1. Record Nr. UNISA996465379303316

Titolo	Information Security and Privacy [[electronic resource]] : 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013, Proceedings / / edited by Colin Boyd, Leonie Simpson
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-39059-5
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XII, 437 p. 70 illus.)
Collana	Security and Cryptology ; ; 7959
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Management information systems Computer science Coding theory Information theory Application software E-commerce Systems and Data Security Cryptology Management of Computing and Information Systems Coding and Information Theory Computer Appl. in Administrative Data Processing e-Commerce/e-business Conference papers and proceedings.
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 author index.
Nota di contenuto	Analysing the IOBC authenticated encryption mode -- A Chosen IV Related Key Attack on Grain -- Cryptanalysis of Helix and Phelix Revisited -- Toward Separating the Strong Adaptive Pseudo-Freeness from the Strong RSA Assumption -- Minkowski sum based lattice construction for multivariate simultaneous -- Coppersmith's technique and applications to RSA -- Lattices and security proofs -- Adaptive

Precision Floating Point LL -- Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors -- Key-Dependent Message Chosen-Ciphertext Security of the Cramer-Shoup Cryptosystem -- Black-Box Separations and their Adaptability to the Non-Uniform Model -- Injective Encodings to Elliptic Curves -- Membership Encryption and Its Applications -- Towards Privacy Preserving Mobile Internet Communications -- Count-min sketches for estimating password frequency with Hamming Distance -- Secret sharing -- A rational secret sharing protocol with unconditional security in the synchronous setting -- Secret Sharing Schemes with Conversion Protocol to Achieve Short Share-Size and Extendibility to Multiparty Computation.

Sommario/riassunto

This book constitutes the refereed conference proceedings of the 18th Australasian Conference on Information Security and Privacy, ACISP 2013, held in Brisbane, Australia, in July 2013. The 28 revised full papers presented were carefully selected from 78 submissions. Conference papers are organized in technical sessions, covering topics of Cryptoanalysis, RSA, Lattices and Security Proofs, Public Key Cryptography, Hashing, Signatures, Passwords, Mobile Security, and Secret Sharing.