1.

Record Nr.	UNINA9910838221303321
Autore	Goldreich Oded
Titolo	Providing Sound Foundations for Cryptography : On the Work of Shafi Goldwasser and Silvio Micali
Pubbl/distr/stampa	San Rafael : , : Morgan & Claypool Publishers, , 2019 ©2019
ISBN	1-4503-7269-4
Edizione	[1st ed.]
Descrizione fisica	1 online resource (838 pages)
Collana	ACM Bks.
Disciplina	005.824
Soggetti	Algorithms Computer algorithms Computer scientists
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Contents -- Preface -- Acknowledgments -- Photo and Text Credits -- PART I. BIOGRAPHIES, INTERVIEWS, AND AWARD LECTURES -- 1. A Story Behind Every Problem: A Brief Biography of Shafi Goldwasser -- 2. One Obsession at a Time: A Brief Biography of Silvio Micali -- 3. An Interview with Shafi Goldwasser -- 4. An Interview with Silvio Micali -- 5. The Cryptographic Lens: Shafi Goldwasser'sTuring Lecture -- 6. Proofs, According to Silvio: Silvio Micali's Turing Lecture -- PART II. ORIGINAL PAPERS -- 7. Probabilistic Encryption -- 8. The Knowledge Complexity of Interactive Proof Systems -- 9. How to Generate Cryptographically Strong Sequences of Pseudorandom Bits -- 10. How to Construct Random Functions -- 11. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks -- 12. Proofs that Yield Nothing but Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems -- 13. How to Play Any Mental Game: A Completeness Theorem for Protocols with Honest Majority -- 14. Non-Interactive Zero-Knowledge (NIZK) Proof Systems -- 15. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation -- 16. Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions -- PART III. PERSPECTIVES -- 17. On the Foundations of Cryptography -- 18. On the Impact of Cryptography on Complexity Theory -- 19. On Some Noncryptographic Works of

Sommario/riassunto

Cryptography is concerned with the construction of schemes that withstand any abuse. A cryptographic scheme is constructed so as to maintain a desired functionality, even under malicious attempts aimed at making it deviate from its prescribed behavior. The design of cryptographic systems must be based on firm foundations, whereas ad hoc approaches and heuristics are a very dangerous way to go. These foundations were developed mostly in the 1980s, in works that are all co-authored by Shafi Goldwasser and/or Silvio Micali. These works have transformed cryptography from an engineering discipline, lacking sound theoretical foundations, into a scientific field possessing a well-founded theory, which influences practice as well as contributes to other areas of theoretical computer science.