1. Record Nr.	UNISA996465508303316
Titolo	Information Systems Security [[electronic resource]] : 9th International Conference, ICISS 2013, Kolkata, India, December 16-20, 2013. Proceedings / / edited by Aditya Bagchi, Indrakshi Ray
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-45204-3
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XVI, 404 p. 70 illus.)
Collana	Security and Cryptology ; ; 8303
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer communication systems Systems and Data Security Cryptology Computer Communication Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Challenges and Opportunities for Security with Differential Privacy -- An Encrypted In-Memory Column-Store: The Onion Selection Problem -- Risk Aware Approach to Data Confidentiality in Cloud Computing -- Jamming Resistant Schemes for Wireless Communication -- Improved Biometric-Based Three-factor Remote User Authentication Scheme with Key Agreement Using Smart Card -- Signcryption from Randomness Recoverable PKE Revisited -- Auctions with Rational Adversary -- A Framework for Formal Reasoning about Privacy Properties Based on Trust Relationships in Complex Electronic Services -- Correctness Verification in Outsourced Databases: More Reliable Fake Tuples Approach -- Policy Mining: A Bottom-Up Approach toward a Model Based Firewall Management -- Secure States versus Secure Executions - From Access Control to Flow Control -- Monitoring for Slow Suspicious Activities Using a Target Centric Approach -- RAPID-FeinSPN: A Rapid Prototyping Framework for Feistel and SPN-Based Block Ciphers -- Simple and Efficient Time-Bound Hierarchical Key

Assignment Scheme -- Traitor-Traceable Key Pre-distribution Based on Visual Secret Sharing -- Web Services Based Attacks against Image CAPTCHAs -- New Long-Term Glimpse of RC4 Stream Cipher -- A Voucher Assisted Adaptive Acknowledgement Based Intrusion Detection Protocol for MANETs -- Cryptanalysis of Pairing-Free Identity-Based Authenticated Key Agreement Protocols -- Information Theoretical Analysis of Side-Channel Attack -- Efficient Multi-bit Image Steganography in Spatial Domain -- Evolutionary Multibit Grouping Steganographic Algorithm -- Let the Right One in: Discovering and Mitigating Permission Gaps -- A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET -- Recipient Anonymous Ciphertext-Policy Attribute Based Encryption -- Error Correction of Partially Exposed RSA Private Keys from MSB Side -- Efficient Enforcement of Privacy for Moving Object Trajectories -- An Administrative Model for Spatio-Temporal Role Based Access Control -- A UC-Secure Authenticated Contributory Group Key Exchange Protocol Based on Discrete Logarithm.

Sommario/riassunto

This book constitutes the refereed proceedings of the 9th International Conference on Information Systems Security, ICISS 2013, held in Kolkata, India, in December 2013. The 20 revised full papers and 6 short papers presented together with 3 invited papers were carefully reviewed and selected from 82 submissions. The papers address theoretical and practical problems in information and systems security and related areas.