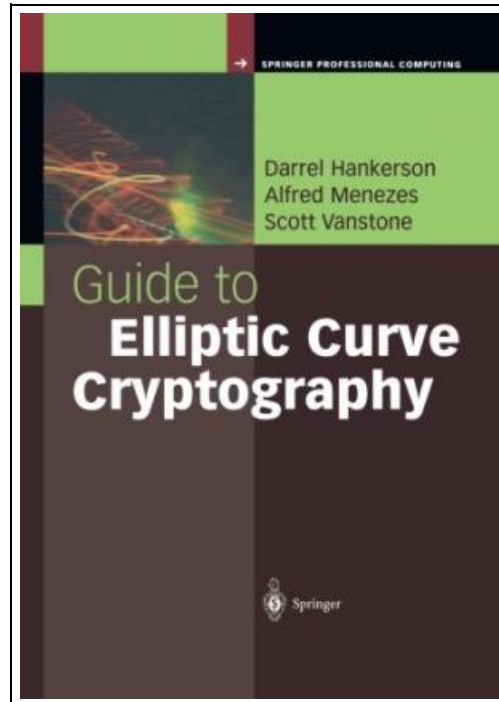


Guide to Elliptic Curve Cryptography



Filesize: 3.61 MB

Reviews

This composed pdf is excellent. We have go through and that i am certain that i am going to likely to read again once more down the road. I am just happy to explain how this is basically the very best publication i have go through within my own daily life and can be he best publication for actually.

(Anika Kertzmann)

GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY


 DOWNLOAD


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 cryptosystems Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic Distills complex mathematics and algorithms for easy understanding Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools This 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. | Contents List of Algorithms List of Tables List of Figures Acronyms Preface 1 Introduction and Overview 1.1 Cryptography basics 1.2 Public-key cryptography 1.2.1 RSA systems 1.2.2 Discrete logarithm systems 1.2.3 Elliptic curve systems 1.3 Why elliptic curve cryptography? 1.4 Roadmap 1.5 Notes and further references 2 Finite Field Arithmetic 2.1 Introduction to finite fields 2.2 Prime field arithmetic 2.2.1 Addition and subtraction 2.2.2 Integer multiplication 2.2.3 Integer squaring 2.2.4 Reduction 2.2.5 Inversion 2.2.6 NIST primes 2.3 Binary field arithmetic 2.3.1 Addition 2.3.2 Multiplication 2.3.3 Polynomial multiplication 2.3.4 Polynomial squaring 2.3.5 Reduction 2.3.6 Inversion and division 2.4 Optimal extension field arithmetic 2.4.1 Addition and subtraction 2.4.2 Multiplication and reduction 2.4.3 Inversion 2.5 Notes and further references 3 Elliptic Curve Arithmetic 3.1 Introduction to elliptic curves 3.1.1 Simplified Weierstrass equations 3.1.2 Group...


[Read Guide to Elliptic Curve Cryptography Online](#)

[Download PDF Guide to Elliptic Curve Cryptography](#)

Other eBooks



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 »](#)



Games with Books : 28 of the Best Childrens Books and How to Use Them to Help Your Child Learn - From Preschool to Third Grade

Book Condition: Brand New. Book Condition: Brand New.

[Save Document »](#)



TJ new concept of the Preschool Quality Education Engineering the daily learning book of: new happy learning young children (3-5 years) Intermediate (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 »](#)



The Religious Drama: An Art of the Church (Beginning to 17th Century) (Christian Classics Revived: 5)

Christian World Imprints/B.R. Publishing Corporation, New Delhi, India, 2014. Hardcover. Book Condition: New. Dust Jacket Condition: New. Reprinted. This classical on ageless Christian Drama aims to present periods when actually dramatic performances or `Religious Drama'...

[Save Document »](#)