Eros Camacho Ruiz

Dr., Investigador en criptografía hardware

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/

Sobre mí

Me centro en la investigación de implementaciones hardware de técnicas criptográficas. Amplia experiencia en el estudio y uso de la criptografía desarrollada hasta la fecha (clave simétrica, clave asimétrica y firmas digitales), así como de la nueva criptografía cuya llegada es inminente: los algoritmos criptográficos post-cuánticos. He desarrollado aceleraciones de estos algoritmos tanto a nivel SW como HW, añadiendo ciertas contramedidas contra ataques de canal lateral. Por mi cuenta, he estudiado técnicas de hacking ético para detectar y explotar vulnerabilidades en entornos web y de comunicaciones.

Formación

Doctorado en Ciencias y Tecnologías Físicas | ***Sobresaliente Cum-Laude*** — Sep. 2020 – Mar. 2024
"Design of a hardware Root-of-Trust on embedded systems" — Univ. de Sevilla, España

Máster en Microelectrónica — Sep. 2018 – Jul. 2020
TFM: "Aceleración de algoritmos criptográficos post-cuánticos mediante técnicas de co-diseño HW/SW" — Univ. de Sevilla, España

Grado en Física — Sep. 2013 – Jul. 2017
TFG: "Implementación de métodos de Monte Carlo cuántico en arquitecturas GPU" — Univ. de Córdoba, España

Experiencia Laboral

Investigador en Proyecto Europeo – QUBIP — Sep. 2023 – Presente
Instituto de Microelectrónica de Sevilla (IMSE) – CSIC — España

- Líder de la parte técnica asignada a CSIC-IMSE.
- Líder de la Tarea 2.2 del Paquete de Trabajo 2.
- Desarrollo e implementación de algoritmos PQC en HW para asegurar dispositivos IoT en base a Elementos Seguros.

Investigador pre-doctoral visitante — Jun. 2023 – Sep. 2023
Universidad de Tampere — Finlandia

- Implementación en hardware de algoritmos post-cuánticos.
- Implementación de Kyber768 con contramedidas contra ataques de canal lateral.

Contratado FPU — Dic. 2021 – Jun. 2023
Instituto de Microelectrónica de Sevilla (IMSE) – CSIC — España

- Contrato obtenido en concurrencia competitiva a nivel nacional.
- Diseño e implementación de una Root-of-Trust (RoT), incluyendo soluciones de identificación de dispositivos mediante PUFs analógicos y módulos de aceleración de algoritmos PQCs digitales además de otros crypto módulos.

Investigador pre-doctoral en proyecto nacional — Sep. 2020 – Nov. 2021
Instituto de Microelectrónica de Sevilla (IMSE) – CSIC — España

- Estudio de SRAMs como PUFs.
- Análisis de simulaciones donde se evaluó el comportamiento de las SRAMs como PUFs en variabilidad térmica y de envejecimiento.
- Estudio del RTN como variable estocástica en PMOS con el fin de estudiar su estabilidad para permitir el desarrollo de PUFs, al igual que su evaluación con la temperatura.

Becario JAE-Intro Sep. 2019 – Ene. 2020
Instituto de Microelectrónica de Sevilla (IMSE) – CSIC España

- Aceleración de algoritmos PQC mediante técnicas de co-diseño HW/SW sobre SoCs basados en ARM+FPGA de la familia Xilinx Zynq 7000 (PYNQ-Z2).
- Realización de módulos HW dedicados (Verilog/VHDL) para la implementación de la multiplicación polinómica.

PATENTES

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.

PUBLICACIONES EN REVISTAS

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.

PUBLICACIONES EN CONFERENCIAS

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-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.

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.

