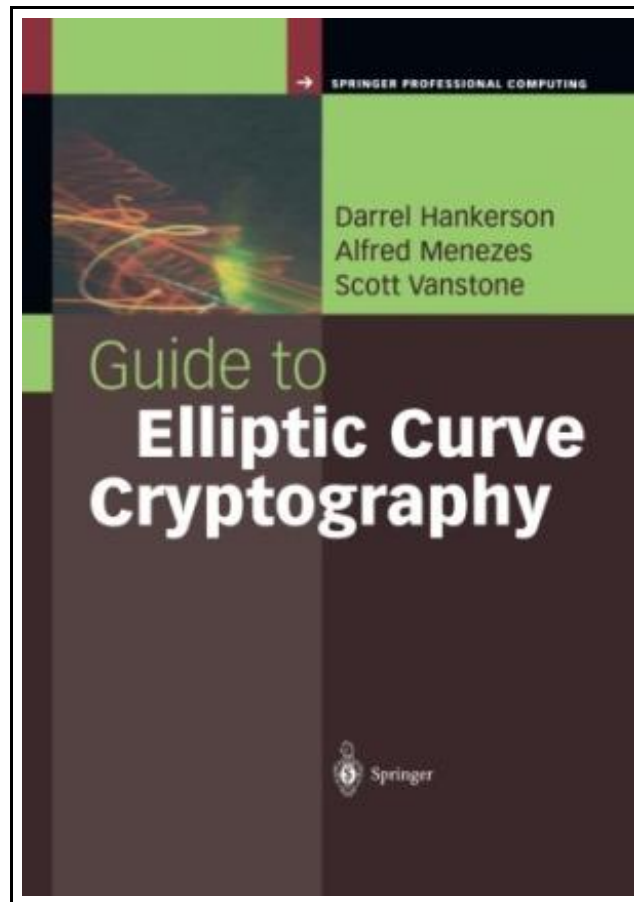# Guide to Elliptic Curve Cryptography

Filesize: 4.18 MB

Reviews

This book is really gripping and intriguing. it was writtern very perfectly and beneficial. I am easily will get a enjoyment of looking at a created ebook.

(Jaeden Stiedemann Sr.)

GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY

To read **Guide to Elliptic Curve Cryptography** eBook, you should click the web link below and save the document or have accessibility to additional information which might be relevant to GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY ebook.

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...

 Read Guide to Elliptic Curve Cryptography Online

 Download PDF Guide to Elliptic Curve Cryptography

 Download ePUB Guide to Elliptic Curve Cryptography

You May Also Like

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

Access the hyperlink below to download and read "JA] early childhood parenting :1-4 Genuine Special(Chinese Edition)" file.

Save eBook »

[PDF] Programming in D: Tutorial and Reference

Access the hyperlink below to download and read "Programming in D: Tutorial and Reference" file.

Save eBook »

[PDF] Programming in D

Access the hyperlink below to download and read "Programming in D" file.

Save eBook »

[PDF] 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)

Access the hyperlink below to download and read "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)" file.

Save eBook »

[PDF] 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)

Access the hyperlink below to download and read "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)" file.

Save eBook »

[PDF] 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)

Access the hyperlink below to download and read "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)" file.

Save eBook »

[PDF] The Knight of the Sacred Lake (Guenevere Novels)

Follow the link below to download "The Knight of the Sacred Lake (Guenevere Novels)" PDF file.

[Download ePub »](#)

[PDF] The Ghost of the Golden Gate Bridge Real Kids, Real Places

Follow the link below to download "The Ghost of the Golden Gate Bridge Real Kids, Real Places" PDF file.

[Download ePub »](#)

[PDF] The genuine book marketing case analysis of the the lam light. Yin Qihua Science Press 21.00(Chinese Edition)

Follow the link below to download "The genuine book marketing case analysis of the the lam light. Yin Qihua Science Press 21.00(Chinese Edition)" PDF file.

[Download ePub »](#)

[PDF] The Sacred Chain: History of the Jews, The

Follow the link below to download "The Sacred Chain: History of the Jews, The" PDF file.

[Download ePub »](#)

[PDF] The Mystery of the Crystal Castle Bavaria, Germany Around the World in 80 Mysteries

Follow the link below to download "The Mystery of the Crystal Castle Bavaria, Germany Around the World in 80 Mysteries" PDF file.

[Download ePub »](#)

[PDF] The Puzzle of the Indian Arrowhead Three Amigos

Follow the link below to download "The Puzzle of the Indian Arrowhead Three Amigos" PDF file.

[Download ePub »](#)