Notes On Hashing Mit

Thank you for reading **Notes On Hashing Mit** . As you may know, people have look hundreds times for their favorite novels like this Notes On Hashing Mit , but end up in harmful downloads.
Rather than enjoying a good book with a cup of coffee in the afternoon, instead they juggled with some harmful virus inside their laptop.

Notes On Hashing Mit is available in our digital library an online access to it is set as public so you can get it instantly.
Our books collection saves in multiple locations, allowing you to get the most less latency time to download any of our books like this one.
Kindly say, the Notes On Hashing Mit is universally compatible with any devices to read

Introduction To Algorithms - Thomas H Cormen 2001
The first edition won the award for Best 1990 Professional and Scholarly Book in Computer Science and Data Processing by the Association of American Publishers. There are books on algorithms that are rigorous but incomplete and others that cover masses of material but lack rigor. Introduction to Algorithms combines rigor and comprehensiveness. The book covers a broad range of algorithms in depth, yet makes their design and analysis accessible to all levels of readers. Each chapter is relatively self-contained and can be used as a unit of study. The algorithms are described in English and in a pseudocode designed to be readable by anyone who has done a little programming. The explanations have been kept elementary without sacrificing depth of coverage or mathematical rigor. The first edition became the standard reference for professionals and a widely used text in universities worldwide. The second edition features new chapters on the role of algorithms, probabilistic analysis and randomized algorithms, and linear programming, as well as extensive revisions to virtually every section of the book. In a subtle but important change, loop invariants are introduced early and used throughout the text to prove algorithm correctness. Without changing the mathematical and analytic focus, the authors have moved much of the mathematical foundations material from Part I to an appendix and have included additional motivational material at the beginning.

Software-optimized Universal Hashing and Message Authentication - Theodore D. Krovetz 2000

Advances in Cryptology - CRYPTO 2001 - Joe Kilian 2003-05-15
Crypto 2001, the 21st Annual Crypto conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The conference received 156 submissions, of which the program committee selected 34 for presentation; one was later withdrawn. These proceedings contain the revised versions of the 33 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers. The conference program included two invited lectures. Mark Sherwin spoke on, \Quantum information processing in semiconductors: an experimentalist’s view." Daniel Weitzner spoke on, \Privacy, Authentication & Identity: A recent history of cryptographic struggles for freedom." The conference program also included its perennial \rump session," chaired by Stuart Haber, featuring short, informal talks on late{breaking research news. As I try to account

for the hours of my life that ?ew o to oblivion, I realize that most of my time was spent cajoling talented innocents into spending even more time on my behalf. I have accumulated more debts than I can ever hope to repay. As mere statements of thanks are certainly insu cient, consider the rest of this preface my version of Chapter 11.

Public Key Cryptography - Hideki Imai 1998-06-24

The intricate 3D structure of the CNS lends itself to multimedia presentation, and is depicted here by way of dynamic 3D models that can be freely rotated, and in over 200 illustrations taken from the successful book 'The Human Central Nervous System' by R. Nieuwenhuys et al, allowing the user to explore all aspects of this complex and fascinating subject. All this fully hyperlinked with over 2000 specialist terms. Optimal exam revision is guaranteed with the self-study option. For further information please contact: http://www.brainmedia.de/html/frames/pr/pr 5/pr 5 02.html

Data Structures -

Computer Performance Evaluation - Ramon Puigjaner 2003-06-26

The need to evaluate computer and communication systems performance and dependability is continuously growing as a consequence of both the increasing complexity of systems and the user requirements in terms of timing behaviour. The 10th International Conference on Modelling Techniques and Tools for C- puter Performance Evaluation, held in Palma in September 1998, was organised with the aim of creating a forum in which both theoreticians and practitioners could interchange recent techniques, tools, and experiences in these areas. This meeting follows the predecessor conferences of this series: 1984 Paris 1988 Palma 1994 Wien 1985 Sophia Antipolis 1991 Torino 1995 Heidelberg 1987 Paris 1992 Edinburgh 1997 Saint Malo The tradition of this conference series continued this year where many high quality papers were submitted. The Programme Committee had a di cult task in selecting the best papers. Many ne papers could not be included in the program due to space constraints. All accepted papers are included in this volume. Also, a set of submissions describing performance modelling tools was transformed into tool presentations and demonstrations. A brief description of these tools is included in this volume. The following table gives the overall statistics for the submissions.

