



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 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.

FORMACIÓN

Doctoral Program in Physics Science and Technology | *Cum-Laude*

"Design of a hardware Root-of-Trust on embedded systems"

Sep. 2020 – Mar. 2024

Univ. of Seville, Spain

MsC on Microelectronics

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

Sep. 2018 – Jul. 2020

Univ. of Seville, Spain

BsC on Physics

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

Sep. 2013 – Jul. 2017

Univ. of Córdoba, Spain

WORK EXPERIENCE

Technical Researcher in European project - QUBIP

Instituto de Microelectrónica de Sevilla (IMSE) – CSIC

Sep. 2023 – Present

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.

Pre-doctoral visiting researcher

Tampere University

Jun. 2023 – Sep. 2023

Finland

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

FPU Grant

Instituto de Microelectrónica de Sevilla (IMSE) – CSIC

Dic. 2021 – Jun. 2023

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.

Technical Researcher in National project

Instituto de Microelectrónica de Sevilla (IMSE) – CSIC

Sep. 2020 – Nov. 2021

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.

IAE-Intro Internship

Instituto de Microelectrónica de Sevilla (IMSE) – CSIC

Sep. 2019 – Jan. 2020
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),”** University of Seville (40 %), CSIC (60 %). PCT Patent PCT/EP2023/057 799, 2023.

JOURNAL PUBLICATIONS

1. **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.
2. **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.
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, 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.
5. **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. **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.
2. **E. Camacho-Ruiz, S. Sánchez-Solano, M. C. Martínez-Rodríguez, E. Tena-Sánchez 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.
3. **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.

4. *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.
5. *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.
6. *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.
7. *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.
8. *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.
9. *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.
10. *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.
11. *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.
12. *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.

OTHER RELEVANT PUBLICATIONS

1. **"Initial Design of RoT Components"** Horizon 2020, SPIRS, Deliverable D2.1, Dic. 2022.
2. **"First VLSI integration of a lightweight RoT"** Horizon 2020, SPIRS, Deliverable D5.2, Mar. 2023.
3. **"Final design of RoT"** Horizon 2020, SPIRS, Deliverable D2.2, Sep. 2023.
4. **"Public repository: Lib-RoT-SPIRS"** [Link](#)
5. **"Public repository: NTRU-Round3 HW"** [Link](#)
6. **"Public repository: Demo Kyber"** [Link](#)
7. **"Public repository: SHA3+SHAKE HW"** [Link](#)
8. **"Public repository: SHA2 HW"** [Link](#)
9. **"Public repository: HMAC HW"** [Link](#)

PROJECTS

Transition to Post-Quantum Cryptography (QUBIP) <i>GA NO. 101119746, PC: PhD. Andrea Vesco</i> HORIZON EUROPE, EUROPEAN UNION	Sep. 2023 – Present
Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process (SPIRS) <i>GA NO. 952622, PC: PhD. Piedad Brox</i> H2020, EUROPEAN UNION	Sep. 2021 - Sep. 2023
The Variability Challenge in Nano-CMOS: from Device Modeling to IC Design for Mitigation ADN Exploitation (VIGILANT) <i>PID2019-103869RB-C31, PC: PhD. Rafael Castro</i> MINISTRY OF SCIENCE, SPAIN	Sep. 2020 - Sep. 2023
Dispositivos Circuitos y Arquitecturas Fiables y de Bajo Consumo para IoT (TOGETHER) <i>TEC2016-75151-C3-3-R, PC: PhD. Rafael Castro</i> MINISTRY OF SCIENCE, SPAIN	Jun. 2021 - Dic. 2021
Design of hardware solutions to manage people and things identities with trust, security, and privacy in IoT ecosystem (HW-IDENTIoT) <i>TEC2017-83557-R, PC: PhD. Piedad Brox</i> MINISTRY OF SCIENCE, SPAIN	Oct. 2019 - Nov. 2019
Advancing in cybersecurity technologies (LINKA20216) <i>CSIC, PC: PhD. Piedad Brox</i> CSIC	Jan. 2020 - Sep. 2020
Diseño hardware de módulos criptográficos integrables en dispositivos IoT (HW-Crypto Cores) <i>CSIC, PC: PhD. Piedad Brox</i> CSIC	Sep. 2019 - Nov. 2020

SUPERVISION EXPERIENCE

MsC Thesis: "Security Assessment in the Hardware Implementation of Elliptic Curve Digital Signature Algorithms" – Author: Pablo Navarro Torero <i>MsC on Microelectronics, Univ. of Seville</i>	2023/2024
BsC Thesis: "Diseño de un comparador en tensión para nuevos módulos criptográficos hardware" – Author: Pedro Sánchez Fernández <i>BsC on Physics, Univ. of Seville</i>	2021/2022

REVIEWER EXPERIENCE

Member of the "Technical Program Committee" of ARC 2025 <i>ARC 2025, TBD</i>	2025 Seville, Spain
Technical reviewer of "CHES-2024 Artifact" <i>CHES 2024, 4-7th Sep. 2024</i>	2024 Halifax, Canada
Journal reviewer of "Sensors" from MDPI	2024 - Present
Member of the "Technical Program Committee" of QSNS 2024 <i>QSNS 2024, 26-27th Jun. 2024</i>	2024 Paris, France

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.