1. Record Nr. UNISA996466000903316

Titolo	Information Security Practice and Experience [[electronic resource]] : 8th International Conference, ISPEC 2012, Hangzhou, China, April 9-12, 2012, Proceedings / / edited by Mark D. Ryan, Ben Smyth, Guilin Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-29101-5
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XIII, 406 p. 68 illus.)
Collana	Security and Cryptology ; ; 7232
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Computer communication systems Information storage and retrieval Computers and civilization Management information systems Computer science Cryptology Systems and Data Security Computer Communication Networks Information Storage and Retrieval Computers and Society Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references and author index.
Nota di contenuto	A Pre-computable Signature Scheme with Efficient Verification for RFID / Fuchun Guo, Yi Mu, Willy Susilo and Vijay Varadharajan -- Redactable Signatures for Independent Removal of Structure and Content / Kai Samelin, Henrich C. Pohls, Arne Bilzhause, Joachim Posegga and Hermann de Meer -- Improved Efficiency of Chosen Ciphertext Secure Encryption from Factoring / Xianhui Lu, Bao Li, Qixiang Mei and Yamin Liu -- Deniable Encryptions Secure against Adaptive Chosen Ciphertext Attack / Chong-zhi Gao, Dongqing Xie and Baodian Wei --

Computational Soundness of Indistinguishability Properties without Computable Parsing / Hubert Comon-Lundh, Masami Hagiya, Yusuke Kawamoto and Hideki Sakurada -- New Impossible Differential Attacks on Camellia / Dongxia Bai and Leibo Li -- Impossible Differential Attacks on Reduced-Round LBlock / Ya Liu, Dawu Gu, Zhiqiang Liu and Wei Li -- New Truncated Differential Cryptanalysis on 3D Block Cipher / Takuma Koyama, Lei Wang, Yu Sasaki, Kazuo Sakiyama and Kazuo Ohta.
iPIN and mTAN for Secure eID Applications / Johannes Braun, Moritz Horsch and Alexander Wiesmaier -- Secure Distributed Computation of the Square Root and Applications / Manuel Liedel -- Prevent Kernel Return-Oriented Programming Attacks Using Hardware Virtualization / Tian Shuo, He Yeping and Ding Baozeng -- Structure-Based RSA Fault Attacks / Benjamin Michele, Juliane Kramer and Jean-Pierre Seifert -- Fault Analysis of the KATAN Family of Block Ciphers / Shekh Faisal Abdul-Latip, Mohammad Reza Reyhanitabar, Willy Susilo and Jennifer Seberry -- Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher / Yanfeng Wang, Wenling Wu and Xiaoli Yu -- On the CCA-1 Security of Somewhat Homomorphic Encryption over the Integers / Zhenfei Zhang, Thomas Plantard and Willy Susilo -- Partial Key Exposure on RSA with Private Exponents Larger Than N / Marc Joye and Tancrede Lepoint -- Linear Cryptanalysis of Reduced-Round ICEBERG / Yue Sun and Meiqin Wang -- Overcoming Significant Noise: Correlation-Template-Induction Attack / An Wang, Man Chen, Zongyue Wang and Yaoling Ding.
; Part 1. Spatio (Temporal) Data Modeling and Visualisation -- Usability of Spatio-Temporal Uncertainty Visualisation Methods / Hansi Senaratne, Lydia Gerharz, Edzer Pebesma and Angela Schwering -- Line Simplification in the Presence of Non-Planar Topological Relationships / Padraig Corcoran, Peter Mooney and Michela Bertolotto -- Critical Remarks on the Use of Conceptual Schemas in Geospatial Data Modelling-A Schema Translation Perspective / Tatjana Kutzner and Andreas Donaubauer -- Part 2. Spatial Data Infrastructures, Geo Web Services and Geo Semantic Web -- Towards an Active Directory of Geospatial Web Services / Francisco J. Lopez-Pellicer, Walter Renteria-Agualimpia, Javier Nogueras-Iso, F. Javier Zarazaga-Soria and Pedro R. Muro-Medrano -- Spatial Sensor Web for the Prediction of Electric Power Supply System Behaviour / Milos Bogdanovic, Natasa Veljkovic and Leonid Stoimenov -- Live Geoinformation with Standardized Geoprocessing Services / Theodor Foerster, Bastian Baranski and Harald Borsutzky -- Interlinking Geospatial Information in the Web of Data / Luis M. Vilches-Blazquez, Victor Saquicela and Oscar Corcho -- Part 3. Modelling and Management of Uncertainty, Spatio (Temporal) Data Quality and Metadata -- QualESTIM: Interactive Quality Assessment of Socioeconomic Data Using Outlier Detection / Christine Plumejeaud and Marlene Villanova-Oliver -- Distributed Integration of Spatial Data with Different Positional Accuracies / Alberto Belussi and Sara Migliorini -- Through a Fuzzy Spatiotemporal Information System for Handling Excavation Data / Asma Zoghlami, Cyril de Runz, Herman Akdag and Dominique Pargny -- Part 4. Mobility of Persons, Objects and Systems, Transports and Flows -- Using Weather Information to Improve Route Planning / Paul Litzinger, Gerhard Navratil, Ake Sivertun and Daniela Knorr -- Simulation of Laser Attacks against Aircrafts / Vaclav Talhofer, Teodor Balaz, Frantisek Racek, Alois Hofmann and Sarka Hoskova-Mayerova -- Automated Traffic Route Identification Through the Shared Nearest Neighbour Algorithm / Maribel Yasmina Santos, Joaquim P. Silva, Joao Moura-Pires and Monica Wachowicz -- Part 5. Spatial Analysis, Geostatistics, and Geo Information Retrieval --