Networking 2004 - Nikolas Mitrou 2004-04-28

This book constitutes the refereed proceedings of the Third IFIP-TC6 Networking Conference, NETWORKING 2004, held in Athens, Greece, in May 2004. The 103 revised full papers and 40 revised short papers were carefully reviewed and selected from 539 submissions. The papers are organized in topical sections on network security; TCP performance; ad-hoc networks; wavelength management; multicast; wireless network performance; inter-domain routing; packet classification and scheduling; services and monitoring; admission control; competition in networks; 3G/4G wireless systems; MPLS and related technologies; flow and congestion control; performance of IEEE 802.11; optical networks; TCP and congestion; key management; authentication and DOS prevention; energy aspects of wireless networks; optical network access; routing in ad-hoc networks; fault detection, restoration, and tolerance; QoS metrics, algorithms, and architecture; content distribution, caching, and replication; and routing theory and path computation.

Information Security and Privacy - Qld.) Acisp 9 (1998 Brisbane 1998-07

This book constitutes the refereed proceedings of the Second Australasian Conference on Information Security and Privacy, ACISP'97, held in Sydney, NSW, Australia, in July 1997. The 20 revised full papers presented were carefully selected for inclusion in the proceedings. The book is divided into sections on security models and access control, network security, secure hardware and implementation issues, cryptographic functions and ciphers, authentication codes and secret sharing systems, cryptanalysis, key escrow, security protocols and key management, and applications.

Advances in Cryptology - ASIACRYPT 2003 - Chi Sung Laih 2003-11-06

This book constitutes the refereed proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2003, held in Taipei, Taiwan in

November/December 2003.The 32 revised full papers presented together with one invited paper were carefully reviewed and selected from 188 submissions. The papers are organized in topical sections on public key cryptography, number theory, efficient implementations, key management and protocols, hash functions, group signatures, block cyphers, broadcast and multicast, foundations and complexity theory, and digital signatures.

Computers for Artificial Intelligence Applications - Benjamin W. Wah 1986

Big Data Analytics for Large-Scale Multimedia Search - Stefanos Vrochidis 2019-05-28

A timely overview of cutting edge technologies for multimedia retrieval with a special emphasis on scalability The amount of multimedia data available every day is enormous and is growing at an exponential rate, creating a great need for new and more efficient approaches for large scale multimedia search. This book addresses that need, covering the area of multimedia retrieval and placing a special emphasis on scalability. It reports the recent works in large scale multimedia search, including research methods and applications, and is structured so that readers with basic knowledge can grasp the core message while still allowing experts and specialists to drill further down into the analytical sections. Big Data Analytics for Large-Scale Multimedia Search covers: representation learning, concept and event-based video search in large collections; big data multimedia mining, large scale video understanding, big multimedia data fusion, large-scale social multimedia analysis, privacy and audiovisual content, data storage and management for big multimedia, large scale multimedia search, multimedia tagging using deep learning, interactive interfaces for big multimedia and medical decision support applications using large multimodal data. Addresses the area of multimedia retrieval and pays close attention to the issue of scalability Presents problem driven techniques with solutions that are demonstrated through realistic case studies and user scenarios Includes tables, illustrations, and figures Offers a Wiley-hosted BCS that features links to open source algorithms, data sets and tools Big Data Analytics for Large-Scale Multimedia Search is an excellent book for academics, industrial researchers, and developers interested in big multimedia data search retrieval. It will also appeal to consultants in computer science problems and professionals in the multimedia industry.

Advances in Cryptology - 2004

High Performance Computing and Communications - Ronald Perrott 2007-09-08

This book constitutes the refereed proceedings of the Third International Conference on High Performance Computing and Communications, HPCC 2007. The 75 revised full papers address all current issues of parallel and distributed systems and high performance computing and communication, including networking protocols, embedded systems, wireless, mobile and pervasive computing, Web services and internet computing, and programming interfaces for parallel systems.

