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

This book constitutes the refereed proceedings of the 10th Interntaional Workshop on Cryptographic Hardware and Embedded Systems, CHES 2008, held in Washington, D.C., USA, during August 10-13, 2008. The book contains 2 invited talks and 27 revised full papers which were carefully reviewed and selected from 107 submissions. The papers are organized in topical sections on side

channel analysis, implementations, fault analysis, random number generation, and cryptography and cryptanalysis.

This book constitutes the refereed proceedings of the 5th International Conference on Pairing-Based Cryptography, Pairing 2012, held in Cologne, Germany, in May 2012. The 17 full papers for presentation at the academic track and 3 full papers for presentation at the industrial track were carefully reviewed and selected from 49 submissions. These papers are presented together with 6 invited talks. The contributions are organized in topical sections on: algorithms for pairing computation, security models for encryption, functional encryption, implementations in hardware and

software, industry track, properties of pairings, and signature schemes and applications.

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. 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.

14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008

Encyclopedia of Cryptography and Security

An Introduction to Cryptography

15th Annual International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, 2008

An Introduction

Number Theory and Cryptography, Second Edition

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.

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.
Expanded into two volumes, the Second Edition of Springer's Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over

300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition's base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition's editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries,

the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text's practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of

Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data

Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

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

Computations in Algebraic Geometry with Macaulay 2

Handbook of Finite Fields

Algorithmic Cryptanalysis

Elliptic Curves

Research Directions in Number Theory

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.

In an age of explosive worldwide

growth of electronic data storage and communications, effective protection of information has become a critical requirement. When used in coordination with other tools for ensuring information security, cryptography in all of its applications, including data confidentiality, data integrity, and user authentication, is a most powerful tool for protecting information. This book presents a collection of research work in the field of cryptography. It discusses some of the critical challenges that are being faced by the current computing world and also describes some mechanisms to defend against these challenges. It is a valuable source of knowledge for researchers, engineers, graduate and doctoral students working in the field of cryptography. It will also be useful for faculty members of graduate

schools and universities.

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.

This book presents algorithmic tools for algebraic geometry, with experimental applications. It also introduces Macaulay 2, a computer algebra system supporting research in algebraic geometry, commutative algebra, and their applications. The algorithmic tools presented here are designed to serve readers wishing to bring such tools to bear on their own problems. The first part of the book covers Macaulay 2 using concrete applications; the second emphasizes details of the mathematics.

Pairing-Based Cryptography - Pairing 2008

Modern Cryptography and Elliptic Curves: A Beginner's Guide

Elliptic Functions and Elliptic Integrals

Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition

Guide to Elliptic Curve Cryptography

This volume is a collection of papers on number theory which evolved out of the workshop WIN--Women In Numbers, held November 2-7, 2008, at the Banff International Research Station (BIRS) in Banff, Alberta, Canada. It includes articles showcasing outcomes from collaborative research initiated during the workshop as well as survey papers aimed at introducing graduate students and recent PhDs to important research topics in number theory. The contributions in this volume span a wide range of topics in arithmetic geometry and algebraic, algorithmic, and analytic number theory. Clusters of papers

center around the four topics of moduli spaces and Shimura curves, curves and Jacobians over finite fields, Galois covers of function fields in positive characteristic, and zeta functions of graphs, with a fifth group of three individual articles on modular forms, Iwasawa theory, and Galois representations, respectively. The workshop and this volume are part of a broader WIN initiative, whose goals are to highlight and increase the research activities of women in number theory and to train female graduate students in number theory and related fields.

You are holding the proceedings of Eurocrypt 2009, the 28th Annual

Inter- tional Conferenceon the Theoryand Applications of CryptographicTechniques. This conference was organized by the International Association for Cryptologic Research in cooperation with the Horst Gort] z Institute for IT-Security at the Ruhr-Universit] at Bochum. The local organization received additional support from several sponsors: Horst G] ortz Stiftung, Deutsche Forschungsgemeinschaft, Bochum 2015, Secunet, NXP, IET, Taylor & Francis, AuthentiDate. The c- ference was held in Cologne, Germany. The Eurocrypt 2009 Program Committee (PC) consisted of 29 members, listed on the next

page. There were 148 submissions and 33 were selected to - pear in this volume.Eachsubmissionwasassigned to at leastthreePCmembers and reviewed anonymously. During the review process, the PC members were assisted by 131 external reviewers.Once the reviews were available, the comm- tee discussed the papers in depth using the EasyChair conference management system. The authors of accepted papers were given ?ve weeks to prepare the- nalversionsincluded in theseproceedings.Therevisedpapersw erenot reviewed again and their authors bear the responsibility for their content. Inadditiontothepapers includedinthisvolume,

theconferencealsofeatured aPostera ndaRumpsession.Thelistofpresented postersappearsinthisvolume before the table of contents. Dan Bernstein served as the Chair of the Rump session. The conference also had the pleasure of hearing invited talks by Sha? Goldwasser and Phillip Rogaway.

