1. Record Nr. UNISA996466207203316

Titolo	Advances in Information and Computer Security [[electronic resource]] : 7th International Workshop on Security, IWSEC 2012, Fukuoka, Japan, November 7-9, 2012, Proceedings / / edited by Goichiro Hanaoka, Toshihiro Yamauchi
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2012
ISBN	3-642-34117-9
Edizione	[1st ed. 2012.]
Descrizione fisica	1 online resource (XII, 261 p. 33 illus.)
Collana	Security and Cryptology ; ; 7631
Disciplina	005.8
Soggetti	Computer security Management information systems Computer science Data encryption (Computer science) Computer science—Mathematics Computer communication systems Algorithms Systems and Data Security Management of Computing and Information Systems Cryptology Discrete Mathematics in Computer Science Computer Communication Networks Algorithm Analysis and Problem Complexity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Model-Based Conformance Testing for Android -- Application of Scalar Multiplication of Edwards Curves to Pairing-Based Cryptography -- Standardized Signature Algorithms on Ultra-constrained 4-Bit MCU -- Very Short Critical Path Implementation of AES with Direct Logic Gates -- One-Round Authenticated Key Exchange with Strong Forward Secrecy in the Standard Model against Constrained Adversary -- Compact Stateful Encryption Schemes with Ciphertext Verifiability --

Structured Encryption for Conceptual Graphs -- Symmetric-Key Encryption Scheme with Multi-ciphertext Non-malleability -- Slide Cryptanalysis of Lightweight Stream Cipher RAKAPOSHI -- Boomerang Distinguishers for Full HAS-160 Compression Function -- Polynomial-Advantage Cryptanalysis of 3D Cipher and 3D-Based Hash Function -- Annihilators of Fast Discrete Fourier Spectra Attacks -- Meet-in-the-Middle Attack on Reduced Versions of the Camellia Block Cipher -- Efficient Concurrent Oblivious Transfer in Super-Polynomial-Simulation Security -- Efficient Secure Primitive for Privacy Preserving Distributed Computations -- Generic Construction of GUC Secure Commitment in the KRK Model.

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Workshop on Security, IWSEC 2012, held in Fukuoka, Japan, in November 2012. The 16 revised selected papers presented in this volume were carefully reviewed and selected from 53 submissions. They are organized in topical sections named: implementation; encryption and key exchange; cryptanalysis; and secure protocols.