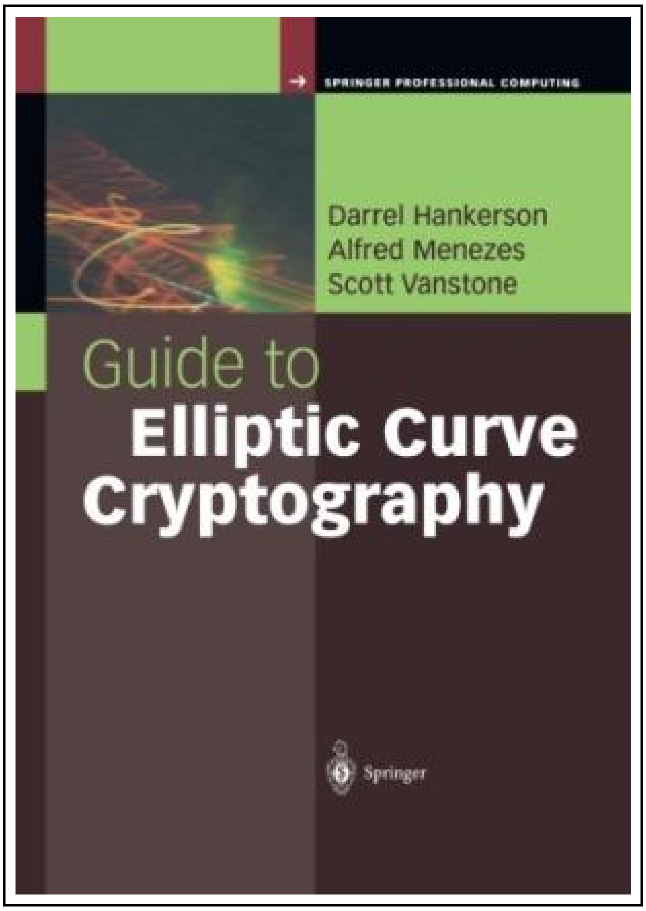
Guide to Elliptic Curve Cryptography



Filesize: 7.92 MB

Reviews

This composed book is excellent. This really is for all who statte that there had not been a worth reading through. Your life period will probably be change as soon as you total looking over this ebook.

(Cheyanne Barrows)

GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY

Book Condition: New. Publisher/Verlag: Springer, Berlin | After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features & Benefits:Breadth of coverage and unified, integrated approach to elliptic curve cryptosystemsDescribes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and TechnologyProvides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmeticDistills complex mathematics and algorithms for easy understandingIncludes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software toolsThis comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security. | ContentsList of AlgorithmsList of TablesList of FiguresAcronymsPreface 1 Introduction and Overview1.1 Cryptography basics1.2 Public-key cryptography1.2.1 RSAsystems1.2.2 Discrete logarithmsystems1.2.3 Elliptic curve systems1.3 Why elliptic curve cryptography?1.4 Roadmap1.5 Notes and further references 2 Finite Field Arithmetic2.1 Introduction to finite fields2.2 Primefieldarithmetic2.2.1 Addition and subtraction2.2.2 Integer multiplication2.2.3 Integer squaring2.2.4 Reduction2.2.5 Inversion2.2.6 NISTprimes2.3 Binary field arithmetic2.3.1 Addition2.3.2 Multiplication2.3.3 Polynomial multiplication2.3.4 Polynomial squaring2.3.5 Reduction2.3.6 Inversion and division2.4 Optimal extension field arithmetic2.4.1 Addition and subtraction2.4.2 Multiplication and reduction2.4.3 Inversion2.5 Notes andfurther references 3 Elliptic Curve Arithmetic3.1 Introduction to elliptic curves3.1.1 Simplified Weierstrass equations3.1.2 Group...

Other eBooks

JA] early childhood parenting :1-4 Genuine Special(Chinese Edition)

paperback. Book Condition: New. Ship out in 2 business day, And Fast shipping, Free Tracking number will be provided after the shipment.Paperback. Pub Date :2006-01-01 Pages: 179 Publisher: the China Pictorial Our book is all...

Save Document »

Programming in D: Tutorial and Reference (Paperback)

Ali Cehreli, 2015. Paperback. Book Condition: New. 254 x 178 mm. Language: English . Brand New Book ***** Print on Demand *****.The main aim of this book is to teach D to readers who are...

Save Document »

Programming in D

Ali Cehreli Dez 2015, 2015. Buch. Book Condition: Neu. 264x182x53 mm. This item is printed on demand - Print on Demand Neuware - The main aim of this book is to teach D to readers...

Save Document »

TJ new concept of the Preschool Quality Education Engineering the daily learning book of: new happy learning young children (2-4 years old) in small classes (3)(Chinese Edition)

paperback. Book Condition: New. Ship out in 2 business day, And Fast shipping, Free Tracking number will be provided after the shipment.Paperback. Pub Date :2005-09-01 Publisher: Chinese children before making Reading: All books are the...

Save Document »

TJ new concept of the Preschool Quality Education Engineering: new happy learning young children (3-5 years old) daily learning book Intermediate (2)(Chinese Edition)

paperback. Book Condition: New. Ship out in 2 business day, And Fast shipping, Free Tracking number will be provided after the shipment.Paperback. Pub Date :2005-09-01 Publisher: Chinese children before making Reading: All books are the...

Save Document »