CV Date	13/04/2026

Part A. PERSONAL INFORMATION

First Name	Erica		
Family Name	Tena Sanchez		
Sex	Female		
Open Researcher and Contributor ID (ORCID)	0000-0002-8905-5715		

A.1. Current position

Job Title	Profesora Titular de Universidad		
Starting date	2025		
Institution	Universidad de Sevilla		
Department / Centre	Tecnología Electrónica		
Country	Spain	Phone Number	
Keywords			

A.3. Education

Degree/Master/PhD	University / Country	Year
CIENCIAS Y TECNOLOGÍAS FÍSICAS	Universidad de Sevilla	2019

Part C. RELEVANT ACCOMPLISHMENTS

C.1. Most important publications in national or international peer-reviewed journals, books and conferences

AC: corresponding author. (nº x / nº y): position / total authors. If applicable, indicate the number of citations

1 **Scientific paper**. Casado-Galán, A; Núñez, J; (3/5) Tena-Sánchez, E; Potestad-Ordóñez, FE; Acosta, AJ. 2026. Assessment of an FPGA Implementation of a Hybrid PUF Based on a Configurable Transient Effect Ring Oscillator and Ring Oscillator (TERORO-PUF). ELECTRONICS. MDPI; MDPI AG. 15-3. ISSN 2079-9292. WOS (0), SCOPUS (0) https://doi.org/10.3390/electronics15030661

2 **Scientific paper**. (1/4) Tena-Sánchez, E (AC); Potestad-Ordóñez, FE; Zúñiga-González, V; Acosta, AJ. 2025. Low-Cost Full Correlated-Power-Noise Generator to Counteract Side-Channel Attacks. APPLIED SCIENCES-BASEL. MDPI; MDPI AG. 15-6. ISSN 2076-3417. WOS (1), SCOPUS (2) https://doi.org/10.3390/app15063064

3 **Scientific paper**. Casado-Galán, Alejandro; Sanchez-Solano, Santiago; (3/7) Tena-Sanchez, Erica; Rojas-Muñoz, Luis F.; Potestad-Ordóñez, Francisco Eugenio; Martínez-Rodríguez, Macarena C.; Acosta-Jiménez, Antonio J.2025. Analysis of EM Side-Channel Leakage on an RO-PUF and Proposed Countermeasures. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. IEEE COMPUTER SOC. ISSN 1545-5971, ISSN 1941-0018. SCOPUS (1) https://doi.org/10.1109/TDSC.2025.3648516

4 **Scientific paper**. Martín-González, M; (2/4) Tena-Sánchez, E; Potestad-Ordóñez, FE; Acosta, AJ. 2025. Detailed Assessment of Hardware Implementations, Attacks and Countermeasures for the Ascon Authenticated Cipher. ELECTRONICS LETTERS. INST ENGINEERING TECHNOLOGY-IET; WILEY. 61-1. ISSN 0013-5194, ISSN 1350-911X. WOS (1), SCOPUS (2) https://doi.org/10.1049/ell2.70260

5 **Scientific paper**. Potestad-Ordóñez, Francisco Eugenio; Casado-Galán, Alejandro; (3/3) Tena-Sánchez, Erica. 2024. Protecting FPGA-Based Cryptohardware Implementations from Fault Attacks Using ADCs. SENSORS. MDPI; MDPI AG. 24-5. ISSN 1424-8220. WOS (6), SCOPUS (8) https://doi.org/10.3390/s24051598

6 **Scientific paper**. Potestad-Ordóñez, F.E.; (2/5) Tena-Sánchez, Erica; Acosta-Jiménez, A.J.; Jiménez-Fernández, C.J.; Chaves, R.2022. Design and evaluation of countermeasures against fault injection attacks and power side-channel leakage exploration for AES block cipher. IEEE ACCESS. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC; Institute of Electrical and Electronics Engineers (IEEE). 10, pp.65548-65561. ISSN 2169-3536, ISSN 2169-3536. WOS (9), SCOPUS (12) https://doi.org/10.1109/ACCESS.2022.3183764

