1. Record Nr. UNISA996466256103316

Titolo	Information Security and Cryptology [[electronic resource]] : Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers / / edited by Dingyi Pei, Moti Yung, Dongdai Lin, Chuankun Wu
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-79499-9
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XII, 534 p.)
Collana	Security and Cryptology ; ; 4990
Disciplina	001.5436
Soggetti	Data protection Cryptography Data encryption (Computer science) Electronic data processing—Management Computers and civilization Computer networks Algorithms Data and Information Security Cryptology IT Operations Computers and Society Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and author index.
Nota di contenuto	Invited Talks -- Cryptanalysis of the SFLASH Signature Scheme -- On the Evolution of User Authentication: Non-bilateral Factors -- Digital Signature Schemes -- ECDSA-Verifiable Signcryption Scheme with Signature Verification on the Signcrypted Message -- Provably Secure Identity-Based Undeniable Signatures with Selective and Universal Convertibility -- An Efficient ID-Based Proxy Signature Scheme from Pairings -- Block Cipher -- Improved and Multiple Linear Cryptanalysis of Reduced Round Serpent -- Linear Slide Attacks on the KeeLoq Block

Cipher -- Key Management -- A Key Predistribution Scheme Based on 3-Designs -- Provably Secure N-Party Authenticated Key Exchange in the Multicast DPWA Setting -- A Provably Secure One-Pass Two-Party Key Establishment Protocol -- Zero Knowledge and Secure Computation Protocols -- Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model under Standard Assumption -- Secure Two-Party Computation of Squared Euclidean Distances in the Presence of Malicious Adversaries -- A Discrete-Logarithm Based Non-interactive Non-malleable Commitment Scheme with an Online Knowledge Extractor -- Secret Sharing -- Verifiable Multi-secret Sharing Schemes for Multiple Threshold Access Structures -- Key Management Based on Hierarchical Secret Sharing in Ad-Hoc Networks -- Probabilistic (n, n) Visual Secret Sharing Scheme for Grayscale Images -- Stream Cipher and Pseudorandomness -- Mutually Clock-Controlled Feedback Shift Registers Provide Resistance to Algebraic Attacks -- Four Families of Binary Sequences with Low Correlation and Large Linear Complexity -- Pseudo-Randomness of Discrete-Log Sequences from Elliptic Curves -- Improved Bounds on the Linear Complexity of Keystreams Obtained by Filter Generators -- Boolean Functions -- Linear Equation on Polynomial Single Cycle T-Functions -- Weight Support Technique and the Symmetric Boolean Functions with Maximum Algebraic Immunity on Even Number of Variables -- Privacy and Deniability -- Anonymity and k-Choice Identities -- Deniable Authentication on the Internet -- Orthogonality between Key Privacy and Data Privacy, Revisited -- Unlinkable Randomizable Signature and Its Application in Group Signature -- Hash Functions -- An Improved Collision Attack on MD5 Algorithm -- Multivariates Polynomials for Hashing -- Public Key Cryptosystems -- Efficient Public Key Encryption with Keyword Search Schemes from Pairings -- Multi-Identity Single-Key Decryption without Random Oracles -- Public Key Analysis -- Kipnis-Shamir Attack on HFE Revisited -- Cryptanalysis of General Lu-Lee Type Systems -- A Timing-Resistant Elliptic Curve Backdoor in RSA -- Application Security -- A Watermarking Scheme in the Encrypted Domain for Watermarking Protocol -- Security Enhancement of a Flexible Payment Scheme and Its Role-Based Access Control -- Systems Security and Trusted Computing -- Building Trusted Sub-domain for the Grid with Trusted Computing -- Enhanced Security by OS-Oriented Encapsulation in TPM-Enabled DRM -- Online Tracing Scanning Worm with Sliding Window -- Network Security -- A New Proactive Defense Model Based on Intrusion Deception and Traceback -- On Modeling Post Decryption Error Processes in UMTS Air Interface -- A Simple, Smart and Extensible Framework for Network Security Measurement.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the Third SKLOIS (State Key Laboratory of Information Security) Conference on Information Security and Cryptology, Inscrypt 2007 (formerly CISC), held in Xining, China, in August/September 2007. The 33 revised full papers and 10 revised short papers presented together with 2 invited papers were carefully reviewed and selected from 167 submissions. The papers are organized in topical sections on digital signature schemes, block cipher, key management, zero knowledge and secure computation protocols, secret sharing, stream cipher and pseudorandomness, boolean functions, privacy and deniability, hash functions, public key cryptosystems, public key analysis, application security, system security and trusted computing, and network security.