1.

Record Nr.	UNISA996465946403316
Titolo	Information Security Applications [[electronic resource]] : 13th International Workshop, WISA 2012, Jeju Island, Korea, August 16-18, 2012, Revised Selected Papers / / edited by Dong Hoon Lee, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-35416-5
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XII, 371 p. 135 illus.)
Collana	Security and Cryptology ; ; 7690
Disciplina	004
Soggetti	Computer networks Algorithms Cryptography Data encryption (Computer science) Electronic data processing—Management Application software Data protection Computer Communication Networks Cryptology IT Operations Computer and Information Systems Applications Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Security on LBlock against Biclique Cryptanalysis -- Improved Impossible Differential Attacks on Reduced-Round MISTY1.- Efficient Parallel Evaluation of Multivariate Quadratic Polynomials on GPUs. - Enumeration of Even-Variable Boolean Functions with Maximum Algebraic Immunity.- Multi-precision Multiplication for Public-Key Cryptography on Embedded Microprocessors.- Three Phase Dynamic Current Mode Logic: A More Secure DyCML to Achieve a More Balanced Power Consumption.- Improved Differential Fault Analysis on Block Cipher ARIA.- Multi-Level Controlled Signature.- Tate Pairing

Computation on Generalized Hessian Curves -- Reduction-Centric Non-programmable Security Proof for the Full Domain Hash in the Random Oracle Model.- An Authentication and Key Management Scheme for the Proxy Mobile IPv6.- Payment Approval for PayWord -- Anonymity-Based Authenticated Key Agreement with Full Binding Property.- A Study for Classification of Web Browser Log and Timeline Visualization.- Intellectual Property Protection for Integrated Systems Using Soft Physical Hash Functions.- N-Victims: An Approach to Determine N-Victims for APT Investigations.- An Efficient Filtering Method for Detecting Malicous Web Pages.- Lightweight Client-Side Methods for Detecting Email Forgery.- AIGG Threshold Based HTTP GET Flooding Attack Detection.- Implementation of GESNIC for Web Server Protection against HTTP GET Flooding Attacks.- Privacy-Aware VANET Security: Putting Data-Centric Misbehavior and Sybil Attack Detection Schemes into Practice.- On Trigger Detection against Reactive Jamming Attacks: A Localized Solution.- Efficient Self-organized Trust Management in Location Privacy Enhanced VANETs.- A Trust Management Model for QoS-Based Service Selection.- Multilevel Secure Database on Security Enhanced Linux for System High Distributed Systems.

Sommario/riassunto

This book constitutes the thoroughly refereed post-workshop proceedings of the 13th International Workshop on Information Security Applications, WISA 2012, held in Jeju Island, Korea, in August 2012. The 26 revised full papers presented together with 8 short papers were carefully reviewed and selected from 100 submissions. The papers are focusing on all technical and practical aspects of symmetric cipher, secure hardware/public key crypto application, cryptographic protocols/digital forensics, network security, and trust management/database security.