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

This is likewise one of the factors by obtaining the soft documents of this **Handbook Of Elliptic And Hyperelliptic Curve Cryptography Discrete Mathematics And Its Applications** by online. You might not require more epoch to spend to go to the books launch as well as search for them. In some cases, you likewise get not discover the message Handbook Of Elliptic And Hyperelliptic Curve Cryptography Discrete Mathematics And Its Applications that you are looking for. It will enormously squander the time.

However below, like you visit this web page, it will be so utterly easy to acquire as skillfully as download lead Handbook Of Elliptic And Hyperelliptic Curve Cryptography Discrete Mathematics And Its Applications

It will not acknowledge many time as we explain before. You can pull off it while piece of legislation something else at home and even in your workplace. thus easy! So, are you question? Just exercise just what we have enough money below as well as review **Handbook Of Elliptic And Hyperelliptic Curve Cryptography Discrete Mathematics And Its Applications** what you afterward to read!

Progress in Cryptology – AFRICACRYPT 2014 - David Pointcheval 2014-05-21
This book constitutes the refereed proceedings of the 7th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICA CRYPT 2014, held in Marrakesh, Morocco in May 2014. The 26 papers presented together with 1 invited talk were carefully reviewed and selected from 83 submissions. The aim of Africa crypt 2014 is to provide an international forum for practitioners and researchers from industry, academia and government from all over the world for a wide ranging discussion of all forms of cryptography and its applications as follows: Public-Key Cryptography, Hash Functions, Secret-Key Cryptanalysis, Number Theory, Hardware Implementation, Protocols and Lattice-based Cryptography.

Information Security and Privacy - Yi Mu 2008-06-24
This book constitutes the refereed proceedings of the 13th Australasian Conference on Information Security and Privacy, ACISP 2008, held in Wollongong, Australia, in July 2008. The 33 revised full papers presented were carefully reviewed and selected from 111 submissions. The papers cover a range of topics in information security, including authentication, key management, public key cryptography, privacy, anonymity, secure communication, ciphers, network security, elliptic curves, hash functions, and database security.

Advances in Computing Systems and Applications - Oualid Demigha 2018-08-09
This book gathers selected papers presented at the 3rd Conference on Computing Systems and Applications (CSA’2018),

held at the Ecole Militaire Polytechnique, Algiers, Algeria on April 24–25, 2018. The CSA'2018 constitutes a leading forum for exchanging, discussing and leveraging modern computer systems technology in such varied fields as: data science, computer networks and security, information systems and software engineering, and computer vision. The contributions presented here will help promote and advance the adoption of computer science technologies in industrial, entertainment, social, and everyday applications. Though primarily intended for students, researchers, engineers and practitioners working in the field, it will also benefit a wider audience interested in the latest developments in the computer sciences.

Computer Security -- ESORICS 2015 - Günther Pernul 2015-10-09

The two-volume set, LNCS 9326 and LNCS 9327 constitutes the refereed proceedings of the 20th European Symposium on Research in Computer Security, ESORICS 2015, held in Vienna, Austria, in September 2015. The 59 revised full papers presented were carefully reviewed and selected from 298 submissions. The papers address issues such as networks and Web security; system security; crypto application and attacks; risk analysis; privacy; cloud security; protocols and attribute-based encryption; code analysis and side-channels; detection and monitoring; authentication; policies; and applied security.

Algorithmic Number Theory - Guillaume Hanrot 2010-07-07

This book constitutes the refereed proceedings of the 9th International Algorithmic Number Theory Symposium, ANTS 2010, held in Nancy, France, in July 2010. The 25 revised full papers presented together with 5 invited papers were carefully reviewed and selected for inclusion in the book. The papers are devoted to algorithmic aspects of number theory, including elementary number theory, algebraic number theory, analytic number theory, geometry of numbers, algebraic geometry, finite fields, and cryptography.

Arithmetic of Finite Fields - Claude Carlet 2007-09-21

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. It covers 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.

