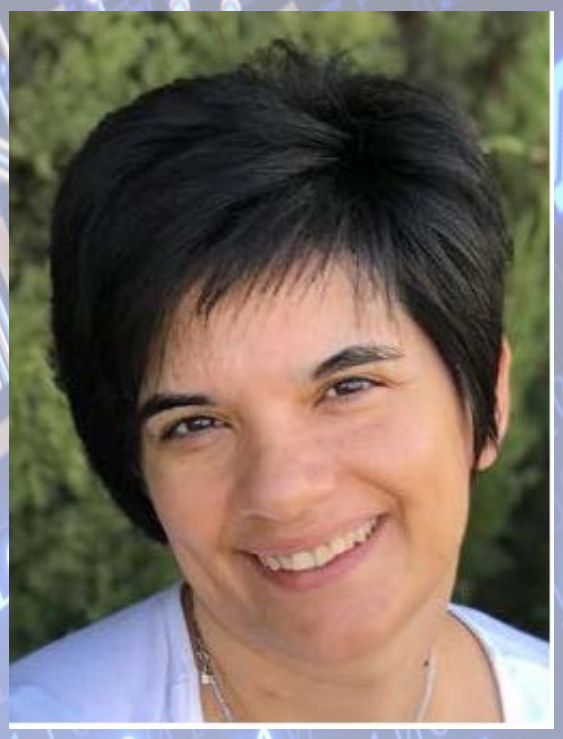
HARDWARE ABIERTO PARA LA PROTECCIÓN DE PROCESADORES EMPOTRADOS



23/04

11:30h

AULA P9. AULARIO AVERROES (CAMPUS DE RABANALES)

Evento sobre Criptografía organizado por el Programa de Doctorado en COMPUTACIÓN AVANZADA, ENERGÍA Y PLASMAS

Los procesadores empotrados pueden protegerse derivando la confianza mediante una Root-of-Trust (RoT). Una RoT en hardware utiliza, como secreto del dispositivo, un identificador digital derivado del hardware. Esto podría implementarse utilizando una función física no clonable (Physical Unclonable Function o PUF) que explota las pequeñas variaciones en los procesos de fabricación del silicio de los circuitos semiconductores. Ni el diseñador de la PUF ni el fabricante del chip conocen estas claves secretas. Otros componentes habituales de la RoT son una fuente de entropía y funciones criptográficas para implementar algoritmos de cifrado/descifrado y firmas digitales. La combinación de estos componentes puede proporcionar un conjunto completo de servicios de seguridad para un sistema empotrado: autenticación de dispositivos, generación en línea de claves criptográficas fiables, arranque seguro habilitado por hardware y protocolos de seguridad. Se describirán algunos ejemplos ilustrativos de un hw RoT para un procesador RISC-V. Este trabajo ha contado con el apoyo de los proyectos financiados por la UE SPIRS (GA 952622), GOIT (GA 101070660) y QUBIP (GA 101119746)

PIEDAD BROX es Científica Titular en el Instituto de Microelectrónica de Sevilla, centro mixto CSIC/Univ. de Sevilla. Actualmente, coordina varios proyectos en el ámbito de la seguridad con el diseño hardware de Funciones PUF, funciones hash, así como aceleradores hardware para esquemas clásicos de clave pública (RSA, ECC) y Criptografía Post-Cuántica (PQC)

UNIVERSIDAD DE CÓRDOBA

ESCUELA POLITÉCNICA SUPERIOR DE CÓRDOBA
Universidad de Córdoba

idep Instituto de Estudios de Postgrado

IMSE-cnm Instituto de Microelectrónica de Sevilla

CSIC

Contacto: María Brox (mbrox@uco.es), Aurora Gil de Castro (agil@uco.es), Eduardo Cañete Carmona (ecanete@uco.es)