1. Record Nr. UNINA9910143899503321

Titolo	Information Security and Privacy : 7th Australian Conference, ACISP 2002 Melbourne, Australia, July 3-5, 2002 Proceedings / / edited by Lynn Batten, Jennifer Seberry
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-45450-0
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (XII, 516 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2384
Disciplina	005.8
Soggetti	Data encryption (Computer science) Management information systems Computer science Operating systems (Computers) Computer communication systems Algorithms Computers and civilization Cryptology Management of Computing and Information Systems Operating Systems Computer Communication Networks Algorithm Analysis and Problem Complexity Computers and Society
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	Key Handling -- A New Distributed Primality Test for Shared RSA Keys Using Quadratic Fields -- Security Analysis and Improvement of the Global Key Recovery System -- The LILI-II Keystream Generator -- A Secure Re-keying Scheme with Key Recovery Property -- Trust and Secret Sharing -- Modelling Trust Structures for Public Key Infrastructures -- Size of Broadcast in Threshold Schemes with Disenrollment -- Requirements for Group Independent Linear

Threshold Secret Sharing Schemes -- Efficient Sharing of Encrypted Data -- Cheating Prevention in Linear Secret Sharing -- Fast Computation -- Note on Fast Computation of Secret RSA Exponents -- Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying -- Cryptanalysis I -- Cryptanalysis of Stream Cipher COS (2, 128) Mode I -- The Analysis of Zheng-Seberry Scheme -- Cryptanalysis of Stream Cipher Alpha1 -- A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem -- Elliptic Curves -- Isomorphism Classes of Hyperelliptic Curves of Genus 2 over -- Compact Representation of Domain Parameters of Hyperelliptic Curve Cryptosystems -- A New Elliptic Curve Scalar Multiplication Algorithm to Resist Simple Power Analysis -- AES -- Strengthening the Key Schedule of the AES -- On the Necessity of Strong Assumptions for the Security of a Class of Asymmetric Encryption Schemes -- Security Management -- Security Management: An Information Systems Setting -- Resolving Conflicts in Authorization Delegations -- Policy Administration Domains -- Authentication -- Maintaining the Validity of Digital Signatures in B2B Applications -- Short 3-Secure Fingerprinting Codes for Copyright Protection -- An Order-Specified Multisignature Scheme Secure against Active Insider Attacks -- Authenticated Operation of Open Computing Devices -- A New Identification Scheme Based on the Bilinear Diffie-Hellman Problem -- Invited Talk -- A Brief Outline of Research on Correlation Immune Functions -- Oblivious Transfer -- m out of n Oblivious Transfer -- Cryptanalysis II -- On the Security of Reduced Versions of 3-Pass HAVAL -- On Insecurity of the Side Channel Attack Countermeasure Using Addition-Subtraction Chains under Distinguishability between Addition and Doubling -- On the Security of a Modified Paillier Public-Key Primitive -- Dealing with Adversaries -- How to Play Sherlock Holmes in the World of Mobile Agents -- A Practical Approach Defeating Blackmailing -- Privacy against Piracy: Protecting Two-Level Revocable P-K Traitor Tracing -- Asynchronous Perfectly Secure Computation Tolerating Generalized Adversaries.

Sommario/riassunto

The Seventh Australasian Conference in Information Security and Privacy (ACISP) was held in Melbourne, 3–5July, 2002. The conference was sponsored by Deakin University and iCORE, Alberta, Canada and the Australian Com- ter Society. The aims of the annual ACISP conferences have been to bring together people working in di?erent areas of computer, communication, and information security from universities, industry, and government institutions. The conferences give the participants the opportunity to discuss the latest developments in the rapidly growing area of information security and privacy. The reviewing process took six weeks and we heartily thank all the m- bers of the program committee and the external referees for the many hours of valuable time given to the conference. The program committee accepted 36 papers from the 94 submitted. From those papers accepted 10 papers were from Australia, 5each from Korea and USA, 4 each from Singapore and Germany, 2 from Japan, and 1 each from The Netherlands, UK, Spain, Bulgaria, and India. The authors of every paper, whether accepted or not, made a valued contribution to the conference. In addition to the contributed papers, we were delighted to have presen- tions from the Victorian Privacy Commissioner, Paul Chadwick, and eminent researchers Professor Hugh Williams, Calgary, Canada, Professor Bimal Roy, ISI, Kolkota, India (whose invited talk was formally referred and accepted by the program committee), and Dr Hank Wolfe from Otago, New Zealand.