Pairing-Based Cryptography - Pairing 2010 - Marc Joye 2010-11-18

This book constitutes the refereed proceedings of the 4th International Conference on Pairing-Based Cryptography, Pairing 2010, held in Yamanaka Hot Spring, Japan, in December 2010. The 25 full papers presented were carefully reviewed and selected from 64 submissions. The contributions are organized in topical sections on: efficient software implementation; digital signatures; cryptographic protocols; key agreement; applications - code generation, time-released encryption, and cloud computing; point encoding and pairing-friendly curves; ID-based encryption schemes; and efficient hardware, FPGAs, and algorithms.

Information Security Theory and Practice. Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems - Ioannis Askoxylakis 2012-06-16

This volume constitutes the refereed proceedings of the 6th IFIP WG 11.2 International Workshop on Information Security Theory and Practice: Security, Privacy and Trust in Computing Systems and Ambient Intelligent Ecosystems, WISTP 2012, held in Egham, UK, in June 2012. The 9 revised full papers and 8 short papers presented together with three keynote speeches were carefully reviewed and selected from numerous submissions. They are organized in topical sections on protocols, privacy, policy and access control, multi-party computation, cryptography, and mobile security.

Computer and Information Sciences - Erol Gelenbe 2010-09-20

Computer and Information Sciences is a unique and comprehensive review of advanced technology and research in the field of Information Technology. It provides an up to date snapshot of research in Europe and the Far East (Hong Kong, Japan and China) in the most active areas of information technology, including Computer Vision, Data Engineering, Web Engineering, Internet Technologies, Bio-Informatics and System Performance Evaluation Methodologies.

Mathematics in Cyber Research - Paul L. Goethals 2022-02-06

In the last decade, both scholars and practitioners have sought novel ways to address the problem of cybersecurity. Innovative outcomes have included applications such as blockchain as well as creative methods for cyber forensics, software development, and intrusion prevention. Accompanying these technological advancements, discussion on cyber matters at national and international levels has focused primarily on the topics of law, policy, and strategy. The objective of these efforts is typically to promote security by establishing agreements among stakeholders on regulatory activities. Varying levels of investment in cyberspace, however, comes with varying levels of risk; in some ways, this can translate directly to the degree of emphasis for pushing substantial change. At the very foundation or root of cyberspace systems and processes are tenets and rules governed by principles in mathematics. Topics such as encrypting or decrypting file transmissions, modeling networks, performing data analysis, quantifying uncertainty, measuring risk, and weighing decisions or adversarial courses of action represent a very small subset of activities highlighted by mathematics. To facilitate education and a greater awareness of the role of mathematics in cyber systems and processes, a description of research in this area is needed. Mathematics in Cyber Research aims to familiarize educators and young researchers with the breadth of mathematics in cyber-related research. Each chapter introduces a mathematical sub-field, describes relevant work in this field associated with the cyber domain, provides methods and tools, as well as details cyber research examples or case studies. Features One of the only books to bring together such a diverse and comprehensive range of topics within mathematics and apply them to cyber research. Suitable for college undergraduate students or educators that are either interested in learning about cyber-related mathematics or intend to perform research within the cyber domain. The book may also appeal to practitioners within the commercial or government industry sectors. Most national and international venues for collaboration and discussion on cyber matters have focused primarily on the topics of law, policy, strategy, and technology. This book is among the first to address the underpinning mathematics.

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.

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.

Algebraic Aspects of Digital Communications - Tanush Shaska 2009

-Proceedings of the NATO Advanced Study Institute on New Challenges in Digital Communications, Vlora, Albania, 27 April - 9 May 2008.---T.p. verso.

The Arithmetic of Elliptic Curves - Joseph H. Silverman 2009-04-20

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.

Selected Areas in Cryptography - Roberto Avanzi 2009-08-22

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.

