

1. Record Nr.	UNISA996465338903316
Titolo	Innovative Security Solutions for Information Technology and Communications [[electronic resource]] : 10th International Conference, SecITC 2017, Bucharest, Romania, June 8–9, 2017, Revised Selected Papers // edited by Pooya Farshim, Emil Simion
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-69284-4
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XII, 201 p. 35 illus.)
Collana	Security and Cryptology ; ; 10543
Disciplina	005.8
Soggetti	Computer security Data structures (Computer science) Computer communication systems Architecture, Computer Special purpose computers Computer science—Mathematics Systems and Data Security Data Structures and Information Theory Computer Communication Networks Computer System Implementation Special Purpose and Application-Based Systems Mathematics of Computing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Faster Zero-Knowledge Protocols and Applications -- Stochastic Side-Channel Leakage Analysis via Orthonormal Decomposition -- Key-policy Attribute-based Encryption from Bilinear Maps -- Security of Pseudo-Random Number Generators with Input -- Securing the Foundations of Democracy -- Exploring Naccache-Stern Knapsack Encryption -- Proximity Assurances Based on Natural and Artificial Ambient Environments -- Challenges of Federating National Data Access Infrastructures -- Strongly Deniable Identification Schemes

Immune to Prover's and Verifier's Ephemeral Leakage -- Evolution of the McEliece Public Key Encryption Scheme -- New Algorithm for Modeling S-box in MILP Based Differential and Division Trail Search -- Secretly Embedding Trapdoors into Contract Signing Protocols -- On A Key Exchange Protocol. .

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Conference on Security for Information Technology and Communications, SecITC 2017, held in Bucharest, Romania, in June 2017. The 6 revised full papers presented together with 7 invited talks were carefully reviewed and selected from 22 submissions. The papers present advances in the theory, design, implementation, analysis, verification, or evaluation of secure systems and algorithms.
