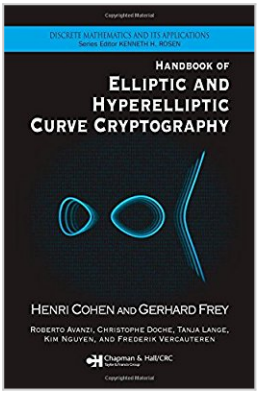

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)

From Brand: Chapman and Hall/CRC

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC

The discrete logarithm problem based on elliptic and hyperelliptic curves has gained a lot of popularity as a cryptographic primitive. The main reason is that no subexponential algorithm for computing discrete logarithms on small genus curves is currently available, except in very special cases. Therefore curve-based cryptosystems require much smaller key sizes than RSA to attain the same security level. This makes them particularly attractive for implementations on memory-restricted devices like smart cards and in high-security applications.

The **Handbook of Elliptic and Hyperelliptic Curve Cryptography** introduces the theory and algorithms involved in curve-based cryptography. After a very detailed exposition of the mathematical background, it provides ready-to-implement algorithms for the group operations and computation of pairings. It explores methods for point counting and constructing curves with the complex multiplication method and provides the algorithms in an explicit manner. It also surveys generic methods to compute discrete logarithms and details index calculus methods for hyperelliptic curves. For some special curves the discrete logarithm problem can be transferred to an easier one; the consequences are explained and suggestions for good choices are given. The authors present applications to protocols for discrete-logarithm-based systems (including bilinear structures) and explain the use of elliptic and hyperelliptic curves in factorization and primality proving. Two chapters explore their design and efficient implementations in smart cards. Practical and theoretical aspects of side-channel attacks and countermeasures and a chapter devoted to (pseudo-)random number generation round off the exposition.

The broad coverage of all- important areas makes this book a complete handbook of elliptic and hyperelliptic curve cryptography and an invaluable reference to anyone interested in this exciting field.

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications)

From Brand: Chapman and Hall/CRC

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC

The discrete logarithm problem based on elliptic and hyperelliptic curves has gained a lot of popularity as a cryptographic primitive. The main reason is that no subexponential algorithm for computing discrete logarithms on small genus curves is currently available, except in very special cases. Therefore curve-based cryptosystems require much smaller key sizes than RSA to attain the same security level. This makes them particularly attractive for implementations on memory-restricted devices like smart cards and in high-security applications.

The **Handbook of Elliptic and Hyperelliptic Curve Cryptography** introduces the theory and algorithms involved in curve-based cryptography. After a very detailed exposition of the mathematical background, it provides ready-to-implement algorithms for the group operations and computation of pairings. It explores methods for point counting and constructing curves with the complex multiplication method and provides the algorithms in an explicit manner. It also surveys generic methods to compute discrete logarithms and details index calculus methods for hyperelliptic curves. For some special curves the discrete logarithm problem can be transferred to an easier one; the consequences are explained and suggestions for good choices are given. The authors present applications to protocols for discrete-logarithm-based systems (including bilinear structures) and explain the use of elliptic and hyperelliptic curves in factorization and primality proving. Two chapters explore their design and efficient implementations in smart cards. Practical and theoretical aspects of side-channel attacks and countermeasures and a chapter devoted to (pseudo-)random number generation round off the exposition.

The broad coverage of all- important areas makes this book a complete handbook of elliptic and hyperelliptic curve cryptography and an invaluable reference to anyone interested in this exciting field.

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC Bibliography

- Rank: #2295947 in Books
- Brand: Brand: Chapman and Hall/CRC
- Published on: 2005-07-19
- Original language: English
- Number of items: 1
- Dimensions: 10.20" h x 1.95" w x 7.28" l, 3.62 pounds
- Binding: Hardcover
- 842 pages

Editorial Review

Review

… very comprehensive coverage of this vast subject area … a useful and essential treatise for anyone involved in elliptic curve algorithms … this book offers the opportunity to grasp the ECC technology with a diversified and comprehensive perspective. … This book will remain on my shelf for a long time and will land on my desk on many occasions, if only because the coverage of the issues common to factoring and discrete log cryptosystems is excellent.
?IACR Book Reviews, June 2011

… the book is designed for people who are working in the area and want to learn more about a specific issue. The chapters are written to be relatively independent so that readers can focus on the part of interest for them. Such readers will be grateful for the excellent index and extensive bibliography. … the handbook covers a wide range of topics and will be a valuable reference for researchers in curve-based cryptography.
?Steven D. Galbraith, Mathematical Reviews, Issue 2007f

Users Review

From reader reviews:

William Grimm:

Book is usually written, printed, or outlined for everything. You can learn everything you want by a e-book. Book has a different type. As we know that book is important matter to bring us around the world. Close to that you can your reading skill was fluently. A book Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) will make you to become smarter. You can feel much more confidence if you can know about every thing. But some of you think which open or reading the book make you bored. It's not make you fun. Why they can be thought like that? Have you searching for best book or ideal book with you?

Joseph Cash:

Now a day individuals who Living in the era everywhere everything reachable by talk with the internet and the resources inside can be true or not need people to be aware of each info they get. How people have to be smart in receiving any information nowadays? Of course the answer is reading a book. Reading a book can help persons out of this uncertainty Information especially this Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) book as this book offers you rich data and knowledge. Of course the details in this book hundred percent guarantees there is no doubt in it you probably know this.

Bradley Sparks:

In this era which is the greater individual or who has ability to do something more are more special than other. Do you want to become one of it? It is just simple method to have that. What you should do is just spending your time not very much but quite enough to experience a look at some books. One of several books in the top list in your reading list is actually Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications). This book which is qualified as The Hungry Hillsides can get you closer in turning out to be precious person. By looking right up and review this reserve you can get many advantages.

Joseph Davis:

Guide is one of source of knowledge. We can add our understanding from it. Not only for students but additionally native or citizen have to have book to know the change information of year to help year. As we know those publications have many advantages. Beside all of us add our knowledge, also can bring us to around the world. From the book Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) we can take more advantage. Don't someone to be creative people? To get creative person must love to read a book. Simply choose the best book that acceptable with your aim. Don't always be doubt to change your life at this book Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications). You can more pleasing than now.

Read Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC for online ebook

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC books to read online.

Online Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC ebook PDF download

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC Doc

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC Mobipocket

Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC EPub

BK5LINPW4U7: Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications) From Brand: Chapman and Hall/CRC