

1. Record Nr.	UNISA996465866503316
Titolo	Fast Software Encryption [[electronic resource]] : 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers // edited by Anne Canteaut
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-34047-4
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XII, 463 p. 82 illus.)
Collana	Security and Cryptology ; ; 7549
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Algorithms Management information systems Computer science Computer security Computer science—Mathematics Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Systems and Data Security Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and author index.
Nota di contenuto	Block ciphers -- Differential cryptanalysis -- Hash functions -- Modes of operation -- New tools for cryptanalysis -- New designs -- Keccak.
Sommario/riassunto	This book constitutes the thoroughly refereed post-conference proceedings of the 19th International Workshop on Fast Software Encryption, held in Washington, DC, USA, in March 2012. The 24 revised full papers presented together with 1 invited talk were carefully reviewed and selected from 89 initial submissions. The papers are organized in topical sections on block ciphers, differential

cryptanalysis, hash functions, modes of operation, new tools for
cryptanalysis, new designs and Keccak.
