1. Record Nr. UNISA996465718303316

Titolo	Information Security and Privacy [[electronic resource]] : 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004, Proceedings / / edited by Huaxiong Wang, Josef Pieprzyk, Vijay Varadharajan
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-27800-1
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XIV, 498 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3108
Disciplina	005.8
Soggetti	Data encryption (Computer science) Management information systems Computer science Operating systems (Computers) Algorithms Computers and civilization Computer communication systems Cryptology Management of Computing and Information Systems Operating Systems Algorithm Analysis and Problem Complexity Computers and Society Computer Communication Networks
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	Broadcast Encryption and Traitor Tracing -- Multi-service Oriented Broadcast Encryption -- Secure and Insecure Modifications of the Subset Difference Broadcast Encryption Scheme -- Linear Code Implies Public-Key Traitor Tracing with Revocation -- TTS without Revocation Capability Secure Against CCA2 -- Private Information Retrieval and Oblivious Transfer -- Single Database Private Information Retrieval with

Logarithmic Communication -- Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions -- Trust and Secret Sharing -- Optimistic Fair Exchange Based on Publicly Verifiable Secret Sharing -- NGSCB: A Trusted Open System -- Cryptanalysis (I) -- The Biryukov-Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers -- Differential-Linear Type Attacks on Reduced Rounds of SHACAL-2 -- The Related-Key Rectangle Attack – Application to SHACAL-1 -- Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1 -- The Security of Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders -- Cryptanalysis (II) -- Analysis of a Conference Scheme Under Active and Passive Attacks -- Cryptanalysis of Two Password-Authenticated Key Exchange Protocols -- Analysis and Improvement of Micali's Fair Contract Signing Protocol -- Digital Signatures (I) -- Digital Signature Schemes with Domain Parameters -- Generic Construction of Certificateless Signature -- Cryptosystems (I) -- A Generalization of PGV-Hash Functions and Security Analysis in Black-Box Model -- How to Re-use Round Function in Super-Pseudorandom Permutation -- How to Remove MAC from DHIES -- Symmetric Key Authentication Services Revisited -- Fast Computation -- Improvements to the Point Halving Algorithm -- Theoretical Analysis of XL over Small Fields -- A New Method for Securing Elliptic Scalar Multiplication Against Side-Channel Attacks -- Mobile Agents Security -- A Mobile Agent System Providing Offer Privacy -- Digital Signatures (II) -- Identity-Based Strong Designated Verifier Signature Schemes -- Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups -- A Group Signature Scheme with Efficient Membership Revocation for Reasonable Groups -- Convertible Nominative Signatures -- Protocols -- Protocols with Security Proofs for Mobile Applications -- Secure Bilinear Diffie-Hellman Bits -- Weak Property of Malleability in NTRUSign -- Security Management -- Information Security Risk Assessment, Aggregation, and Mitigation -- Access Control and Authorisation -- A Weighted Graph Approach to Authorization Delegation and Conflict Resolution -- Authorization Mechanisms for Virtual Organizations in Distributed Computing Systems -- Cryptosystems (II) -- Unconditionally Secure Encryption Under Strong Attacks -- ManTiCore: Encryption with Joint Cipher-State Authentication -- Cryptanalysis (III) -- On Security of XTR Public Key Cryptosystems Against Side Channel Attacks -- On the Exact Flexibility of the Flexible Countermeasure Against Side Channel Attacks -- Fault Attacks on Signature Schemes.

Sommario/riassunto

The 9th Australasian Conference on Information Security and Privacy (ACISP 2004) was held in Sydney, 13–15 July, 2004. The conference was sponsored by the Centre for Advanced Computing – Algorithms and Cryptography (ACAC), Information and Networked Security Systems Research (INSS), Macquarie U- versity and the Australian Computer Society.
Theaimsoftheconferencearetobringtogetherresearchersandpractitioners working in areas of information security and privacy from universities, industry and government sectors. The conference program covered a range of aspects including cryptography, cryptanalysis, systems and network security. The program committee accepted 41 papers from 195 submissions. The - viewing process took six weeks and each paper was carefully evaluated by at least three members of the program committee. We appreciate the hard work of the members of the program committee and external referees who gave many hours of their valuable time. Of the accepted papers, there were nine from Korea, six from Australia, ?ve each from Japan and the USA, three each from China and Singapore, two each from Canada and Switzerland, and

one each from Belgium, France, Germany, Taiwan, The Netherlands and the UK. All the authors, whether or not their papers were accepted, made valued contributions to the conference. In addition to the contributed papers, Dr Arjen Lenstra gave an invited talk, entitled Likely and Unlikely Progress in Factoring.

ThisyeartheprogramcommitteeintroducedtheBestStudentPaperAward. The winner of the prize for the Best Student Paper was Yan-Cheng Chang from Harvard University for his paper Single Database Private Information Retrieval with Logarithmic Communication.