Blockchain is emerging as a powerful technology, which has attracted the wider attention of all businesses across the globe. In addition to financial businesses, IT companies and business organizations are keenly analyzing and adapting this technology for improving business processes. Security is the primary enterprise

application. There are other crucial applications that include creating decentralized applications and smart contracts, which are being touted as the key differentiator of this pioneering technology. The power of any technology lies in its ecosystem. Product and tool vendors are building and releasing a variety of versatile and robust toolsets and platforms in order to speed up and simplify blockchain application development, deployment and management. There are other infrastructure-related advancements in order to streamline blockchain adoption. Cloud computing, big data analytics, machine and deep learning

algorithm, and connected and embedded devices all are driving blockchain application development and deployment. Blockchain Technology and Applications illustrates how blockchain is being sustained through a host of platforms, programming languages, and enabling tools. It examines: Data confidential, integrity, and authentication Distributed consensus protocols and algorithms Blockchain systems design criteria and systems interoperability and scalability Integration with other technologies including cloud and big data It also details how blockchain is being blended with cloud computing, big data analytics

and IoT across all industry verticals. The book gives readers insight into how this path-breaking technology can be a value addition in several business domains ranging from healthcare, financial services, government, supply chain and retail.

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

First International Workshop, WAIFI 2007, Madrid, Spain, June 21-22, 2007, Proceedings
Mathematical Aspects of Logic Programming Semantics
Mathematics of Public Key Cryptography
Handbook of Applied Cryptography
Modern Computer Arithmetic
Theory and Applications of Models of Computation

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.

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.

This volume constitutes the selected papers of the 15th Annual International Workshop on Selected Areas in Cryptography, SAC 2008, held in Sackeville, New Brunswick, Canada, in August 14-15, 2008. From a total of 99 technical papers, 27 papers were accepted for presentation at the workshop. They cover the following topics: elliptic and hyperelliptic arithmetic, block ciphers, hash functions, mathematical aspects of applied cryptography, stream ciphers cryptanalysis, cryptography with algebraic curves, curve-based primitives in hardware.

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 - ASIACRYPT 2008

Win-- Women in Numbers

Moduli of Curves

Modern Computer Algebra

Software Technology and Engineering

Advances in Elliptic Curve Cryptography

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.
This book constitutes the refereed proceedings of the 4th International Conference on Theory and Applications of Models of Computation, TAMC 2007, held in Shanghai, China in May 2007. The 67 revised full papers presented together with 2 plenary lectures were carefully reviewed and selected from over 500 submissions. All major areas in computer science, mathematics (especially logic) and

the physical sciences particularly with regard to computation and computability theory are addressed. The papers ? featuring this crossdisciplinary character ? particularly focus on algorithms, complexity and computability theory, giving the conference a special flavor and distinction.

This handbook provides a complete reference on elliptic and hyperelliptic curve cryptography. Addressing

every aspect of the field, the book contains all of the background necessary to understand the theory and security of cryptosystems as well as the algorithms that can be used to implement them. This second edition features the latest developments on pairing-based cryptography, new ideas on index-calculus attacks, improved algorithms for genus-2 arithmetic, and a number of other new additions. It also includes many

new applications and provides better explanations on some of the more mathematical presentations.

Handbook of Elliptic and Hyperelliptic Curve CryptographyCRC Press

4th International Conference, TAMC 2007, Shanghai, China, May 22-25, 2007, Proceedings

Cryptographic Hardware and Embedded Systems – CHES 2008

Theory and Practice of Cryptography and Network Security Protocols and Technologies

Blockchain Technology and Applications

Pairing-Based Cryptography -- Pairing 2012

Advances in Cryptology - EUROCRYPT 2009

This advanced graduate textbook gives an authoritative and insightful description of the major ideas and techniques of public key cryptography.

