

1. Record Nr.	UNISA996466002103316
Titolo	Selected Areas in Cryptography - SAC 2015 [[electronic resource]] : 22nd International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers // edited by Orr Dunkelman, Liam Keliher
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
ISBN	3-319-31301-0
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XIX, 528 p. 117 illus.)
Collana	Security and Cryptology ; ; 9566
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Algorithms Coding theory Information theory Computer science—Mathematics Cryptology Systems and Data Security Algorithm Analysis and Problem Complexity Coding and Information Theory Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Sommario/riassunto	This book contains revised selected papers from the 22nd International Conference on Selected Areas in Cryptography, SAC 2015, held in Sackville, NB, Canada in August 2015. The 26 full papers and 3 short papers presented in this volume were carefully reviewed and selected from 91 submissions. They are organized in topical sections named: privacy enhancing technologies; cryptanalysis of symmetric-key primitives; implementation of cryptographic schemes; short papers; privacy preserving data processing; side channel attacks and defenses;

new cryptographic constructions; authenticated encryption; on the hardness of mathematical problems; and cryptanalysis of authenticated encryption schemes.
