1. Record Nr. UNINA9910473459903321

Autore	Avoine Gildas
Titolo	Security of Ubiquitous Computing Systems : Selected Topics / / edited by Gildas Avoine, Julio Hernandez-Castro
Pubbl/distr/stampa	Springer Nature, 2021 Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-10591-1
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XVIII, 265 p. 25 illus., 8 illus. in color.)
Classificazione	COM000000COM053000TEC007000TEC009000
Disciplina	005.8 004
Soggetti	Computer security Computer engineering Internet of things Embedded computer systems Computer software System safety Systems and Data Security Cyber-physical systems, IoT Professional Computing Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I: Introduction -- Emerging Security Challenges for Ubiquitous Devices -- Part II: Lightweight Cryptographic Primitives -- Catalog and Illustrative Examples of Lightweight Cryptographic Primitives -- Selected Design and Analysis Techniques in Contemporary Symmetric Encryption -- An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families -- Part III: Authentication Protocols -- ePassport and eID Technologies -- Ultra-lightweight Authentication -- From Relay Attacks to Distance-Bounding Protocols -- Part IV: Hardware Implementation and Systems -- It Started With Templates: The Future of Profiling in Side-Channel Analysis -- Side Channel Attack

	Assessment Platforms and Tools for Ubiquitous Systems -- Challenges in Certifying Small-scale (IoT) Hardware Random Number Generators -- Finding Software Bugs in Embedded Devices -- Part V: Privacy and Forensics -- Privacy-Oriented Analysis of Ubiquitous Computing Systems: A 5-D Approach -- IoT Forensics.
Sommario/riassunto	The chapters in this open access book arise out of the EU Cost Action project Cryptacus, the objective of which was to improve and adapt existent cryptanalysis methodologies and tools to the ubiquitous computing framework. The cryptanalysis implemented lies along four axes: cryptographic models, cryptanalysis of building blocks, hardware and software security engineering, and security assessment of real-world systems. The authors are top-class researchers in security and cryptography, and the contributions are of value to researchers and practitioners in these domains. This book is open access under a CC BY license.