1.

Record Nr.	UNINA9910484539803321
Titolo	Information Security and Cryptology : First SKLOIS Conference, CISC 2005, Beijing, China, December 15-17, 2005, Proceedings / / edited by Dengguo Feng, Dongdai Lin, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
ISBN	3-540-32424-0 3-540-30855-5
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 428 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3822
Altri autori (Persone)	FengDengguo LinDongdai YungMoti
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Computer networks Operating systems (Computers) Algorithms Computers and civilization Cryptology Coding and Information Theory Computer Communication Networks Operating Systems 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 and index.
Nota di contenuto	Invited Talks -- On Bluetooth Repairing: Key Agreement Based on Symmetric-Key Cryptography -- You Can Prove So Many Things in Zero-Knowledge -- Identity Based Cryptography -- Improvements on Security Proofs of Some Identity Based Encryption Schemes -- An ID-Based Verifiable Encrypted Signature Scheme Based on Hess's Scheme

-- ID-Based Signature Scheme Without Trusted PKG -- Security Modelling -- Specifying Authentication Using Signal Events in CSP -- Modeling RFID Security -- Systems Security -- Enforcing Email Addresses Privacy Using Tokens -- Efficient Authentication of Electronic Document Workflow -- Signature Schemes -- Practical Strong Designated Verifier Signature Schemes Based on Double Discrete Logarithms -- Efficient Group Signatures from Bilinear Pairing -- Enhanced Aggregate Signatures from Pairings -- Constructing Secure Proxy Cryptosystem -- Symmetric Key Mechanisms -- Towards a General RC4-Like Keystream Generator -- HCTR: A Variable-Input-Length Enciphering Mode -- The kth-Order Quasi-Generalized Bent Functions over Ring Z p -- A Fast Algorithm for Determining the Linear Complexity of Periodic Sequences -- Zero-Knowledge and Secure Computations -- An Unbounded Simulation-Sound Non-interactive Zero-Knowledge Proof System for NP -- An Improved Secure Two-Party Computation Protocol -- Threshold Cryptography -- Security Analysis of Some Threshold Signature Schemes and Multi-signature Schemes -- ID-Based Threshold Unsigncryption Scheme from Pairings -- Intrusion Detection Systems -- Improvement of Detection Ability According to Optimum Selection of Measures Based on Statistical Approach -- The Conflict Detection Between Permission Assignment Constraints in Role-Based Access Control -- Toward Modeling Lightweight Intrusion Detection System Through Correlation-Based Hybrid FeatureSelection -- Protocol Cryptanalysis -- Security Analysis of Three Cryptographic Schemes from Other Cryptographic Schemes -- An Effective Attack on the Quantum Key Distribution Protocol Based on Quantum Encryption -- ECC Algorithms -- A Remark on Implementing the Weil Pairing -- Efficient Simultaneous Inversion in Parallel and Application to Point Multiplication in ECC -- Applications -- Key Management for Secure Overlay Multicast -- Design and Implementation of IEEE 802.11i Architecture for Next Generation WLAN -- Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault -- Secret Sharing -- Classification of Universally Ideal Homomorphic Secret Sharing Schemes and Ideal Black-Box Secret Sharing Schemes -- New Methods to Construct Cheating Immune Multisecret Sharing Scheme -- Denial of Service Attacks -- Detection of Unknown DoS Attacks by Kolmogorov-Complexity Fluctuation -- MIPv6 Binding Update Protocol Secure Against Both Redirect and DoS Attacks.

Sommario/riassunto

The ?rst SKLOIS Conference on Information Security and Cryptography (CISC 2005) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences. It was held in Beijing, China, December 15-17,2005 andwassponsoredbytheInstituteofSoftware,theChineseAcademy of Sciences, the Graduate School of the Chinese Academy of Sciences and the National Science Foundation of China. The conference proceedings, represe- ing invited and contributed papers, are published in this volume of Springer’s Lecture Notes in Computer Science (LNCS) series. The area of research covered by CISC has been gaining importance in recent years, and a lot of fundamental, experimental and applied work has been done, advancing the state of the art. The program of CISC 2005 covered numerous ?elds of research within the general scope of the conference. The International Program Committee of the conference received a total of 196 submissions (from 21 countries). Thirty-three submissions were selected for presentation as regular papers and are part of this volume. In addition to this track, the conference also hosted a short-paper track of 32 presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas and based on their ranking and strict selection criteria the papers were selected for the various tracks. We note that stricter criteria were applied to papers co-authored by program committee members. We further note that, obviously, no member took part in in?uencing the ranking of his or her own submissions.