Handbook Of Elliptic And Hyperelliptic Curve Cryptography Discrete Mathematics And Its Applications

Thank you for reading **handbook of elliptic and hyperelliptic curve cryptography discrete mathematics and its applications**. As you may know, people have look numerous times for their chosen readings like this handbook of elliptic and hyperelliptic curve cryptography discrete mathematics and its applications, but end up in infectious downloads.
Rather than reading a good book with a cup of coffee in the afternoon, instead they juggled with some harmful virus inside their computer.

handbook of elliptic and hyperelliptic curve cryptography discrete mathematics and its applications is available in our digital library an online access to it is set as public so you can get it instantly.
Our books collection spans in multiple countries, allowing you to get the most less latency time to download any of our books like this one.
Merely said, the handbook of elliptic and hyperelliptic curve cryptography discrete mathematics and its applications is universally compatible with any devices to read

Handbook of Elliptic and Hyperelliptic Curve Cryptography - Henri Cohen 2005-07-19
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.
Pairing-Based Cryptography - Pairing 2009 - Hovav Shacham 2009-07-31

This book constitutes the refereed proceedings of the Third International Conference on Pairing-Based Cryptography, Pairing 2009, held in Palo Alto, CA, USA, in August 2009. The 16 full papers presented were carefully reviewed and selected from 38 submissions. The papers are organized in topical sections on signature security, curves, pairing computation, non-interactive zero-knowledge systems and applications, group signatures, and protocols.

Advances in Cryptology - EUROCRYPT 2009 - Antoine Joux 2009-04-20

This book constitutes the refereed proceedings of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2009, held in Cologne, Germany, in April 2009. The 33 revised full papers presented together with 1 invited lecture were carefully reviewed and selected from 148 submissions. The papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications. The papers are organized in topical sections on security, proofs, and models, hash cryptanalysis, group and broadcast encryption, cryptosystems, cryptanalysis, side channels, curves, and randomness.

Functional Encryption - Khairol Amali Bin Ahmad 2021

This book provides awareness of methods used for functional encryption in the academic and professional communities. The book covers functional encryption algorithms and its modern applications in developing secure systems via entity authentication, message authentication, software security, cyber security, hardware security, Internet of Thing (IoT), cloud security, smart card technology, CAPTCHA, digital signature and digital watermarking. Explains the latest functional encryption algorithms in a simple way with examples; Includes applications of functional encryption in information security, application security, and network security; Relevant to academics, research scholars, software developers, etc.

Elliptic Curves - Lawrence C. Washington 2008-04-03

Like its bestselling predecessor, Elliptic Curves: Number Theory and Cryptography, Second Edition develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications. With additional exercises, this edition offers more comprehensive coverage of the fundamental theory, techniques, and applications of elliptic curves. New to the Second Edition Chapters on isogenies and hyperelliptic curves A discussion of alternative coordinate systems, such as projective, Jacobian, and Edwards coordinates, along with related computational issues A more complete treatment of the Weil and Tate–Lichtenbaum pairings Doud’s analytic method for computing torsion on elliptic curves over Q An explanation of how to perform calculations with elliptic curves in several popular computer algebra systems Taking a basic approach to elliptic curves, this accessible book prepares readers to tackle more advanced problems in the field. It introduces elliptic curves over finite fields early in the text, before moving on to interesting applications, such as cryptography, factoring, and primality testing. The book also discusses the use of elliptic curves in Fermat’s Last Theorem. Relevant abstract algebra material on group theory and fields can be found in the appendices.

