Eros Camacho Ruiz

Dr., Investigador en criptografía hardware

Número de teléfono: +34 691798638

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

Idiomas: Spanish (Native) / English (C1)

Página web: http://www2.imse-cnm.csic.es/~camacho/

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.

Experiencia Laboral

SEPTIEMBRE 2023 - PRESENTE

Investigador en Proyecto europeo - QUBIP

Instituto de Microelectrónica de Sevilla (IMSE) – CSIC, España

Desarrollo e implementación del algoritmo PQC en HW para asegurar los dispositivos IoT.

JUNIO 2023 - SEPTIEMBRE 2023

Investigador visitante

Universidad de Tampere, Finlandia

Implementación en hardware de algoritmos post-cuánticos. En concreto, implementaciones de Kyber768 que incluyan contramedidas contra ataques de canal lateral.

DICIEMBRE 2021 - JUNIO 2023

Contratado FPU

Instituto de Microelectrónica de Sevilla (IMSE) – CSIC, España

Contrato obtenido en concurrencia competitiva a nivel nacional. El objetivo era el diseño e implementación de una Root-of-Trust (RoT). Esta RoT incluirá soluciones de identificación de dispositivos mediante PUFs (Physical Unclonable Functions) y módulos de aceleración de algoritmos PQC. El objetivo final era el diseño y la integración en un mismo ASIC.

SEPTIEMBRE 2020 - NOVIEMBRE 2021

Investigador en proyecto nacional

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.

SEPTIEMBRE 2019 - ENERO 2020

Becario JAE-Intro

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.

Formación

2020 – 2024

Doctorado

Programa de Doctorado en Ciencias y Tecnologías Físicas

Universidad de Sevilla, España

En relación a los conocimientos adquiridos durante el desarrollo de la tesina, cabe destacar el conocimiento global de los entornos criptográficos y sus implicaciones actuales; el uso de estos sistemas en entornos IoT, donde los recursos o el área son limitados para soluciones HW; el conocimiento en profundidad de las técnicas de implementación HW de soluciones criptográficas tanto para aceleración como para ofuscación e identificación de dispositivos; así como el conocimiento de técnicas de ataque y contramedidas propuestas.

2018 – 2020

Máster

Máster en Microelectrónica

Universidad de Sevilla, España

TFM: "Aceleración de algoritmos criptográficos post-cuánticos mediante técnicas de co-diseño HW/SW".

2013 – 2017

Grado

Grado en Física

Universidad de Córdoba, España

TFG: "Implementación de métodos de Monte Carlo cuántico en arquitecturas GPU".

Publicaciones en revistas

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.

Publicaciones en conferencias

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.*

Publicaciones en conferencias

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.*

Proyectos

SEPTIEMBRE 2023 - PRESENTE

Transition to Post-Quantum Cryptography (QUBIP)

GA NO. 101119746, IP: Dr. Andrea Vesco

HORIZON EUROPE, UNIÓN EUROPEA

SEPTIEMBRE 2021 - SEPTIEMBRE 2023

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

GA NO. 952622, IP: Dr. Piedad Brox

H2020, UNIÓN EUROPEA

SEPTIEMBRE 2020 - SEPTIEMBRE 2023

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

PID2019-103869RB-C31, IP: Dr. Rafael Castro

MINISTERIO DE CIENCIA, ESPAÑA

JUNIO 2021 - DICIEMBRE 2021

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

TEC2016-75151-C3-3-R, IP: Dr. Rafael Castro

MINISTERIO DE CIENCIA, ESPAÑA

Proyectos

OCTUBRE 2019 - NOVIEMBRE 2019

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

TEC2017-83557-R, IP: Dr. Piedad Brox

MINISTERIO DE CIENCIA, ESPAÑA

ENERO 2020 - SEPTIEMBRE 2020

Advancing in cybersecurity technologies (LINKA20216)

CSIC, IP: Dr. Piedad Brox

CSIC

SEPTIEMBRE 2019 - NOVIEMBRE 2020

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

CSIC, IP: Dr. Piedad Brox

CSIC

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:
  - 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.