1.

Record Nr.	UNINA9910299459803321
Autore	Guo Fuchun
Titolo	Introduction to Security Reduction / / by Fuchun Guo, Willy Susilo, Yi Mu
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-93049-4
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (262 pages)
Disciplina	005.82
Soggetti	Data structures (Computer science) Computer security Data protection Data Structures and Information Theory Systems and Data Security Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Notions, Definitions and Models -- Identity-Based Encryption -- Foundations of Group-Based Cryptography -- Foundations of Security Reduction -- Digital Signatures With Random Oracles -- Digital Signatures Without Random Oracles -- Public Key Encryption With Random Oracles -- Public Key Encryption Without Random Oracles -- Identity-Based Encryption With Random Oracles -- Identity-Based Encryption Without Random Oracles.
Sommario/riassunto	This monograph illustrates important notions in security reductions and essential techniques in security reductions for group-based cryptosystems. Using digital signatures and encryption as examples, the authors explain how to program correct security reductions for those cryptographic primitives. Various schemes are selected and re-proven in this book to demonstrate and exemplify correct security reductions. This book is suitable for researchers and graduate students engaged with public-key cryptography.