1. Record Nr.	UNISA996547953003316
Autore	Ren Kui
Titolo	Searchable encryption : from concepts to systems / / Kui Ren and Cong Wang
Pubbl/distr/stampa	Cham, Switzerland : , : Springer International Publishing, , [2023] ©2023
ISBN	3-031-21377-7
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (178 pages)
Collana	Wireless Networks, , 2366-1445
Disciplina	005.8
Soggetti	Data encryption (Computer science) Data encryption (Computer science) - Technological innovations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Fundamental Cryptographic Algorithms and Technologies -- Searchable Encryption Semantics -- Recent Advancements on Functionality and Performance -- Security Impact of Leakage Profiles: Threats and Countermeasures -- Towards Fully-functional Encrypted Databases -- Conclusion.
Sommario/riassunto	This book comprehensively reviews searchable encryption, which represents a series of research developments that directly enable search functionality over encrypted data. The book majorly covers: 1) the design and implementation of encrypted search algorithms, data structures, and systems that facilitate various forms of search over always-encrypted databases; 2) different threat models, assumptions, and the related security guarantees, when using searchable encryption in the real-world settings; and 3) latest efforts in building full-fledged encrypted database systems that draw insights from searchable encryption constructions. The book fits in the timely context, where the necessity of safeguarding important and sensitive data has been globally recognized. Traditional security measures, such as storing data behind network firewalls and layers of access control mechanisms to keep attackers out, are no longer sufficient to cope with the expanding landscape of surging cyber threats. There is an urgent call to keep sensitive data always encrypted to protect the data at rest, in transit, and in use. Doing so guarantees data confidentiality for owners, even if

the data is out of their hands, e.g., hosted at in-the-cloud databases. The daunting challenge is how to perform computation over encrypted data. As we unfold in this book, searchable encryption, as a specific line of research in this broadly defined area, has received tremendous advancements over the past decades. This book is majorly oriented toward senior undergraduates, graduate students, and researchers, who want to work in the field and need extensive coverage of encrypted database research. It also targets security practitioners who want to make well-informed deployment choices of the latest advancements in searchable encryption for their targeted applications. Hopefully, this book will be beneficial in both regards.