1. Record Nr. UNISA996465563603316

Titolo	Advances in Cryptology -- ASIACRYPT 2013 [[electronic resource]] : 19th International Conference on the Theory and Application of Cryptology and Information, Bengaluru, India, December 1-5, 2013, Proceedings, Part II / / edited by Kazue Sako, Palash Sarkar
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-42045-1
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XXIV, 542 p. 58 illus.) : online resource
Collana	Security and Cryptology ; ; 8270
Disciplina	005.82
Soggetti	Data encryption (Computer science) Algorithms Management information systems Computer science Computer science—Mathematics Computer security Applied mathematics Engineering mathematics Cryptology Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Discrete Mathematics in Computer Science Systems and Data Security Applications of Mathematics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Message Authentication Codes -- Signatures -- Cryptography Based Upon Physical Assumptions -- Multi-Party Computation -- Cryptographic Primitives -- Analysis, Cryptanalysis and Passwords -- Leakage-Resilient Cryptography -- Two-Party Computation -- Hash Functions.
Sommario/riassunto	The two-volume set LNCS 8269 and 8270 constitutes the refereed

proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information, Asiacrypt 2013, held in Bengaluru, India, in December 2013. The 54 revised full papers presented were carefully selected from 269 submissions. They are organized in topical sections named: zero-knowledge, algebraic cryptography, theoretical cryptography, protocols, symmetric key cryptanalysis, symmetric key cryptology: schemes and analysis, side-channel cryptanalysis, message authentication codes, signatures, cryptography based upon physical assumptions, multi-party computation, cryptographic primitives, analysis, cryptanalysis and passwords, leakage-resilient cryptography, two-party computation, hash functions.