Modern Computer Arithmetic - Richard P. Brent 2010-11-25

Modern Computer Arithmetic focuses on arbitrary-precision algorithms for efficiently performing arithmetic operations such as addition, multiplication and division, and their connections to topics such as modular arithmetic, greatest common divisors, the Fast Fourier Transform (FFT), and the computation of elementary and special functions. Brent and Zimmermann present algorithms that are ready to implement in your favourite language, while keeping a high-level description and avoiding too low-level or machine-dependent details. The book is intended for anyone interested in the design and implementation of efficient high-precision algorithms for computer arithmetic, and more generally efficient multiple-precision numerical algorithms. It may also be used in a graduate course in mathematics or computer science, for which exercises are included. These vary considerably in difficulty, from easy to small research projects, and expand on topics discussed in the text. Solutions to selected exercises are available from the authors.

Algorithmic Number Theory - Alf J. van der Poorten 2008-05-07
This book constitutes the refereed proceedings of the 8th International Algorithmic Number Theory Symposium, ANTS 2008, held in Banff, Canada, in May 2008. The 28 revised full papers presented together with 2 invited papers were carefully reviewed and selected for inclusion in the book. The papers are organized in topical sections on elliptic curves cryptology and generalizations, arithmetic of elliptic curves, integer factorization, K3 surfaces, number fields, point counting, arithmetic of function fields, modular forms, cryptography, and number theory.

Arithmetic of Finite Fields - Claude Carlet 2007-06-11
This book constitutes the refereed proceedings of the First International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, held in Madrid, Spain in June 2007. The 27 revised full papers presented were carefully reviewed and selected from 94 submissions. The papers are organized in topical sections on structures in finite fields, efficient implementation and architectures, efficient finite field arithmetic, classification and construction of mappings over finite fields, curve algebra, cryptography, codes, and discrete structures.

Modern Cryptography and Elliptic Curves: A Beginner’s Guide - Thomas R. Shemanske 2017-07-31
This book offers the beginning undergraduate student some of the vista of modern mathematics by developing and presenting the tools needed to gain an understanding of the arithmetic of elliptic curves over finite fields and their applications to modern cryptography. This gradual introduction also makes a significant effort to teach students how to produce or discover a proof by presenting mathematics as an exploration, and at the same time, it provides the necessary mathematical underpinnings to investigate the practical and implementation side of elliptic curve cryptography (ECC). Elements of abstract algebra, number theory, and affine and projective geometry are introduced and developed, and their interplay is exploited. Algebra and geometry combine to characterize congruent numbers via rational points on the unit circle, and group law for the set of points on an elliptic curve arises from geometric intuition provided by Bézout's theorem as well as the construction of projective space. The structure of the unit group of the integers modulo a prime explains RSA encryption, Pollard's method of factorization, Diffie–Hellman key exchange, and ElGamal encryption, while the group of points of an elliptic curve over a finite field motivates Lenstra's elliptic curve factorization method and ECC. The only real prerequisite for this book is a course on one-variable calculus; other necessary mathematical topics are introduced on-the-fly. Numerous exercises further guide the exploration.

An Introduction to Cryptography - Richard A. Mollin 2006-09-18
Continuing a bestselling tradition, An Introduction to Cryptography, Second Edition provides a solid foundation in cryptographic concepts that features all of the requisite background material on number theory and algorithmic complexity as well as a historical look at the field. With numerous additions and restructured material, this edition

Mathematics of Public Key Cryptography - Steven D. Galbraith 2012-03-15
This advanced graduate textbook gives an authoritative and insightful description of the major ideas and techniques of public key cryptography.

Algebraic Geometry and Its Applications -

Cryptography and Security: From Theory to Applications - David Naccache 2012-02-21
This Festschrift volume, published in honor of Jean-Jaques Quisquater on the occasion of his 65th Birthday, contains 33 papers from colleagues all over the world and deals with all the fields to which Jean-Jaques dedicated his work during his academic career. Focusing on personal tributes and re-visits of Jean-Jaques Quisquater's legacy, the volume addresses the following central topics: symmetric and asymmetric cryptography, side-channels attacks, hardware and implementations, smart cards, and information security. In addition there are four more contributions just "as diverse as Jean-Jacques' scientific interests".

