1.	Record Nr.	UNISA996466370003316
	Titolo	Applied Cryptography and Network Security [[electronic resource]] : 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers / / edited by Tal Malkin, Vladimir Kolesnikov, Allison Lewko, Michalis Polychronakis
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
	ISBN	3-319-28166-6
	Edizione	[1st ed. 2015.]
	Descrizione fisica	1 online resource (XVIII, 698 p. 152 illus. in color.)
	Collana	Security and Cryptology ; ; 9092
	Disciplina	005.82
	Soggetti	Computer security
		Data encryption (Computer science)
		Computer communication systems
		Management information systems
		Computer science
		Computers
		Computers and civilization
		Systems and Data Security
		Cryptology
		Computer Communication Networks
		Management of Computing and Information Systems
		Theory of Computation
		Computers and Society
	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	Secure computation: primitives and new models -- Public key cryptographic primitives -- Secure computation II: applications -- Anonymity and related applications -- Cryptanalysis and attacks (symmetric crypto) -- Privacy and policy enforcement -- Authentication via eye tracking and proofs of proximity -- Malware analysis and side channel attacks -- Side channel countermeasures and tamper resistance/PUFs -- Leakage resilience and pseudorandomness.

Sommario/riassunto   This book constitutes the refereed proceedings of the 13th
International Conference on Applied Cryptography and Network
Security, ACNS 2015, held in New York, NY, USA, in June 2015. The 33
revised full papers included in this volume and presented together with
2 abstracts of invited talks, were carefully reviewed and selected from
157 submissions. They are organized in topical sections on secure
computation: primitives and new models; public key cryptographic
primitives; secure computation II: applications; anonymity and related
applications; cryptanalysis and attacks (symmetric crypto); privacy and
policy enforcement; authentication via eye tracking and proofs of
proximity; malware analysis and side channel attacks; side channel
countermeasures and tamper resistance/PUFs; and leakage resilience
and pseudorandomness.