Comparing Support Vector Regression and Statistical Linear Regression for Predicting Poverty Incidence in Vietnam / Cornelius Senf and Tobia Lakes -- Do Expressive Geographic Queries Lead to Improvement in Retrieval Effectiveness? / Damien Palacio, Christian Sallaberry, Guillaume Cabanac, Gilles Hubert and Mauro Gaio -- The GP-SET Method: A Spatial and Temporal Probabilistic Model for Geoprospective / Stephane Bourrelly and Christine Voiron-Canicio -- Part 6. Modelling and Spatial Analysis of Urban Dynamics, Urban GIS -- Predicting Spatiotemporal Distribution of Transient Occupants in Urban Areas / Toshihiro Osaragi and Takeshi Hoshino -- Towards Urban Fabrics Characterization Based on Buildings Footprints / Rachid Hamaina, Thomas Leduc and Guillaume Moreau -- The Use of Point Pattern Statistics in UrbanAnalysis / Ioannis Pissourios, Pery Lafazani, Stavros Spyrellis, Anastasia Christodoulou and Myron Myridis -- Part 7. GIS and Spatial Analysis for Global Change Modelling, Impact on Space -- Beach-Dune Morphological Relationships at Youghal Beach, Cork / Sarah Kandrot -- A New Method for Computing the Drainage Network Based on Raising the Level of an Ocean Surrounding the Terrain / Salles V. G. Magalhaes, Marcus V. A. Andrade, W. Randolph Franklin and Guilherme C. Pena -- Part 8. Geographic Information Science: Links with other Disciplines and Citizens -- Geographic Information Science as a Common Cause for Interdisciplinary Research / Thomas Blaschke, Josef Strobl, Lothar Schrott, Robert Marschallinger and Franz Neubauer, et al. -- Enhancing the Quality of Volunteered Geographic Information: A Constraint-Based Approach / Olga Yanenko and Christoph Schlieder.

Sommario/riassunto

This book constitutes the refereed proceedings of the 8th International Conference on Information Security Practice and Experience, ISPEC 2012, held in Hangzhou, China, in April 2012. The 20 revised full papers presented together with 7 work-in-progress papers were carefully reviewed and selected from 109 submissions. The papers are oranized in topical sections on digital signatures, public key cryptography, cryptanalysis, differential attacks, oblivious transfer, internet security, key management, applied cryptography, pins, fundamentals, fault attacks, and key recovery.