1.

Record Nr.	UNISA996465579803316
Titolo	Selected Areas in Cryptography [[electronic resource]] : 6th Annual International Workshop, SAC'99 Kingston, Ontario, Canada, August 9-10, 1999 Proceedings / / edited by Howard Heys, Carlisle Adams
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-46513-8
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (VIII, 241 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1758
Disciplina	005.82
Soggetti	Data encryption (Computer science) Coding theory Information theory Computer science Computer communication systems Algorithms Management information systems Cryptology Coding and Information Theory Computer Science, general Computer Communication Networks Algorithm Analysis and Problem Complexity Management of Computing and Information Systems
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 at the end of each chapters and index.
Nota di contenuto	Cryptosystems and Pseudorandom Number Generators -- A Universal Encryption Standard -- Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator -- Elliptic Curve Pseudorandom Sequence Generators -- Security Aspects of Block Ciphers -- Adaptive-Attack Norm for Decorrelation and Super-Pseudorandomness -- Guesswork and Variation Distance as Measures of Cipher Security -- Modeling Linear Characteristics of Substitution-

Permutation Networks -- Strong Linear Dependence and Unbiased Distribution of Non-propagative Vectors -- Cryptanalysis of Block Ciphers -- Security of E2 against Truncated Differential Cryptanalysis -- Key-Schedule Cryptanalysis of DEAL -- Efficient Evaluation of Security against Generalized Interpolation Attack -- Efficient Implementations of Cryptosystems -- Efficient Implementation of Cryptosystems Based on Non-maximal Imaginary Quadratic Orders -- Improving and Extending the Lim/Lee Exponentiation Algorithm -- Software Optimization of Decorrelation Module -- Cryptography for Network Applications -- Pseudonym Systems -- Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures -- Protecting a Mobile Agent’s Route against Collusions -- Photuris: Design Criteria.