OTRAS PUBLICACIONES RELEVANTES

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. "**Repositorio público: Lib-RoT-SPIRS**" Enlace
5. "**Repositorio público: NTRU-Round3 HW**" Enlace
6. "**Repositorio público: Demo Kyber**" Enlace
7. "**Repositorio público: SHA3+SHAKE HW**" Enlace
8. "**Repositorio público: SHA2 HW**" Enlace
9. "**Repositorio público: HMAC HW**" Enlace

PROYECTOS

Transition to Post-Quantum Cryptography (QUBIP) — Sep. 2023 – Presente
GA NO. 101119746, IP: Dr. Andrea Vesco
HORIZON EUROPE, UNIÓN EUROPEA

Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process (SPIRS) — Sep. 2021 - Sep. 2023
GA NO. 952622, IP: Dr. Piedad Brox
H2020, UNIÓN EUROPEA

The Variability Challenge in Nano-CMOS: from Device Modeling to IC Design for Mitigation ADN Exploitation (VIGILANT) — Sep. 2020 - Sep. 2023
PID2019-103869RB-C31, IP: Dr. Rafael Castro
MINISTERIO DE CIENCIA, ESPAÑA

Dispositivos Circuitos y Arquitecturas Fiables y de Bajo Consumo para IoT (TOGETHER) — Jun. 2021 - Dic. 2021
TEC2016-75151-C3-3-R, IP: Dr. Rafael Castro
MINISTERIO DE CIENCIA, ESPAÑA

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, IP: Dr. Piedad Brox
MINISTERIO DE CIENCIA, ESPAÑA

Advancing in cybersecurity technologies (LINKA20216) — Ene. 2020 - Sep. 2020
CSIC, IP: Dr. Piedad Brox
CSIC

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

TAREAS DE SUPERVISIÓN

TFM: "Security Assessment in the Hardware Implementation of Elliptic Curve Digital Signature Algorithms" – Autor: Pablo Navarro Torrero — 2023/2024
Máster en Microelectrónica, Univ. de Sevilla

TFG: "Diseño de un comparador en tensión para nuevos módulos criptográficos hardware" – Autor: Pedro Sánchez Fernández — 2021/2022
Grado en Física, Univ. de Sevilla

TAREAS COMO REVISOR

Miembro del "Technical Program Committee" de ARC 2025 — 2025
ARC 2025, TBD — Sevilla, España

Revisor técnico en "CHES-2024 Artifact" — 2024
CHES 2024, 4-7 Sep. 2024 — Halifax, Canada

Revisor de la revista "Sensors" de la Editorial MDPI — 2024 – Presente

Miembro del "Technical Program Committee" de QSNS 2024 — 2024
QSNS 2024, 26-27 Jun. 2024 — Paris, Francia

HABILIDADES

Lenguajes de descripción de HW digital :VHDL, Verilog, SystemVerilog
Lenguajes de descripción de HW analógico :Spice, Verilog-A, Verilog-AMS
Lenguajes de programación SW :C, C++, Python, Java
Lenguajes de paralelización de GPU: CUDA
Lenguajes matemáticos: Matlab

Habilidades de diseño

- Conocimiento de los flujos de diseño analógico, digital y mixto.
- Diseño e implementación de circuitos integrados (CI) analógicos, digitales y mixtos.
- Implementación de diseños HW en sistemas embebidos (SoCs). Entorno de desarrollo utilizado: Vivado Design Suite, Vitis HLS e ISE.
- Herramientas de diseño de circuitos integrados: Cadence y Spectre (simulador).
- Implementación de diseños en plataformas como: Arduino y Raspberry Pi.

Habilidades criptográficas

- Alto grado de conocimiento de los algoritmos criptográficos simétricos, asimétricos y de firma digital actuales.
- Alto grado de conocimiento de algoritmos criptográficos post-cuánticos.
- Conocimiento de las técnicas de implementación HW para la aceleración de estos algoritmos.
- Conocimiento de la evaluación de Side-Channel Attacks y el diseño de contramedidas.
- Dominio de las técnicas de implementación HW más comunes para PUFs.
- Conocimiento del uso de PUFs tanto ofuscadores de claves como generadores de identidades en entornos criptográficos.
- Entornos de evaluación y explotación de vulnerabilidades para sistemas host, web y de red: KaliLinux (y todas sus herramientas) y Parrot.

Otras habilidades

- Redacción de artículos científicos.
- Redacción de proyectos técnicos.
- Gran habilidad de exponer oralmente contenido científico.
- Capacidad de organización y responsabilidad en el trabajo.
- Motivación por la resolución de problemas.
- Gran capacidad de aprendizaje y adaptación.
- Alto grado de compromiso con el trabajo a realizar.
- Manejo de herramientas Office: Word, Excel, Powerpoint.