Algebraic Aspects of Cryptography - Neal Koblitz 2012-12-06
From the reviews: "This is a textbook in cryptography with emphasis on algebraic methods. It is supported by many exercises (with answers)

making it appropriate for a course in mathematics or computer science. [...] Overall, this is an excellent expository text, and will be very useful to both the student and researcher." Mathematical Reviews

Handbook of Information and Communication Security - Peter Stavroulakis 2010-02-23

At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called “Y2K” issue. Te Y2K scare was the fear that c- puter networks and the systems that are controlled or operated by sofware would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several Computer Emergency Response Teams (CERTs) around the world that now work - operatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment. Te terrorist attacks of 11 September 2001 raised security concerns to a new level. Te - ternational community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about - tential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communi- tions conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security. Te ?rst editor was intimately involved with security for the Athens Olympic Games of 2004.

Cryptography Made Simple - Nigel Smart 2015-11-12

In this introductory textbook the author explains the key topics in cryptography. He takes a modern approach, where defining what is meant by "secure" is as important as creating something that achieves that goal, and security definitions are central to the discussion throughout. The author balances a largely non-rigorous style — many proofs are sketched only — with appropriate formality and depth. For example, he uses the terminology of groups and finite fields so that the reader can understand both the latest academic research and "real-world" documents such as application programming interface descriptions and cryptographic standards. The text employs colour to distinguish between public and private information, and all chapters include summaries and suggestions for further reading. This is a suitable textbook for advanced undergraduate and graduate students in computer science, mathematics and engineering, and for self-study by professionals in information security. While the appendix summarizes most of the basic algebra and notation required, it is assumed that the reader has a basic knowledge of discrete mathematics, probability, and elementary calculus.

Mathematical Aspects of Logic Programming Semantics - Pascal Hitzler 2016-04-19

Covering the authors' own state-of-the-art research results, this book presents a rigorous, modern account of the mathematical methods and tools required for the semantic analysis of logic programs. It significantly extends the tools and methods from traditional order theory to include nonconventional methods from mathematical analysis that depend on topology, domain theory, generalized distance functions, and associated fixed-point theory. The authors closely examine the interrelationships between various semantics as well as the integration of logic programming and connectionist systems/neural networks.

Elliptic Curves and Their Applications to Cryptography - Andreas Enge 2012-12-06

Since their invention in the late seventies, public key cryptosystems have become an indispensable asset in establishing private and secure electronic communication, and this need, given the tremendous growth of the Internet, is likely to continue growing. Elliptic curve cryptosystems represent the state of the art for such systems. Elliptic Curves and Their Applications to Cryptography: An Introduction provides a comprehensive and self-contained introduction to elliptic curves and how they are employed to secure public key cryptosystems. Even though the elegant mathematical theory underlying cryptosystems is considerably more involved than for other systems, this text requires the reader to have only an elementary knowledge of basic algebra. The text nevertheless leads to problems at the forefront of current research, featuring chapters on point counting algorithms and security issues. The Adopted unifying approach treats with equal care elliptic curves over fields of even characteristic, which are especially suited for hardware implementations, and curves over fields of odd characteristic, which have traditionally received more attention. Elliptic Curves and Their Applications: An Introduction has been used successfully for teaching advanced undergraduate courses. It will be of greatest interest to mathematicians, computer scientists, and engineers who are curious about elliptic curve cryptography in practice, without losing the beauty of the underlying mathematics.

Process-Driven SOA - Carsten Hentrich 2016-04-19

Process-Driven SOA: Patterns for Aligning Business and IT supplies detailed guidance on how to design and build software architectures that follow the principles of business-IT alignment. It illustrates the design process using proven patterns that address complex business/technical scenarios, where integrated concepts of service-oriented architect

Handbook of Elliptic and Hyperelliptic Curve Cryptography - Henri Cohen 2005-07-19

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 Applied Cryptography - Alfred J. Menezes 2018-12-07

