. Saraza-Canflanca, R. Castro-Lopez, E. Roca, P. Brox and F. V. Fernandez,* ***"A 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.*
3. *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.*

## Conference Publications

4. *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.*
5. *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.*
6. *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.*
7. *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.*
8. *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.*
9. *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.*
10. *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.*
11. *E. Camacho-Ruiz, S. Sánchez-Solano, M. C. Martínez-Rodríguez, E. Tena-Sanchez and P. Brox,* ***"A 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.*

## Projects

**SEPTEMBER 2023 - PRESENT**

### Transition to Post-Quantum Cryptography (QUBIP)

*GA NO. 101119746, PC: PhD. Andrea Vesco*

**HORIZON EUROPE, EUROPEAN UNION**

**SEPTEMBER 2021 - SEPTEMBER 2023**

### Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process (SPIRS)

*GA NO. 952622, PC: PhD. Piedad Brox*

**H2020, EUROPEAN UNION**

**SEPTEMBER 2020 - SEPTEMBER 2023**

### The Variability Challenge in Nano-CMOS: from Device Modeling to IC Design for Mitigation ADN Exploitation (VIGILANT)

*PID2019-103869RB-C31, PC: PhD. Rafael Castro*

**MINISTRY OF SCIENCE, SPAIN**

**JUNE 2021 - DECEMBER 2021**

### Dispositivos Circuitos y Arquitecturas Fiables y de Bajo Consumo para IoT (TOGETHER)

*TEC2016-75151-C3-3-R, PC: PhD. Rafael Castro*

**MINISTRY OF SCIENCE, SPAIN**

## Projects

**OCTOBER 2019 - NOVEMBER 2019**

### Design of hardware solutions to manage people and things identities with trust, security, and privacy in IoT ecosystem (HW-IDENTIoTY)

*TEC2017-83557-R, PC: PhD. Piedad Brox*

**MINISTRY OF SCIENCE, SPAIN**

**JANUARY 2020 - SEPTEMBER 2020**

### Advancing in cybersecurity technologies (LINKA20216)

*CSIC, PC: PhD. Piedad Brox*

**CSIC**

**SEPTEMBER 2019 - NOVEMBER 2020**

### Diseño hardware de módulos criptográficos integrables en dispositivos IoT (HW-Crypto Cores)

*CSIC, PC: PhD. Piedad Brox*

**CSIC**

## 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 in platforms such as: Arduino and Raspberry Pi.
- Cryptography 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 the Side-Channel Attacks evaluation and the design of countermeasures.
  - 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:
  - Capacity for organization and responsibility in the work.
  - Motivation for problem solving.
  - Great learning capacity.
  - High degree of commitment to the work to be performed.
  - Office tools: Word, Excel, PowerPoint.