1. Record Nr. UNISA996466357003316

Titolo	Cryptography and Information Security in the Balkans [[electronic resource]] : Second International Conference, BalkanCryptSec 2015, Koper, Slovenia, September 3-4, 2015, Revised Selected Papers / / edited by Enes Pasalic, Lars R. Knudsen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-29172-6
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (VIII, 207 p. 19 illus.)
Collana	Security and Cryptology ; ; 9540
Disciplina	652.8
Soggetti	Data encryption (Computer science) Computer security Cryptology Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Symmetric key cryptography -- Boolean Functions with Maximum Algebraic Immunity Based on Properties of Punctured Reed-Muller Codes -- Results on characterizations of vectorial Bent and Plateaued Functions in arbitrary characteristic p -- Cryptographically Strong S-boxes Generated by Modified Immune Algorithm -- Cryptanalysis -- Analysis of the Authenticated Cipher MORUS -- Linear Cryptanalysis and Modified DES with Embedded Parity Check in the S-boxes -- Time-Success Ratios under Simple Transformations: Analysis and Applications -- Security and protocols -- Synchronous Universally Composable Computer Networks -- Key-policy Attribute-based Encryption for General Boolean Circuits from Secret Sharing and Multi-linear Maps -- Closing the Gap: A Universal Privacy Framework for Outsourced Data -- Implementation and verifiable encryption -- On the Efficient Arithmetic for Lattice-Based Cryptography on GPU Using the CUDA Platform -- cuHE: A Homomorphic Encryption Accelerator Library -- Extended Functionality in Verifiable Searchable Encryption.
Sommario/riassunto	This book contains revised selected papers from the Second International Conference on Cryptology and Information Security in the

Balkans, BalkanCryptSec 2015, held in Koper, Slovenia, in September 2015. The 12 papers presented in this volume were carefully reviewed and selected from 27 submissions. They are organized in topical sections named: symmetric key cryptography; cryptanalysis; security and protocols; and implementation and verifiable encryption.