1. Record Nr.	UNINA9910483451303321
Titolo	Information Security : 10th International Conference, ISC 2007, Valparaiso, Chile, October 9-12, 2007, Proceedings / / edited by Juan Garay, Arjen K. Lenstra, Masahiro Mambo, Rene Peralta
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-75496-2
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XIII, 440 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4779
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Algorithms Computers, Special purpose Cryptology Computer Communication Networks Operating Systems Special Purpose and Application-Based Systems
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	Intrusion Detection -- Detecting System Emulators -- Features vs. Attacks: A Comprehensive Feature Selection Model for Network Based Intrusion Detection Systems -- E-NIPS: An Event-Based Network Intrusion Prediction System -- Digital Rights Management -- Enabling Fairer Digital Rights Management with Trusted Computing -- Traitor Tracing with Optimal Transmission Rate -- Symmetric-Key Cryptography -- The Security of Elastic Block Ciphers Against Key-Recovery Attacks -- Impossible-Differential Attacks on Large-Block Rijndael -- High-Speed Pipelined Hardware Architecture for Galois Counter Mode -- Cryptographic Protocols and Schemes -- Efficient Committed Oblivious Transfer of Bit Strings -- An Efficient Certified Email Protocol -- Revisiting the Security Model for Timed-Release

Encryption with Pre-open Capability -- On the Soundness of Restricted Universal Designated Verifier Signatures and Dedicated Signatures -- Identify-Based Cryptography -- Identity-Based Proxy Re-encryption Without Random Oracles -- Strongly-Secure Identity-Based Key Agreement and Anonymous Extension -- Cryptanalysis -- Small Private-Exponent Attack on RSA with Primes Sharing Bits -- Multiple Modular Additions and Crossword Puzzle Attack on NLSv2 -- New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py -- Network Security -- Queue Management as a DoS Counter-Measure? -- Software Obfuscation -- On the Concept of Software Obfuscation in Computer Security -- Specifying Imperative Data Obfuscations -- Public-Key Cryptosystems -- Token-Controlled Public Key Encryption in the Standard Model -- Trapdoor Permutation Polynomials of ?/n? and Public Key Cryptosystems -- A Generalization and a Variant of Two Threshold Cryptosystems Based on Factoring -- Towards a DL-Based Additively Homomorphic EncryptionScheme -- Elliptic Curves and Applications -- Differential Properties of Elliptic Curves and Blind Signatures -- Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication Using Multibase Number Representation -- Database Security and Privacy -- Enforcing Confidentiality in Relational Databases by Reducing Inference Control to Access Control -- Efficient Negative Databases from Cryptographic Hash Functions.

Sommario/riassunto

The 10th Information Security Conference (ISC 2007) was held in Valpara´ ?so, Chile, October 9–12, 2007. ISC is an annual international conference covering research in theory and applications of information security, aiming to attract high quality papers in all of its technical aspects. ISC was ?rst initiated as a workshop (ISW) in Japan in 1997, ISW 1999 was held in Malaysia and ISW 2000 in Australia. The name was changed to the current one when the conf- ence was held in Spain in 2001 (ISC 2001). The latest conferences were held in Brazil (ISC 2002), the UK (ISC 2003), the USA (ISC 2004), Singapore (ISC 2005),and Greece (ISC 2006). This year the event wassponsored by the Univ- sidad T´ ecnica Federico Santa Mar´ ?a (Valpara´ ?so, Chile), the Support Center for AdvancedTelecommunicationsTechnologyResearch,Foundation, SCAT(Tokyo, Japan), Microsoft Corporation, and Yahoo! Research. Re? ectingtheconference'sbroadscope,thisyear'smainProgramCommittee consisted of a relatively large number (49) of experts. Additionally, given the timely topic of cryptanalysis and design of hash functions and the NIST hash competition, the conference also featured a special Hash Subcommittee, chaired by Arjen Lenstra (EPFL and Bell Labs), as well as a panel on hashing, chaired by Bill Burr (NIST). The conference received 116 submissions, 29 of which were selected by the committee members for presentation at the conference, based on quality, originality and relevance. Each paper was anonymously reviewed by at least three committee members.