Pairing-Based Cryptography - Pairing 2007 - Tsuyoshi Takagi 2007-06-21

Pairing-based cryptography is at the very leading edge of the current wave in computer cryptography. That makes this book all the more relevant, being as it is the refereed proceedings of the First International Conference on Pairing-Based Cryptography, Pairing 2007, held in Tokyo, Japan in 2007. The 18 revised full papers presented together were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections including those on applications, and certificateless public key encryption.

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.

Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition - Henri Cohen 2016-03-26

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.

An Introduction to Mathematical Cryptography - Jeffrey Hoffstein 2014-09-11

This self-contained introduction to modern cryptography emphasizes the mathematics behind the theory of public key cryptosystems and digital signature schemes. The book focuses on these key topics while developing the mathematical tools needed for the construction and security analysis of diverse cryptosystems. Only basic linear algebra is required of the reader; techniques from algebra, number theory, and probability are introduced and developed as required. This text provides an ideal introduction for mathematics and computer science students to the mathematical foundations of modern cryptography. The book includes an extensive bibliography and index; supplementary materials are available online. The book covers a variety of topics that are considered central to mathematical cryptography. Key topics include: classical cryptographic constructions, such as Diffie–Hellmann key exchange, discrete logarithm-based cryptosystems, the RSA cryptosystem, and digital signatures; fundamental mathematical tools for cryptography, including primality testing, factorization algorithms, probability theory, information theory, and collision algorithms; an in-depth treatment of important cryptographic innovations, such as elliptic curves, elliptic curve and pairing-based cryptography, lattices, lattice-based cryptography, and the NTRU cryptosystem. The second edition of An Introduction to Mathematical Cryptography includes a significant revision of the material on digital signatures, including an earlier introduction to RSA, Elgamal, and DSA signatures, and new material on lattice-based signatures and rejection sampling. Many sections have been rewritten or expanded for clarity, especially in the chapters on information theory, elliptic curves, and lattices, and the chapter of additional topics has been expanded to include sections on digital cash and homomorphic encryption. Numerous new exercises have been included.

Mathematical Aspects of Computer and Information Sciences - Johannes Blömer 2017-12-20

This book constitutes the refereed proceedings of the 7th International Conference on Mathematical Aspects of Computer and Information Sciences, MACIS 2017, held in Vienna, Austria, in November 2017. The 28 revised papers and 8 short papers presented were carefully reviewed and selected from 67 submissions. The papers are organized in the following topical sections: foundation of algorithms in mathematics, engineering and scientific computation; combinatorics and codes in computer science; data modeling and analysis; and mathematical aspects of information security and cryptography.

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.

Foundations of Coding - Jean-Guillaume Dumas 2015-01-05
Offers a comprehensive introduction to the fundamentalstructures and applications of a wide range of contemporary codingoperations This book offers a comprehensive introduction to the fundamentalstructures and applications of a wide range of contemporary codingoperations. This text focuses on the ways to structure informationso that its transmission will be in the safest, quickest, and mostefficient and error-free manner possible. All coding operations arecovered in a single framework, with initial chapters addressingearly mathematical models and algorithmic developments which led tothe structure of code. After discussing the general foundations ofcode, chapters proceed to cover individual topics such as notionsof compression, cryptography, detection, and correction codes. Bothclassical coding theories and the most cutting-edge models areaddressed, along with helpful exercises of varying complexities toenhance comprehension. Explains how to structure coding information so that itstransmission is safe, error-free, efficient, and fast Includes a pseudo-code that readers may implement in theirpreferential programming language Features descriptive diagrams and illustrations, and almost 150exercises, with corrections, of varying complexity to enhancecomprehension Foundations of Coding: Compression, Encryption,Error-Correction is an invaluable resource for understandingthe various ways information is structured for its secure andreliable transmission in the 21st-century world.