Engineers and physicists are more and more encountering integrations involving nonelementary integrals

and higher transeendental functions. Such integrations frequently involve (not always in immediately re cognizable form) elliptic functions and elliptic integrals. The numerous books written on elliptic integrals, while of great value to the student or mathematician, are not especially suitable for the scientist whose primary objective is the ready evaluation of the integrals that occur in

his practical problems. As a result, he may entirely avoid problems which lead to elliptic integrals, or is likely to resort to graphical methods or other means of approximation in dealing with all but the siruplest of these integrals. It became apparent in the course of my work in theoretical aero dynamics that there was a need for a handbook embodying in convenient form a comprehensive table of elliptic

integrals together with auxiliary formulas and numerical tables of values. Feeling that such a book would save the engineer and physicist much valuable time, I prepared the present volume.

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.

Image Processing for Cinema presents a detailed overview of image processing techniques that are used in practice in digital cinema. The book shows how image processing has become ubiquitous in movie-making, from shooting to exhibition. It covers all the ways in which image processing algorithms are used to enhance,

restore, adapt, and convert moving images. These techniques and algorithms make the images look as good as possible while exploiting the capabilities of cameras, projectors, and displays. The author focuses on the ideas behind the methods, rather than proofs and derivations. The first part of the text presents fundamentals on optics and color. The second part explains how cameras work and details

all the image processing algorithms that are applied in-camera. With an emphasis on state-of-the-art methods that are actually used in practice, the last part describes image processing algorithms that are applied offline to solve a variety of problems. The book is designed for advanced undergraduate and graduate students in applied mathematics, image processing, computer science, and related fields. It is

also suitable for academic researchers and professionals in the movie industry.
Third International Conference Palo Alto, CA, USA, August 12-14, 2009 Proceedings
Software and Hardware Implementation of Hyperelliptic Curve Cryptosystems
Understanding Cryptography
5th International Conference, Cologne, Germany, May 16-18, 2012, Revised Selected Papers

Second International Conference, Egham, UK, September 1-3, 2008, Proceedings

Handbook of Information and Communication Security

The subject of conformal mappings is a major part of geometric function theory that gained prominence after the publication of the Riemann mapping theorem — for every simply connected domain of the extended complex plane there is a univalent and meromorphic function that maps such a domain conformally onto the unit disk. The Handbook of Conformal Mappings and Applications is a compendium of at least all known conformal maps to date, with diagrams and description,

and all possible applications in different scientific disciplines, such as: fluid flows, heat transfer, acoustics, electromagnetic fields as static fields in electricity and magnetism, various mathematical models and methods, including solutions of certain integral equations.

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.

A guide to a rich and fascinating subject: algebraic curves and how they vary in families. Providing a broad but compact overview of the field, this book is accessible to readers with a modest background in algebraic geometry. It develops many techniques, including Hilbert schemes, deformation theory, stable reduction, intersection theory, and geometric invariant theory, with the focus on examples and applications arising in the study of moduli of curves. From such foundations, the book goes on to show how moduli spaces of curves are constructed, illustrates typical applications with the proofs of the Brill-

Noether and Gieseker-Petri theorems via limit linear series, and surveys the most important results about their geometry ranging from irreducibility and complete subvarieties to ample divisors and Kodaira dimension. With over 180 exercises and 70 figures, the book also provides a concise introduction to the main results and open problems about important topics which are not covered in detail.

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

Handbook of Conformal Mappings and Applications

Selected Areas in Cryptography

A Textbook for Students and Practitioners

Handbook of Elliptic Integrals for Engineers and Physicists

28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009, Proceedings

Arithmetic of Finite Fields

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

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.
This book constitutes the thoroughly refereed proceedings of the Second International Conference on Pairing-Based Cryptography, Pairing 2008, held in London, UK, in September 2008. The 20 full papers, presented together with the contributions resulting

from 3 invited talks, were carefully reviewed and selected from 50 submissions. The contents are organized in topical sections on cryptography, mathematics, constructing pairing-friendly curves, implementation of pairings, and hardware implementation.

Now in its third edition, this highly successful textbook is widely regarded as the 'bible of computer algebra'.

Elliptic Curves and Their Applications to Cryptography

Image Processing for Cinema

Algebraic Aspects of Cryptography

10th International Workshop, Washington, D.C., USA, August 10-13, 2008, Proceedings

Handbook of Elliptic and Hyperelliptic Curve Cryptography

Functional Encryption

recipients of the Best Paper Award.

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.

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.