1. Record Nr. UNINA9910299845903321

Titolo	Trusted Computing for Embedded Systems / / edited by Bernard Candaele, Dimitrios Soudris, Iraklis Anagnostopoulos
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-09420-3
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (315 p.)
Disciplina	004.1 005.8 620 621.381 621.3815
Soggetti	Electronic circuits Microprocessors Electronics Microelectronics Computer security Circuits and Systems Processor Architectures Electronics and Microelectronics, Instrumentation Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Part I Introduction -- Programming Interfaces for the TPM -- Part II Application-Use cases -- Chapter 2: ARM TrustZone -- Computer Security Anchors in Smart Grids: The Smart Metering Scenario and Challenges -- Authentication and mutual authentication -- Low power Wireless Sensor Networks: Secure applications and remote distribution of FW updates with key management on WSN -- Part III Building blocks -- Physically Unclonable Function: Principle, design and characterization of the Loop PUF -- Physically Unclonable Function:

Design of a silicon arbiter-PUF on CMOS 65 nm -- Secure Key Generator using a Loop-PUF -- Fault Sensitivity Analysis at Design Time -- Information Theoretic Comparison of Side-channel Distinguishers -- Part III Advanced Galileo Positioning technologies -- Wireless Sensor Networks: Routing protocol for critical infrastructure protection -- Wireless Sensor Networks: Virtual platform for performance analysis and attack simulation -- Heap management for trusted operating environments -- IP-XACT extensions for cryptographic IP.

Sommario/riassunto

This book describes the state-of-the-art in trusted computing for embedded systems. It shows how a variety of security and trusted computing problems are addressed currently and what solutions are expected to emerge in the coming years. The discussion focuses on attacks aimed at hardware and software for embedded systems, and the authors describe specific solutions to create security features. Case studies are used to present new techniques designed as industrial security solutions. Coverage includes development of tamper resistant hardware and firmware mechanisms for lightweight embedded devices, as well as those serving as security anchors for embedded platforms required by applications such as smart power grids, smart networked and home appliances, environmental and infrastructure sensor networks, etc. · Enables readers to address a variety of security threats to embedded hardware and software; · Describes design of secure wireless sensor networks, to address secure authentication of trusted portable devices for embedded systems; · Presents secure solutions for the design of smart-grid applications and their deployment in large-scale networked and systems. .