7 **Scientific paper**. Delgado-Lozano, Ignacio M.; (2/4) Tena-Sánchez, Erica; Núñez, Juan; Acosta, Antonio J.2022. Gate-level design methodology for side-channel resistant logic styles using TFETs. IEEE Embedded Systems Letters. 14-2, pp.99-102. ISSN 1943-0663, ISSN 1943-0671. WOS (3), SCOPUS (3) https://doi.org/10.1109/LES.2021.3122395

8 **Scientific paper**. (1/5) Tena-Sánchez, Erica (AC); Potestad-Ordóñez, Francisco E.; Jiménez-Fernández, Carlos J.; Acosta, Antonio J.; Chaves, Ricardo. 2022. Gate-level hardware countermeasure comparison against power analysis attacks. APPLIED SCIENCES-BASEL. MDPI; MDPI AG. 12-5. ISSN 2076-3417. WOS (8), SCOPUS (12) https://doi.org/10.3390/app12052390

9 **Scientific paper**. Potestad-Ordóñez, Francisco E.; (2/5) Tena-Sánchez, Erica; Acosta-Jiménez, Antonio José; Jiménez-Fernández, Carlos Jesús; Chaves, Ricardo. 2022. Hardware countermeasures benchmarking against fault attacks. APPLIED SCIENCES-BASEL. MDPI; MDPI AG. 12-5. ISSN 2076-3417. WOS (10), SCOPUS (13) https://doi.org/10.3390/app12052443

10 **Scientific paper**. Potestad-Ordóñez, Francisco E.; (2/5) Tena-Sánchez, Erica; Mora-Gutiérrez, J. M.; Valencia-Barrero, M.; Jiménez-Fernández, C. J.2021. Trivium stream cipher countermeasures against fault injection attacks and DFA. IEEE ACCESS. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC; Institute of Electrical and Electronics Engineers (IEEE). 9, pp.168444-168454. ISSN 2169-3536, ISSN 2169-3536. WOS (2), SCOPUS (5) https://doi.org/10.1109/ACCESS.2021.3136609

11 **Scientific paper**. Delgado-Lozano, Ignacio M.; (2/4) Tena-Sánchez, Erica; Núñez, Juan; Acosta, Antonio J.2021. Design and analysis of secure emerging crypto-hardware using HyperFET devices. IEEE Transactions on Emerging Topics in Computing. Institute of Electrical and Electronics Engineers; IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. 9-2, pp.787-796. ISSN 2376-4562, ISSN 2168-6750. WOS (5), SCOPUS (7) https://doi.org/10.1109/tetc.2020.2977735

12 **Scientific paper**. Potestad-Ordóñez, Francisco E.; (2/5) Tena-Sánchez, Erica; Mora-Gutiérrez, José Miguel; Valencia-Barrero, Manuel; Jiménez-Fernández, Carlos Jesús. 2021. Experimental FIA methodology using clock and control signal modifications under power supply and temperature variations. SENSORS. MDPI; MDPI AG. 21-22. ISSN 1424-8220. WOS (0), SCOPUS (0) https://doi.org/10.3390/s21227596

13 **Scientific paper**. Delgado-Lozano, I. M.; (2/4) Tena-Sánchez, Erica; Núñez, J.; Acosta, A. J.2020. Projection of dual-rail dpa countermeasures in future finfet and emerging tfet technologies. ACM Journal on Emerging Technologies in Computing Systems. 16-3. ISSN 1550-4832, ISSN 1550-4840. WOS (4), SCOPUS (7) https://doi.org/10.1145/3381857

14 **Scientific paper**. (1/2) Tena-Sánchez, Erica (AC); Acosta, Antonio J.2019. Logic minimization and wide fan-in issues in DPL-based cryptocircuits against power analysis attacks. INTERNATIONAL JOURNAL OF CIRCUIT THEORY AND APPLICATIONS. WILEY. 47-2, pp.238-253. ISSN 0098-9886, ISSN 1097-007X. WOS (3), SCOPUS (5) https://doi.org/10.1002/cta.2587