Guide to Pairing-Based Cryptography - Nadia El Mrabet 2017-01-06
This book is devoted to efficient pairing computations and implementations, useful tools for cryptographers working on topics like identity-based cryptography and the simplification of existing protocols like signature schemes. As well as exploring the basic mathematical background of finite fields and elliptic curves, Guide to Pairing-Based Cryptography offers an overview of the most recent developments in optimizations for pairing implementation. Each chapter includes a presentation of the problem it discusses, the mathematical formulation, a discussion of implementation issues, solutions accompanied by code or pseudocode, several numerical results, and references to further reading and notes. Intended as a self-contained handbook, this book is an invaluable resource for computer scientists, applied mathematicians and security professionals interested in cryptography.

Open Problems in Mathematics and Computational Science - Çetin Kaya Koç 2015-03-25
This book presents interesting, important unsolved problems in the mathematical and computational sciences. The contributing authors are leading researchers in their fields and they explain outstanding challenges in their domains, first by offering basic definitions, explaining the context, and summarizing related algorithms, theorems, and proofs, and then by suggesting creative solutions. The authors feel a strong motivation to excite deep research and discussion in the mathematical and computational sciences community, and the book will be of value to postgraduate students and researchers in the areas of theoretical computer science, discrete mathematics, engineering, and cryptology.

Bent Functions - Sihem Mesnager 2016-08-09
This book gives a detailed survey of the main results on bent functions over finite fields, presents a systematic overview of their generalizations, variations and applications, considers open problems in classification and systematization of bent functions, and discusses proofs of several results. This book uniquely provides a necessary comprehensive coverage of bent functions.It serves as a useful reference for researchers in discrete mathematics, coding and cryptography. Students and professors in mathematics and computer science will also find the content valuable, especially those interested in mathematical foundations of cryptography. It can be used as a supplementary text for university courses on discrete mathematics, Boolean functions, or cryptography, and is appropriate for both basic classes for undergraduate students and advanced courses for specialists in cryptography and mathematics.
Selected Areas in Cryptography -- SAC 2014 - Antoine Joux 2014-12-04
This book constitutes the proceedings of the 21st International Conference on Selected Areas in Cryptography, SAC 2014, held in Montreal, QC, Canada, in August 2014. The 22 papers presented in this volume were carefully reviewed and selected from 103 submissions. There are four areas covered at each SAC conference. The three permanent areas are: design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash function, MAC algorithms, cryptographic permutations, and authenticated encryption schemes; efficient implementations of symmetric and public key algorithms; mathematical and algorithmic aspects of applied cryptology. This year, the fourth area for SAC 2014 is: algorithms for cryptography, cryptanalysis and their complexity analysis.
Research in Cryptology - Stefan Lucks 2008-10-01
This book constitutes the refereed proceedings of the Second Western European Workshop on Research in Cryptology, WEWoRC 2007, held in Bochum, Germany, in July 2007 The 12 revised full papers were carefully reviewed and selected from a total of 36 submissions. The papers cover topics such as foundations of cryptology, secret-key cryptosystems and hash functions, public-key cryptosystems, cryptographic protocols, implementation of cryptosystems and their integration into secure systems, secure operating systems and trusted computing, applications such as watermarking and code obfuscation.
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.
Algorithmic Arithmetic, Geometry, and Coding Theory - Stéphane Ballet 2015-04-20
This volume contains the proceedings of the 14th International Conference on Arithmetic, Geometry, Cryptography, and Coding

Theory (AGCT), held June 3-7, 2013, at CIRM, Marseille, France. These international conferences, held every two years, have been a major event in the area of algorithmic and applied arithmetic geometry for more than 20 years. This volume contains 13 original research articles covering geometric error correcting codes, and algorithmic and explicit arithmetic geometry of curves and higher dimensional varieties. Tools used in these articles include classical algebraic geometry of curves, varieties and Jacobians, Suslin homology, Monsky-Washnitzer cohomology, and -functions of modular forms.

