1.	Record Nr.	UNISA996466266603316
	Titolo	Advances in Information and Computer Security [[electronic resource]] : 5th International Worshop on Security, IWSEC 2010, Kobe, Japan, November 22-24, 2010, Proceedings / / edited by Isao Echizen, Noboru Kunihiro, Ryoichi Sasaki
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
	ISBN	3-642-16825-6
	Edizione	[1st ed. 2010.]
	Descrizione fisica	1 online resource (XIII, 371 p. 83 illus.)
	Collana	Security and Cryptology ; ; 6434
	Disciplina	005.8
	Soggetti	User interfaces (Computer systems) Computers and civilization Computer programming Computer security Management information systems Computer science Data encryption (Computer science) User Interfaces and Human Computer Interaction Computers and Society Programming Techniques Systems and Data Security Management of Computing and Information Systems Cryptology Kongress. Kobe <2010>
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Index unnumbered.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Invited Talks -- Automating Security Configuration and Administration: An Access Control Perspective -- Security Metrics and Security Investment Models -- Encryption -- Publishing Upper Half of RSA Decryption Exponent -- PA1 and IND-CCA2 Do Not Guarantee PA2: Brief Examples -- A Generic Method for Reducing Ciphertext Length of

Reproducible KEMs in the RO Model -- An Improvement of Key Generation Algorithm for Gentry’s Homomorphic Encryption Scheme -- Data and Web Security -- Practical Universal Random Sampling -- Horizontal Fragmentation for Data Outsourcing with Formula-Based Confidentiality Constraints -- Experimental Assessment of Probabilistic Fingerprinting Codes over AWGN Channel -- Validating Security Policy Conformance with WS-Security Requirements -- Protocols -- Efficient Secure Auction Protocols Based on the Boneh-Goh-Nissim Encryption -- Hierarchical ID-Based Authenticated Key Exchange Resilient to Ephemeral Key Leakage -- Group Signature Implies PKE with Non-interactive Opening and Threshold PKE -- Network Security -- A Generic Binary Analysis Method for Malware -- A-HIP: A Solution Offering Secure and Anonymous Communications in MANETs -- Securing MANET Multicast Using DIPLOMA -- Block Cipher -- Preimage Attacks against Variants of Very Smooth Hash -- Matrix Representation of Conditions for the Collision Attack of SHA-1 and Its Application to the Message Modification -- Mutual Information Analysis under the View of Higher-Order Statistics -- Known-Key Attacks on Rijndael with Large Blocks and Strengthening ShiftRow Parameter -- Implementation and Real Life Security -- Differential Addition in Generalized Edwards Coordinates -- Efficient Implementation of Pairing on BREW Mobile Phones -- Introducing Mitigation Use Cases to Enhance the Scope of Test Cases -- Optimal Adversary Behavior for the Serial Model of Financial Attack Trees.

Sommario/riassunto

The Fifth International Workshop on Security (IWSEC 2010) was held at Kobe InternationalConferenceCenter,Kobe,Japan,November22–24,2010. Thewo- shop was co-organized by CSEC, a special interest group concerned with the computer security of the Information Processing Society of Japan (IPSJ) and ISEC,atechnicalgroupconcernedwiththe informationsecurityofTheInstitute of Electronics, Information and Communication Engineers (IEICE). The exclentLocalOrganizingCommitteewasledbytheIWSEC2010GeneralCo-chairs, Hiroaki Kikuchi and Toru Fujiwara. This year IWSEC 2010 had three tracks, the Foundations of Security (Track I), Security in Networks and Ubiquitous Computing Systems (Track II), and Security in Real Life Applications (Track III), and the review and selection processes for these tracks were independent of each other. We received 75 paper submissions including 44 submissions for Track I, 20 submissions for Track II, and 11 submissions for Track III. We would like to thank all the authors who submitted papers. Each paper was reviewed by at least three reviewers. In - dition to the Program Committee members, many external reviewers joined the review process from their particular areas of expertise. We were fortunate to have this energetic team of experts, and are grateful to all of them for their hard work. This hard work included very active discussions; the discussion phase was almost as long as the initial individual reviewing. The review and discussions weresupportedbyaveryniceWeb-basedsystem,iChair. Wewouldliketothank its developers. Following the review phases, 22 papers including 13 papers for Track I, 6 papers for Track II, and 3 papers for Track III were accepted for publication in this volume of Advances in Information and Computer Security.