15 **Scientific paper**. Acosta, Antonio J.; Addabbo, Tommaso; (3/3) Tena-Sánchez, Erica. 2017. Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. INTERNATIONAL JOURNAL OF CIRCUIT THEORY AND APPLICATIONS. WILEY. 45-2, pp.145-169. ISSN 0098-9886, ISSN 1097-007X. WOS (33), SCOPUS (37) https://doi.org/10.1002/cta.2296

16 **Scientific paper**. Acosta Jiménez, Antonio J.; (2/4) Tena Sánchez, Erica; Jiménez Fernández, Carlos Jesús; Mora, José M.2017. Power and energy issues on lightweight cryptography. JOURNAL OF LOW POWER ELECTRONICS. AMER SCIENTIFIC PUBLISHERS. 13-3, pp.326-337. ISSN 1546-1998, ISSN 1546-2005. WOS (0), SCOPUS (3) https://doi.org/10.1166/jolpe.2017.1490

17 **Scientific paper**. Brox, Piedad; Martínez-Rodríguez, Macarena C.; (3/5) Tena-Sánchez, Erica; Baturone, Iluminada; Acosta, Antonio J.2016. Application specific integrated circuit solution for multi-input multi-output piecewise-affine functions. INTERNATIONAL JOURNAL OF CIRCUIT THEORY AND APPLICATIONS. WILEY. 44-1, pp.4-20. ISSN 0098-9886, ISSN 1097-007X. WOS (5), SCOPUS (5) https://doi.org/10.1002/cta.2058

18 **Scientific paper**. (1/3) Tena-Sánchez, Erica (AC); Castro, Javier; Acosta, Antonio J.2014. A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits. IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC. 4-2, pp.203-215. ISSN 2156-3357, ISSN 2156-3365. WOS (25), SCOPUS (27) https://doi.org/10.1109/JETCAS.2014.2315878

19 **Scientific paper**. Brox Jiménez, Piedad; Castro Ramírez, Javier; Martínez-Rodríguez, Macarena C.; (4/7) Tena Sánchez, Erica; Jiménez Fernández, Carlos Jesús; Baturone, Iluminada; Acosta, Antonio J.2013. A programmable and configurable ASIC to generate piecewise-affine functions defined over general partitions. IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS I-REGULAR PAPERS. IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC; Institute of Electrical and Electronics Engineers (IEEE). 60-12, pp.3182-3194. ISSN 1549-8328, ISSN 1558-0806. WOS (8), SCOPUS (10) https://doi.org/10.1109/TCSI.2013.2265962

C.2. Conferences and meetings

1 Casado-Galan, A.; Nunez-Martinez, J.; Tena-Sanchez, E.; Potestad-Ordonez, F. E.; Acosta, A. J.. TERORO - Transient Effect Ring Oscillator and Ring Oscillator Configurable Hybrid PUF. Conference.

2 Potestad-Ordonez, F. E.; Tena-Sanchez, E.; Zuniga-Gonzalez, V.; Acosta, A. J.. Design and Evaluation of Combined Hardware FIA and SCA Countermeasures for AES Cipher. Conference.

3 Casado-Galan, A.; Potestad-Ordonez, F. E.; Acosta, A. J.; Tena-Sanchez, E.. Electromagnetic Fault Injection Attack Methodology against AES Hardware Implementation. Conference.

4 Martin-Gonzalez, Miguel; Tena-Sanchez, Erica; Ordonez, F. Eugenio Potestad; Acosta, Antonio J.. Hardware implementations, SCA/FIA attacks, and countermeasures for the ASCON AEAD cipher: A review. Conference.

5 Zuñiga Gonzalez, Virginia; Tena-Sanchez, Erica; Acosta, Antonio J.. A Security Comparison between AES-128 and AES-256 FPGA implementations against DPA attacks. Conference.

6 Camacho-Ruiz, Eros; Sanchez-Solano, Santiago; Martinez-Rodriguez, Macarena C.; Tena-Sanchez, Erica; Brox, Piedad. A Simple Power Analysis of an FPGA implementation of a polynomial multiplier for the NTRU cryptosystem. Conference.

7 Tena Sánchez, Erica; Casado Galán, Alejandro; Zúñiga González, Virginia; Potestad Ordóñez, Francisco Eugenio; Acosta Jiménez, Antonio José. Automated experimental setup for EM cartography to enhance EM attacks. Conference.