Secure IT Systems - Sonja Buchegger 2015-10-26

This book constitutes the proceedings of the 20th Nordic Conference on Secure IT Systems, held in Stockholm, Sweden, in October 2015. The 11 full papers presented together with 5 short papers in this volume were carefully reviewed and selected from 38 submissions. They are organized in topical sections named: cyber-physical systems security, privacy, cryptography, trust and fraud, and network and software security.

Pairing-Based Cryptography – Pairing 2008 - Steven Galbraith 2008-08-25

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.

Pairing-Based Cryptography -- Pairing 2012 - Michel Abdalla 2013-02-01

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.

Advances in Cryptology – EUROCRYPT 2007 - Moni Naor 2007-06-23

This book constitutes the refereed proceedings of the 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2007, held in Barcelona, Spain in May 2007. The 33 revised full papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications.

Progress in Cryptology - INDOCRYPT 2006 - Rana Barua 2006-11-28

This book constitutes the refereed proceedings of the 7th International Conference on Cryptology in India, INDOCRYPT 2006, held in Kolkata, India in December 2006. The 29 revised full papers and 2 invited papers cover such topics as symmetric cryptography, provable security, fast implementation of public key cryptography, id-based cryptography, as well as embedded systems and side channel attacks.

Topics in Cryptology - CT-RSA 2012 - Orr Dunkelman 2012-01-30

This book constitutes the refereed proceedings of the Cryptographers' Track at the RSA Conference 2012, CT-RSA 2012, held in San Francisco, CA, USA, in February/March 2012. The 26 revised full papers presented were carefully reviewed and selected from 113 submissions. The papers are organized in topical sections on side channel attacks, digital signatures, public-key encryption, cryptographic protocols, secure implementation methods, symmetric key primitives, and secure multiparty computation.

Selected Areas in Cryptography - Ali Miri 2012-02-21
This book constitutes the thoroughly refereed post-conference proceedings of the 18th Annual International Workshop on Selected Areas in Cryptography, SAC 2011, held in Toronto, Canada in August 2011. The 23 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 92 submissions. The papers are organized in topical sections on cryptanalysis of hash functions, security in clouds, bits and randomness, cryptanalysis of ciphers, cryptanalysis of public-key crypthography, cipher implementation, new designs and mathematical aspects of applied cryptography.
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
Advances in Cryptology – EUROCRYPT 2012 - David Pointcheval 2012-04-05
This book constitutes the refereed proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2012, held in Cambgridge, UK, in April 2012. The 41 papers, presented together with 2 invited talks, were carefully reviewed and selected from 195 submissions. The papers are organized in topical sections on index calculus, symmetric constructions, secure computation, protocols, lossy trapdoor functions, tools, symmetric cryptanalysis, fully homomorphic encryption, asymmetric cryptanalysis, efficient reductions, public-key schemes, security models, and lattices.
Advances in Cryptology -- ASIACRYPT 2014 - Palash Sarkar 2014-11-07
The two-volume set LNCS 8873 and 8874 constitutes the refereed proceedings of the 20th International Conference on the Theory and Applications of Cryptology and Information Security, ASIACRYPT 2014, held in Kaoshiung, Taiwan, in December 2014. The 55 revised full papers and two invited talks presented were carefully selected from 255 submissions. They are organized in topical sections on cryptology and coding theory; authenticated encryption; symmetric key cryptanalysis; side channel analysis; hyperelliptic curve cryptography; factoring and discrete log; cryptanalysis; signatures; zero knowledge; encryption schemes; outsourcing and delegation; obfuscation; homomorphic cryptography; secret sharing; block ciphers and passwords; black-box separation; composability; multi-party computation.
Algebraic Curves in Cryptography - San Ling 2013-06-13
The reach of algebraic curves in cryptography goes far beyond elliptic curve or public key cryptography yet these other application areas have not been systematically covered in the literature. Addressing this gap, Algebraic Curves in Cryptography explores the rich uses of algebraic curves in a range of cryptographic applications, such as secret sh