

1. Record Nr.	UNINA9911010531003321
Autore	Guo Fuchun
Titolo	Introduction to Cryptographic Definitions : A Step-by-Step Guide for Beginners // by Fuchun Guo, Willy Susilo, Khoa Nguyen, Xiaofeng Chen, Zhen Zhao
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-91969-6
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (0 pages)
Collana	Undergraduate Topics in Computer Science, , 2197-1781
Altri autori (Persone)	SusiloWilly NguyenKhoa ChenXiaofeng ZhaoZhen
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Data protection Cryptology Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Overview of Cryptographic Definitions -- Mathematics -- Computing Machines -- Computational Complexity -- From Computational Complexity to Cryptography -- Cryptographic Primitives for Syntax Definitions -- Cryptographic Primitives for Security Definitions -- Other Readings.
Sommario/riassunto	Cryptographic definitions are often abstract and complex, making them challenging for beginners to understand and apply. This concise textbook/resource provides a structured introduction to cryptographic definitions, explaining the syntax definitions and security definitions of cryptographic primitives. It builds foundational knowledge by covering essential mathematical concepts and formal definitions in cryptology. Through a carefully designed learning curve, readers will grasp key elements, why they are defined this way, and how new definitions are developed. The book's presentation enables readers to validate and propose cryptographic definitions, offering a step-by-step guide to

understanding them. Topics and features: · Covers all essential components of cryptographic definitions from sets and functions, making the subject accessible to beginners · Introduces intermediate concepts to smooth the transition from basic principles to formal definitions · Equips readers with the skills to validate and propose cryptographic definitions, linking theory with research · Minimizes unnecessary complexity while retaining depth, thereby ensuring a smooth learning experience Advanced undergraduate students, security engineers, and professionals interested in the formal foundations of cryptographic definitions will find the work an invaluable guide. The text is also an ideal reference for graduate students and early-stage researchers in cryptology and computer security. Dr. Fuchun Guo, Dr. Willy Susilo, Dr. Khoa Nguyen are affiliated with the University of Wollongong, Australia. Dr. Xiaofeng Chen and Dr. Zhen Zhao are affiliated with the Xidian University, China. .
