1.	Record Nr.	UNINA9910484780003321
	Titolo	Information Security and Privacy : 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings / / edited by Colin Boyd, Juan M. González Nieto
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
	Edizione	[1st ed. 2005.]
	Descrizione fisica	1 online resource (XIV, 594 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 3574
	Altri autori (Persone)	BoydColin <1959-> Gonzalez NietoJuan M
	Disciplina	005.8
	Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Coding theory Information theory Algorithms Electronic data processing - Management Cryptology Computer Communication Networks Operating Systems Coding and Information Theory IT Operations
	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 and author index.
	Nota di contenuto	Invited Talk -- All Sail, No Anchor III: Risk Aggregation and Time's Arrow -- Network Security -- Traversing Middleboxes with the Host Identity Protocol -- An Investigation of Unauthorised Use of Wireless Networks in Adelaide, South Australia -- An Efficient Solution to the ARP Cache Poisoning Problem -- Cryptanalysis -- On Stern's Attack Against Secret Truncated Linear Congruential Generators -- On the Success Probability of ? 2-attack on RC6 -- Solving Systems of

Differential Equations of Addition -- Group Communications -- A Tree Based One-Key Broadcast Encryption Scheme with Low Computational Overhead -- Dynamic Group Key Agreement in Tree-Based Setting -- Immediate Data Authentication for Multicast in Resource Constrained Network -- Elliptic Curve Cryptography -- Redundant Trinomials for Finite Fields of Characteristic 2 -- Efficient Tate Pairing Computation for Elliptic Curves over Binary Fields -- A Complete Divisor Class Halving Algorithm for Hyperelliptic Curve Cryptosystems of Genus Two -- Mobile Security -- Using “Fair Forfeit” to Prevent Truncation Attacks on Mobile Agents -- An Improved Execution Integrity Solution for Mobile Agents -- RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management -- Side Channel Attacks -- Enhanced DES Implementation Secure Against High-Order Differential Power Analysis in Smartcards -- Improved Zero Value Attack on XTR -- Efficient Representations on Koblitz Curves with Resistance to Side Channel Attacks -- Evaluation and Biometrics -- SIFA: A Tool for Evaluation of High-Grade Security Devices -- Cancelable Key-Based Fingerprint Templates -- Public Key Cryptosystems -- Hybrid Signcryption Schemes with Insider Security -- On the Possibility of Constructing Meaningful Hash Collisions for Public Keys -- Tunable Balancing of RSA.-Access Control I -- Key Management for Role Hierarchy in Distributed Systems -- A Formalization of Distributed Authorization with Delegation -- Signatures I -- Two Improved Partially Blind Signature Schemes from Bilinear Pairings -- On the Security of Nominative Signatures -- Invited Talk -- Who Goes There? Internet Banking: A Matter of Risk and Reward -- Access Control II -- Role Activation Management in Role Based Access Control -- VO-Sec: An Access Control Framework for Dynamic Virtual Organization -- Threshold Cryptography -- An Efficient Implementation of a Threshold RSA Signature Scheme -- GBD Threshold Cryptography with an Application to RSA Key Recovery -- An (n–t)-out-of-n Threshold Ring Signature Scheme -- Protocols I -- Deposit-Case Attack Against Secure Roaming -- Security Requirements for Key Establishment Proof Models: Revisiting Bellare–Rogaway and Jeong–Katz–Lee Protocols -- Group Signatures -- Group Signature Schemes with Membership Revocation for Large Groups -- An Efficient Group Signature Scheme from Bilinear Maps -- Group Signature Where Group Manager, Members and Open Authority Are Identity-Based -- Protocols II -- Analysis of the HIP Base Exchange Protocol -- ID-based Authenticated Key Agreement for Low-Power Mobile Devices -- Signatures II -- On the Security of Two Key-Updating Signature Schemes -- Building Secure Tame-like Multivariate Public-Key Cryptosystems: The New TTS -- Invited Talk -- Potential Impacts of a Growing Gap Between Theory and Practice in Information Security -- Credentials -- Security Analysis and Fix of an Anonymous Credential System -- Counting Abuses Using Flexible Off-line Credentials -- Symmetric Cryptography -- Cryptanalysis of Two Variants of PCBC Mode When Used for Message Integrity -- New Cryptographic Applications of Boolean FunctionEquivalence Classes.