Cryptography, in particular public-key cryptography, has emerged in the last 20 years as an important discipline that is not only the subject of an enormous amount of research, but provides the foundation for information security in many applications. Standards are emerging to meet the demands for cryptographic protection in most areas of data communications. Public-key cryptographic techniques are now in widespread use, especially in the financial services industry, in the public sector, and by individuals for their personal privacy, such as in electronic mail. This Handbook will serve as a valuable reference for the novice as well as for the expert who needs a wider scope of coverage within the area of cryptography. It is a necessary and timely guide for professionals who practice the art of cryptography. The Handbook of Applied Cryptography provides a treatment that is multifunctional: It serves as an introduction to the more practical aspects of both conventional and public-key cryptography It is a valuable source of the latest techniques and algorithms for the serious practitioner It provides an integrated treatment of the field, while still presenting each major topic as a self-contained unit It provides a mathematical treatment to accompany practical discussions It contains enough abstraction to be a valuable reference for theoreticians while containing enough detail to actually allow implementation of the algorithms discussed Now in its third printing, this is the definitive cryptography reference that the novice as well as experienced developers, designers, researchers, engineers, computer scientists, and mathematicians alike will use.

Differentiation and Integration - W. Bolton 2016-04-15

This book is concerned with the principles of differentiation and integration. The principles are then applied to solve engineering problems. A familiarity with basic algebra and a basic knowledge of common functions, such as polynomials, trigonometric, exponential, logarithmic and hyperbolic is assumed but reference material on these is included in an appendix.

Understanding Cryptography - Christof Paar 2009-11-27

Cryptography is now ubiquitous – moving beyond the traditional environments, such as government communications and banking systems, we see cryptographic techniques realized in Web browsers, e-mail programs, cell phones, manufacturing systems, embedded software, smart buildings, cars, and even medical implants. Today's designers need a comprehensive understanding of applied cryptography. After an introduction to cryptography and data security, the authors explain the main techniques in modern cryptography, with chapters addressing stream ciphers, the Data Encryption Standard (DES) and 3DES, the Advanced Encryption Standard (AES), block ciphers, the RSA cryptosystem, public-key cryptosystems based on the discrete logarithm problem, elliptic-curve cryptography (ECC), digital signatures, hash functions, Message Authentication Codes (MACs), and methods for key establishment, including certificates and public-key infrastructure (PKI). Throughout the book, the authors focus on communicating the essentials and keeping the mathematics to a minimum, and they move quickly from explaining the foundations to describing practical implementations, including recent topics such as lightweight ciphers for RFIDs and mobile devices, and current key-length recommendations. The authors have considerable experience teaching applied cryptography to engineering and computer science students and to professionals, and they make extensive use of examples, problems, and chapter reviews, while the book’s website offers slides, projects and links to further resources. This is a suitable textbook for graduate and advanced undergraduate courses and also for self-study by engineers.

Cryptographic Hardware and Embedded Systems - CHES 2007 - Pascal Paillier 2007-08-23

This book constitutes the refereed proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2007. The 31 revised full papers cover side channels, low resources, hardware attacks and countermeasures, special purpose hardware, efficient algorithms for embedded processors, efficient hardware, trusted computing.

Elliptic Tales - Avner Ash 2014-10-19

Elliptic Tales describes the latest developments in number theory by looking at one of the most exciting unsolved problems in contemporary mathematics--the Birch and Swinnerton-Dyer Conjecture. The Clay Mathematics Institute is offering a prize of $1 million to anyone who can discover a general solution to the problem. The key to the conjecture lies in elliptic curves, which are cubic equations in two variables. These equations may appear simple, yet they arise from some very deep--and often very mystifying--mathematical ideas. Using only basic algebra and calculus while presenting numerous eye-opening examples, Ash and Gross make these ideas accessible to general readers, and, in the process, venture to the very frontiers of modern mathematics. Along the way, they give an informative and entertaining introduction to some of the most profoundmay appear simple, yet they arise from some very deep--and often very mystifying--mathematical ideas. Using only basic algebra and calculus while presenting numerous eye-opening examples, Ash and Gross make these ideas accessible to general readers, and, in the process, venture to the very frontiers of modern mathematics. Along the way, they give an informative and entertaining introduction to some of the most profound discoveries of the last three centuries in algebraic geometry, abstract algebra, and number theory. They demonstrate how mathematics grows more abstract to tackle ever more challenging problems, and how each new generation of mathematicians builds on the accomplishments of those who preceded them. Ash and Gross fully explain how the Birch and Swinnerton-Dyer Conjecture sheds light on the number theory of elliptic curves, and how it provides a beautiful and startling connection between two very different objects arising from an elliptic curve, one based on calculus, the other on algebra.

