1. Record Nr. UNINA9910484064703321

Titolo	Advances in Cryptology -- ASIACRYPT 2014 : 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, China, December 7-11, 2014, Part II / / edited by Palash Sarkar, Tetsu Iwata
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2014
ISBN	3-662-45608-7
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (XXII, 528 p. 76 illus.)
Collana	Security and Cryptology ; ; 8874
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Coding theory Information theory Management information systems Computer science Computers Computer science—Mathematics Cryptology Systems and Data Security Coding and Information Theory Management of Computing and Information Systems Theory of Computation Mathematics of Computing
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	Cryptology and coding theory -- Authenticated encryption -- Symmetric key cryptanalysis -- Side channel analysis -- Hyperelliptic curve cryptography -- Factoring and discrete log -- Cryptanalysis -- Signatures -- Zero knowledge -- Encryption schemes -- Outsourcing and delegation -- Obfuscation -- Homomorphic cryptography -- Secret sharing -- Block ciphers and passwords -- Black-box separation

-- Composability -- Multi-party computation.

Sommario/riassunto

The two-volume set LNCS 8873 and 8874 constitutes the refereed proceedings of the 20th International Conference on the Theory and Applications of Cryptology and Information Security, ASIACRYPT 2014, held in Kaoshiung, Taiwan, in December 2014. The 55 revised full papers and two invited talks presented were carefully selected from 255 submissions. They are organized in topical sections on cryptology and coding theory; authenticated encryption; symmetric key cryptanalysis; side channel analysis; hyperelliptic curve cryptography; factoring and discrete log; cryptanalysis; signatures; zero knowledge; encryption schemes; outsourcing and delegation; obfuscation; homomorphic cryptography; secret sharing; block ciphers and passwords; black-box separation; composability; multi-party computation.