RED2018-102384-T

Digital and Mixed-Signal Integrated Circuits

IMSE-CNM (CSIC)

A. J. Acosta, R. Arjona, M. C. Baena, A. Barriga, I. Baturone, P. Brox, C. J. Jiménez,
M. C. Martínez-Rodríguez, J. M. Mora, P. Parra, **S. Sánchez-Solano**, M. Valencia

Contact: santiago@imse-cnm.csic.es

IMSE Research Activities

The area of specialization of IMSE is the design of CMOS analog and mixed-signal integrated circuits and their use in different application contexts such as radiofrequency, data conversion or cybersecurity.

IMSE Research Infrastructure

IMSE has CAD tools to cover all stages of the design flow for circuits and systems designs, as well as laboratories for logical, electrical, functional and thermal characterization of mixed signal ICs, and RF, optoelectronic and cryptographic devices.

Group Profile

Recent / Ongoing Results

Research

- **CMOS Digital Integrated Circuits**
- **Digital Embedded Systems**
- **Microelectronic Systems for Computational Intelligence**
- **Microelectronics for Security**
  - PUF- and TRNG-based Roots-of-Trust
  - Biometric & Cryptographic algorithms
  - Side-Channel & Fault-injection Attacks
  - Countermeasure Design

- **CRYPTOHARDWEAR (FEDER-US-1265146):** *Hardware solutions to face the new cryptographic challenges of wearable devices.*
- **HW-IDENTIoTY (TEC2017-83557-R)**: *Design of hardware solutions to manage people and things identities with trust, security, and privacy in IoT ecosystem.*
- **INTERVALO (TEC2016-80549-R):** *Integration and laboratory validation of side channel attacks countermeasures in microelectronics cryptocircuits.*
- **ID-EO (TEC2014-57971-R):** *Design of crypto-biometric hardware for video encryption and authentication.*
- **(LINKA20216):** *Advancing in cybersecurity technologies.*

Training/Teaching

- **Physics and Computer Science Degrees at US** [1]
- **Master in Microelectronics: Design and Applications of Micro/Nanoscale Systems** [2]
- **Postgraduate Courses at CUJAE, La Habana (Cuba)** [3]

- **Digital Systems Design** [1]
  - *USERV: rv32i processor with Harvard architecture and five-stage pipeline*
- **Applications, Systems and Techniques for Information Processing** [2]
  - *ASTIRV: rv32i core with Von Neumann architecture, without pipeline*
- **Neuromorphic and Fuzzy Systems: Applications and Case Studies** [2]
- **Development of Embedded Systems on Reconfigurable Hardware** [3]

Innovation

- **RTC Projects**
- **Transfer Actions**
- **Industrial Contracts**
- **Patents**
- **EBTs**

- **HARDBLOCK (RTC-2017-6595-7):** *Hardware-based security for blockchain technologies.*
- **(FEDER-US-5926):** *Transferencia de conocimiento y de tecnología microelectrónica sobre cripto-biometría multi-modal.*
- **EP19382623:** *A behavioral and physical unclonable function and a multi-modal cryptographic authentication method using the same.*

Group positioning & Perspectives in front of Open-Hw & RISC-V

R+D+i+T

- **Xfuzzy: Fuzzy Logic Design Tools: http://www.imse-cnm.csic.es/Xfuzzy/**
- **SHORES (Software & Hardware Open Repository for Embedded Systems): http://www.imse-cnm.csic.es/shores/**
- **Introduction of RISC-V in the curricula of some undergraduate and graduate courses.**
- **Development of TFMs & TFGs on RISC-V implementations.**
- **H2020 proposal for improving security and data-privacy in RISC-V based ICT systems for IoT applications.**

Global Remarks

“Strengthening security in the RISC-V ecosystem is a fundamental aspect to guarantee its growth and promote its application in many different sectors”

“This issue has led to the establishment of the RISC-V Security Standing Committee of the RISC-V Foundation and the participation in said organization of different institutions and companies in the security sector”