

1. Record Nr.	UNINA9910484552103321
Titolo	Theory of Cryptography : 12th International Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I // edited by Yevgeniy Dodis, Jesper Buus Nielsen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
ISBN	3-662-46494-2
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XX, 660 p. 89 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 9014
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer science Algorithms Computer science - Mathematics Discrete mathematics Cryptology Data and Information Security Theory of Computation Discrete Mathematics in Computer Science
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	Foundations -- Symmetric Key -- Multiparty Computation -- Concurrent and Resettable Security -- Non-malleable Codes and Tampering -- Privacy Amplification -- Encryption and Key Exchange.
Sommario/riassunto	The two-volume set LNCS 9014 and LNCS 9015 constitutes the refereed proceedings of the 12th International Conference on Theory of Cryptography, TCC 2015, held in Warsaw, Poland in March 2015. The 52 revised full papers presented were carefully reviewed and selected from 137 submissions. The papers are organized in topical sections on foundations, symmetric key, multiparty computation, concurrent and resettable security, non-malleable codes and tampering, privacy

amplification, encryption and key exchange, pseudorandom functions and applications, proofs and verifiable computation, differential privacy, functional encryption, obfuscation.
