

1. Record Nr.	UNINA9910484220403321
Titolo	Innovative Security Solutions for Information Technology and Communications : 9th International Conference, SECITC 2016, Bucharest, Romania, June 9-10, 2016, Revised Selected Papers // edited by Ion Bica, Reza Reyhanitabar
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-47238-0
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (X, 287 p. 86 illus.)
Collana	Security and Cryptology ; ; 10006
Disciplina	005.8
Soggetti	Computer security Information storage and retrieval Application software Data encryption (Computer science) Computer communication systems Management information systems Computer science Systems and Data Security Information Storage and Retrieval Information Systems Applications (incl. Internet) Cryptology Computer Communication Networks Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Circular Security Reconsidered -- Visual Cryptography: Models, Issues, Applications and New Directions -- Paper Tigers: An Endless Fight -- Security of Identity-based Encryption Schemes from Quadratic Residues -- Long-Term Secure One-Round Group Key Establishment from Multilinear Mappings -- RSA Weak Public Keys Available on the Internet -- A Tweak for a PRF Mode of a Compression Function and Its Applications -- May-Ozerov Algorithm for Nearest-Neighbor Problem

over \mathbb{F}_q and Its Application to Information Set Decoding -- A Cryptographic Approach for Implementing Semantic Web's Trust Layer -- Schnorr-like Identification Scheme Resistant to Malicious Subliminal Setting of Ephemeral Secret -- Homomorphic Encryption Based On Group Algebras and Goldwasser-Micali Scheme -- Increasing the Robustness of the Montgomery kP-Algorithm against SCA by Modifying its Initialization -- When Pythons Bite -- Secure Virtual Machine for Real Time Forensic Tools on Commodity Workstations -- Pushing the Optimization Limits of Ring Oscillator-based True Random Number Generators -- TOR - Didactic Pluggable Transport -- Preparation of SCA Attacks: Successfully Decapsulating BGA Packages -- Comparative Analysis of Security Operations Center Architectures; Proposals and Architectural Considerations for Frameworks and Operating Models -- Secure Transaction Authentication Protocol -- Proposed Scheme for Data Confidentiality and Access Control in Cloud Computing. .

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 9th International Conference on Security for Information Technology and Communications, SECITC 2016, held in Bucharest, Romania, in June 2016. The 16 revised full papers were carefully reviewed and selected from 35 submissions. In addition with 4 invited talks the papers cover topics such as Cryptographic Algorithms and Protocols, and Security Technologies for ITC.
