1. Record Nr. UNINA9910483554203321

Titolo	Information, security and cryptology-- ICISC 2009 : 12th International Conference, Seoul, Korea, December 2-4, 2009 : revised selected papers / / Donghoon Lee, Seokhie Hong, (eds.)
Pubbl/distr/stampa	New York, : Springer, 2010
ISBN	1-280-38800-5 9786613565921 3-642-14423-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (XIII, 387 p. 70 illus.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 5984 LNCS sublibrary. SL 4, Security and cryptology
Altri autori (Persone)	LeeDonghoon HongSeokhie
Disciplina	004.6
Soggetti	Computer security Cryptography
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	Key Management and Key Exchange -- Generic One Round Group Key Exchange in the Standard Model -- Modeling Leakage of Ephemeral Secrets in Tripartite/Group Key Exchange -- Efficient Certificateless KEM in the Standard Model -- Public Key Cryptography -- Accelerating Twisted Ate Pairing with Frobenius Map, Small Scalar Multiplication, and Multi-pairing -- Factoring Unbalanced Moduli with Known Bits -- Algebraic Cryptanalysis and Stream Cipher -- Algebraic Cryptanalysis of SMS4: Gröbner Basis Attack and SAT Attack Compared -- MXL3: An Efficient Algorithm for Computing Gröbner Bases of Zero-Dimensional Ideals -- Improved Linear Cryptanalysis of SOSEMANUK -- Security Management and Efficient Implementation -- Serial Model for Attack Tree Computations -- Lightweight Cryptography and RFID: Tackling the Hidden Overheads -- Side Channel Attack -- Power Analysis of Single-Rail Storage Elements as Used in MDPL -- A Timing Attack against Patterson Algorithm in the McEliece PKC -- Side-Channel Analysis of Cryptographic Software via Early-Terminating Multiplications -- Privacy Enhanced Technology -- First CPIR Protocol with Data-Dependent

Computation -- Efficient Fuzzy Matching and Intersection on Private Datasets -- Efficient Privacy-Preserving Face Recognition -- Cryptographic Protocol -- Linear, Constant-Rounds Bit-Decomposition -- Attacking and Repairing the Improved ModOnions Protocol -- Secret Handshakes with Revocation Support -- Cryptanalysis of Hash Function -- Practical Rebound Attack on 12-Round Cheetah-256 -- Preimage Attacks on Reduced Steps of ARIRANG and PKC98-Hash -- Improved Preimage Attack for 68-Step HAS-160 -- Distinguishing Attack on Secret Prefix MAC Instantiated with Reduced SHA-1 -- Network Security -- Cryptanalysis of a Message Recognition Protocol by Mashatan and Stinson -- Analysis of the Propagation Pattern of a Worm with Random Scanning Strategy Based on Usage Rate of Network Bandwidth.

Sommario/riassunto

ICISC 2009, the 12th International Conference on Information Security and Cryptology, was held in Seoul, Korea, during December 2–4, 2009. It was organized by the Korea Institute of Information Security and Cryptology (KIISC) and the Ministry of Public Administration and Security (MOPAS). The aim of this conference was to provide a forum for the presentation of new results in research, development, and applications in the field of information security and cryptology. It also served as a place for research information exchange. The conference received 88 submissions from 22 countries, covering all areas of information security and cryptology. The review and selection processes were carried out in two stages by the Program Committee (PC) comprising 57 prominent - searchers via online meetings. First, at least three PC members blind-reviewed each paper, and papers co-authored by the PC members were reviewed by at least five PC members. Second, individual review reports were revealed to PC members, and detailed interactive discussion on each paper followed. Through this process, the PC finally selected 25papers from15countries. The acceptance rate was 28. 4%. The authors of selected papers had a few weeks to prepare for their final versions based on the comments received from more than 80 external reviewers. The conference featured one tutorial and one invited talk. The tutorial was given by Amit Sahai from the University of California and the talk ´ was given by Michel Abdalla from Ecole normale sup´ erieure.