1. Record Nr. UNISA996465856603316

Titolo	Advances in Cryptology – EUROCRYPT 2000 [[electronic resource]] : International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14-18, 2000 Proceedings / / edited by Bart Preneel
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2000
ISBN	3-540-45539-6
Edizione	[1st ed. 2000.]
Descrizione fisica	1 online resource (XIII, 612 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1807
Disciplina	618.9268
Soggetti	Data encryption (Computer science) Computer communication systems Algorithms Operating systems (Computers) Computer mathematics Cryptology Computer Communication Networks Algorithm Analysis and Problem Complexity Operating Systems Computational Mathematics and Numerical Analysis
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Factoring and Discrete Logarithm -- Factorization of a 512-Bit RSA Modulus -- An Algorithm for Solving the Discrete Log Problem on Hyperelliptic Curves -- Analysis and Optimization of the TWINKLE Factoring Device -- Cryptanalysis I: Digital Signatures -- Noisy Polynomial Interpolation and Noisy Chinese Remaindering -- A Chosen Messages Attack on the ISO/IEC 9796-1 Signature Scheme -- Cryptanalysis of Countermeasures Proposed for Repairing ISO 9796-1 -- Security Analysis of the Gennaro-Halevi-Rabin Signature Scheme -- Invited Talk -- On the Security of 3GPP Networks -- Private Information Retrieval -- One-Way Trapdoor Permutations Are Sufficient for Non-trivial Single-Server Private Information Retrieval -- Single Database