Cryptographic Hardware and Embedded Systems – CHES 2008 - Elisabeth Oswald 2008-07-18

by Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp and Christopher Wolf. The purpose of the award is to formally acknowledge excellence in research. We would like to c- gratulate the authors of these two papers.

Rational Points on Elliptic Curves - Joseph H. Silverman 2013-04-17

The theory of elliptic curves involves a blend of algebra, geometry, analysis, and number theory. This book stresses this interplay as it develops the basic theory, providing an opportunity for readers to appreciate the unity of modern mathematics. The book’s accessibility, the informal writing style, and a wealth of exercises make it an ideal introduction for those interested in learning about Diophantine equations and arithmetic geometry.

Crypto Dictionary - Jean-Philippe Aumasson 2021-03-16

Rigorous in its definitions yet easy to read, Crypto Dictionary covers the field of cryptography in an approachable, and sometimes humorous way. Expand your mind and your crypto knowledge with the ultimate desktop dictionary for all things cryptography. Written by a renowned cryptographer for experts and novices alike, Crypto Dictionary is rigorous in its definitions, yet easy to read and laced with humor. Flip to any random page to find something new, interesting, or mind-boggling, such as: • A survey of crypto algorithms both widespread and niche, from RSA and DES to the USSR’s GOST cipher • Trivia from the history of cryptography, such as the MINERVA backdoor in Crypto AG’s encryption algorithms • An explanation of why the reference to the Blowfish cipher in the TV show 24 makes absolutely no sense • Types of cryptographic protocols like zero-knowledge; security; and proofs of work, stake, and resource • A polemic against referring to cryptocurrency as “crypto” • Discussions of numerous cryptographic attacks, including slide and biclique The book also looks toward the future of cryptography, with discussions of the threat quantum computing poses to current cryptosystems and a nod to post-quantum algorithms, such as lattice-based cryptographic schemes. With hundreds of incisive entries organized alphabetically, Crypto Dictionary is the crypto go-to guide you’ll always want within reach.

The Arithmetic of Elliptic Curves - Joseph H. Silverman 2013-03-09

The theory of elliptic curves is distinguished by its long history and by the diversity of the methods that have been used in its study. This book treats the arithmetic approach in its modern formulation, through the use of basic algebraic number theory and algebraic geometry. Following a brief discussion of the necessary algebro-geometric results, the book proceeds with an exposition of the geometry and the formal group of elliptic curves, elliptic curves over finite fields, the complex numbers, local fields, and global fields. Final chapters deal with integral and rational points, including Siegels theorem and explicit computations for the curve Y = X + DX, while three appendices conclude the whole: Elliptic Curves in Characteristics 2 and 3, Group Cohomology, and an overview of more advanced topics.

Advances in Cryptology – ASIACRYPT 2007 - Kaoru Kurosawa 2007-11-05

This book constitutes the refereed proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2007, held in Kuching, Malaysia, in December 2007. The papers are organized in topical sections on number theory and elliptic curve, protocol, hash function design, group/broadcast cryptography, mac and implementation, multiparty computation, block ciphers, foundation, public key encryption, and cryptanalysis.

Guide to Elliptic Curve Cryptography - Darrel Hankerson 2006-06-01

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.

Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems - Thomas Wollinger 2004

Public Key Cryptography - PKC 2010 - Phong Q. Nguyen 2010-05-15

Annotation This book constitutes the refereed proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography, PKC 2010, held in Paris, France, in May 2010. The 29 revised full papers presented were carefully reviewed and selected from 145 submissions. The papers are organized in topical sections on encryption; cryptanalysis; protocols; network coding; tools; elliptic curves; lossy trapdoor functions; discrete logarithm; and signatures.

Advances in Elliptic Curve Cryptography - Ian F. Blake 2005-04-25

Since the appearance of the authors' first volume on elliptic curve cryptography in 1999 there has been tremendous progress in the field. In some topics, particularly point counting, the progress has been spectacular. Other topics such as the Weil and Tate pairings have been applied in new and important ways to cryptographic protocols that hold great promise. Notions such as provable security, side channel analysis and the Weil descent technique have also grown in importance. This second volume addresses these advances and brings the reader up to date. Prominent contributors to the research literature in these areas have provided articles that reflect the current state of these important topics. They are divided into the areas of protocols, implementation techniques, mathematical foundations and pairing based cryptography. Each of the topics is presented in an accessible, coherent and consistent manner for a wide audience that will include mathematicians, computer scientists and engineers.

Advances in Cryptology - ASIACRYPT 2008 - Josef Pawel Pieprzyk 2008-12-02

This book constitutes the refereed proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2008, held in Melbourne, Australia, in December 2008. The 33 revised full papers presented together with the abstract of 1 invited lecture were carefully reviewed and selected from 208 submissions. The papers are organized in topical sections on muliti-party computation, cryptographic protocols, cryptographic hash functions, public-key cryptograhy, lattice-based cryptography, private-key cryptograhy, and analysis of stream ciphers.

Algorithmic Cryptanalysis - Antoine Joux 2009-06-15

Illustrating the power of algorithms, Algorithmic Cryptanalysis describes algorithmic methods with cryptographically relevant examples. Focusing on both private- and public-key cryptographic algorithms, it presents each algorithm either as a textual description, in pseudo-code, or in a C code program. Divided into three parts, the book begins with a short introduction to cryptography and a background chapter on elementary number theory and algebra. It then moves on to algorithms, with each chapter in this section dedicated to a single topic and often illustrated with simple cryptographic applications. The final part addresses more sophisticated cryptographic applications, including LFSR-based stream ciphers and index calculus methods. Accounting for the impact of current computer architectures, this book explores the algorithmic and implementation aspects of cryptanalysis methods. It can serve as a handbook of algorithmic methods for cryptographers as well as a textbook for undergraduate and graduate courses on cryptanalysis and cryptography.

Elliptic Functions and Elliptic Integrals - Viktor Vasil_evich Prasolov 1997-09-16

This book is devoted to the geometry and arithmetic of elliptic curves and to elliptic functions with applications to algebra and number theory. It includes modern interpretations of some famous classical algebraic theorems such as Abel's theorem on the lemniscate and Hermite's solution of the fifth degree equation by means of theta functions. Suitable as a text, the book is self-contained and assumes as prerequisites only the standard one-year courses of algebra and analysis.

Handbook of Finite Fields - Gary L. Mullen 2013-06-17

Poised to become the leading reference in the field, the Handbook of Finite Fields is exclusively devoted to the theory and applications of finite fields. More than 80 international contributors compile state-of-the-art research in this definitive handbook. Edited by two renowned researchers, the book uses a uniform style and format throughout and

Elliptic Curves in Cryptography - I. Blake 1999-07-08

This book explains the mathematics behind practical implementations of elliptic curve systems.

Cryptographic Engineering - Cetin Kaya Koc 2008-12-11

This book is for engineers and researchers working in the embedded hardware industry. This book addresses the design aspects of cryptographic hardware and embedded software. The authors provide tutorial-type material for professional engineers and computer information specialists.