8 Jimenéz-Fernández, Carlos Jesús; Baena Oliva, Carmen; Parra Fernández, Pilar; Valencia Barrero, Manuel; Potestad Ordóñez, Francisco Eugenio; Tena Sánchez, Erica; Gallardo Soto, Alejandro. Teaching based on proposed by students designs: a case study. Conference.

9 Tena-Sánchez, E.; Delgado-Lozano, I. M.; Núñez, J.; Acosta, A. J.. Benchmarking of nanometer technologies for DPA-resilient DPL-based cryptocircuits. Conference.

10 Tena-Sánchez, Erica; Acosta, Antonio J.. Optimized DPA attack on Trivium stream cipher using correlation shape distinguishers. Conference.

11 Martinez-Rodriguez, MC; Brox, P; Tena, E; Acosta, AJ; Baturone, I. Programmable ASICs for Model Predictive Control. Conference.

12 Tena-Sánchez, Erica; Castro, Javier; Acosta, Antonio J.. Low-Power Differential Logic Gates for DPA Resistant Circuits. Conference.
13 Martinez-Rodriguez, MC; Brox, P; Castro, J; Tena Sánchez, Erica; Acosta, AJ; Baturone, I. ASIC-in-the-loop methodology for verification of piecewise affine controllers. Conference.
14 Eiroa, S; Castro, J; Martinez-Rodriguez, MC; Tena Sánchez, Erica; Brox, P; Baturone, I. Reducing bit flipping problems in SRAM physical unclonable functions for chip identification. Conference.

C.3. Research projects and contracts

1 **Project**. PID2024-158044OB-I00, Diseño basado en inteligencia artificial de circuitos criptográficos seguros y sostenibles. Ministerio de Ciencia, Innovación y Universidades. Tena Sánchez, Erica. 01/09/2025-31/08/2028. 222.612,5 €.
2 **Project**. TSI-069100-2023-001, USECHIP: Cátedra en Microelectrónica de la Universidad de Sevilla. Ministerio de Asuntos Económicos y Transformación Digital. Acosta Jiménez, Antonio José. 19/06/2024-19/06/2027. 4.200.000 €.
3 **Project**. PID2020-116664RB-I00, Diseño, implementación y validación en hardware de una raíz de confianza resistente a ataques, para sistemas empotrados seguros. Ministerio de Ciencia e Innovación. Jiménez Fernández, Carlos Jesús. 01/09/2021-31/08/2025. 146.410 €.
4 **Project**. GA-952622, Secure Platform for ICT Systems Rooted at the Silicon Manufacturin Process" - (SPIRS). Comisión Europea. Jiménez Fernández, Carlos Jesús. 01/10/2021-30/09/2024. 61.991,61 €.
5 **Project**. US-1380823, SCARoT: Side-Channel Attacks on Root of Trust / Ataques laterales sobre la Raíz de Confianza. Consejería de Economía, Conocimiento, Empresas y Universidad. Acosta Jiménez, Antonio José. 01/01/2022-31/05/2023. 90.000 €.
6 **Project**. TEC2016-80549-R, Integración y Validación en Laboratorio de Contramedidas Frente a Ataques Laterales en Criptocircuitos Microelectrónicos. Ministerio de Economía y Competitividad. Acosta Jiménez, Antonio José. 30/12/2016-29/12/2019. 104.544 €.
7 **Project**. TEC2013-45523-R, Cesar: Circuitos Microelectrónicos Seguros Frente a Ataques Laterales. Ministerio de Economía y Competitividad. Acosta Jiménez, Antonio José. 01/01/2014-30/09/2017. 144.474 €.
8 **Project**. TEC2010-16870, Circuitos Integrados para Transmisión de Información Especialmente Segura. Ministerio de Ciencia e Innovación. Jiménez Fernández, Carlos Jesús. 01/01/2011-30/09/2014. 106.722 €.
9 **Contract**. RISCCOM_DEKRA-USE DEKRA Testing and Certification, S.A.U.. Tena Sánchez, Erica. 01/01/2024-01/01/2026. 145.200 €.