1. Record Nr. UNISA996465967803316

Titolo	Fast Software Encryption [[electronic resource]] : 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers / / edited by Thomas Peyrin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2016
ISBN	3-662-52993-9
Edizione	[1st ed. 2016.]
Descrizione fisica	1 online resource (XI, 592 p. 105 illus.)
Collana	Security and Cryptology ; ; 9783
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Management information systems Computer science Coding theory Information theory Computer science—Mathematics Cryptology Systems and Data Security Management of Computing and Information Systems Coding and Information Theory Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Operating modes -- Stream-cipher cryptanalysis -- Components -- Side-channels and implementations -- Automated tools for cryptanalysis -- Designs -- Block-cipher cryptanalysis -- Foundations and theory -- Authenticated-encryption and hash function cryptanalysis.
Sommario/riassunto	This book constitutes the thoroughly refereed post-conference proceedings of the 23rd International Conference on Fast Software Encryption, held in Bochum, Germany, in March 2016. The 29 revised full papers presented were carefully reviewed and selected from 86

initial submissions. The papers are organized in topical sections on operating modes; stream-cipher cryptanalysis; components; side-channels and implementations; automated tools for cryptanalysis; designs; block-cipher cryptanalysis; foundations and theory; and authenticated-encryption and hash function cryptanalysis.