1. Record Nr. UNINA9910373926603321

Autore	Omondi Amos R
Titolo	Cryptography Arithmetic : Algorithms and Hardware Architectures / / by Amos R. Omondi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-34142-9
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XIV, 336 p. 73 illus.)
Collana	Advances in Information Security, , 1568-2633 ; ; 77
Disciplina	652.8
Soggetti	Data structures (Computer science) Data encryption (Computer science) Microprocessors Electronic circuits Data Structures and Information Theory Cryptology Processor Architectures Circuits and Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 Basic Computer Arithmetic -- 2 Mathematical Fundamentals I: Number Theory -- 3 Modular-Arithmetic Cryptosystems -- 4 Modular Reduction -- 5 Modular Addition and Multiplication -- 6 Modular Exponentiation, Inversion, and Division -- 7 Mathematical Fundamentals II: Abstract Algebra -- 8 Elliptic-Curve Basics -- 9 Elliptic-Curve Cryptosystems -- 10 Polynomial-basis arithmetic -- 11 Normal-basis arithmetic -- A Mathematical Proofs -- Index.
Sommario/riassunto	Modern cryptosystems, used in numerous applications that require secrecy or privacy - electronic mail, financial transactions, medical-record keeping, government affairs, social media etc. - are based on sophisticated mathematics and algorithms that in implementation involve much computer arithmetic. And for speed it is necessary that the arithmetic be realized at the hardware (chip) level. This book is an introduction to the implementation of cryptosystems at that level. The aforementioned arithmetic is mostly the arithmetic of finite fields, and

the book is essentially one on the arithmetic of prime fields and binary fields in the context of cryptography. The book has three main parts. The first part is on generic algorithms and hardware architectures for the basic arithmetic operations: addition, subtraction, multiplication, and division. The second part is on the arithmetic of prime fields. And the third part is on the arithmetic of binary fields. The mathematical fundamentals necessary for the latter two parts are included, as are descriptions of various types of cryptosystems, to provide appropriate context. This book is intended for advanced-level students in Computer Science, Computer Engineering, and Electrical and Electronic Engineering. Practitioners too will find it useful, as will those with a general interest in "hard" applications of mathematics.