No Better Time - Molly Knight Raskin 2013-09-10

No Better Time tells of a young, driven mathematical genius who wrote a set of algorithms that would create a faster, better Internet. It's the story of a beautiful friendship between a loud, irreverent student and his soft-spoken MIT professor, of a husband and father who spent years struggling to make ends meet only to become a billionaire almost overnight with the success of Akamai Technologies, the Internet content delivery network he cofounded with his mentor. Danny Lewin's brilliant but brief life is largely unknown because, until now, those closest to him have guarded their memories and quietly mourned their loss. For Lewin was almost certainly the first victim of 9/11, stabbed to death at age 31 while trying to overpower the terrorists who would eventually fly American Flight 11 into the World Trade Center. But ironically it was 9/11 that proved the ultimate test for Lewin's vision—while phone communication failed and web traffic surged as never before, the critical news and government sites that relied on Akamai—and the technology pioneered by Danny Lewin—remained up and running.

Krypto-Mining für Dummies - Peter Kent 2022-11-14

Kryptowährungen versprechen schnelles Geld und Reichtum. Anders als die Goldsucher im vorletzten Jahrhundert brauchen Sie als Investor aber sehr viel mehr technisches Know-how, um in das Krypto-Mining einzusteigen. Dieses Buch wurde von zwei Insidern geschrieben. Sie erläutern, welche Hard- und Software Sie brauchen und wie Sie bei der Gewinnung von Bitcoin, Ethereum, Monero, LiteCoin und Dash am besten vorgehen - und zwar so, dass Sie der Konkurrenz voraus sind und Ihren Return on Investment maximieren.

Introduction to Algorithms, third edition - Thomas H. Cormen 2009-07-31

The latest edition of the essential text and professional reference, with substantial new material on such topics as vEB trees, multithreaded algorithms, dynamic programming, and edge-based flow. Some books on algorithms are rigorous but incomplete; others cover masses of material but lack rigor. Introduction to Algorithms uniquely combines rigor and comprehensiveness. The book covers a broad range of algorithms in depth, yet makes their design and analysis accessible to all levels of readers. Each chapter is relatively self-contained and can be used as a unit of study. The algorithms are described in English and in a pseudocode designed to be readable by anyone who has done a little programming. The explanations have been kept elementary without sacrificing depth of coverage or mathematical rigor. The first edition became a widely used text in universities worldwide as well as the standard reference for professionals. The second edition featured new chapters on the role of algorithms, probabilistic analysis and randomized algorithms, and linear programming. The third edition has been revised and updated throughout. It includes two completely new chapters, on van Emde Boas trees and multithreaded algorithms, substantial additions to the chapter on recurrence (now called "Divide-and-Conquer"), and an appendix on matrices. It features improved treatment of dynamic programming and greedy algorithms and a new notion of edge-based flow in the material on flow networks. Many exercises and problems have been added for this edition. The international paperback edition is no longer available; the hardcover is available worldwide.

Mathematics for Computer Science - Eric Lehman 2017-03-08

This book covers elementary discrete mathematics for computer science and engineering. It emphasizes mathematical definitions and proofs as well as applicable methods. Topics include formal logic notation, proof methods; induction, well-ordering; sets, relations; elementary graph theory; integer congruences; asymptotic notation and growth of functions; permutations and combinations, counting principles; discrete probability. Further selected topics may also be covered, such as recursive definition and structural induction; state machines and invariants; recurrences; generating functions.

Fast Software Encryption - Bart Preneel 1995-10-25

This book contains a set of revised refereed papers selected from the presentations at the Second International Workshop on Fast Software Encryption held in Leuven, Belgium, in December 1994. The 28 papers presented significantly advance the state of the art of software algorithms for two cryptographic primitives requiring very high speeds, namely encryption algorithms and hash functions: this volume contains six proposals for new ciphers as well as new results on the security of the new proposals. In addition, there is an introductory overview by the volume editor. The papers are organized in several sections on stream ciphers and block ciphers; other papers deal with new algorithms and protocols or other recent results.

Advances in Cryptology - CRYPTO 2002 - Moti Yung 2003-08-02

Crypto 2002, the 22nd Annual Crypto Conference, was sponsored by IACR, the International Association for Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. It is published as Vol. 2442 of the Lecture Notes in Computer Science (LNCS) of Springer Verlag. Note that 2002, 22 and 2442 are all palindromes... (Don't nod!) Theconferencereceived175submissions,ofwhich40wereaccepted;twos-missionsweremergedintoasinglepaper,yieldingthetotalof39papersaccepted for presentation in the technical program of the conference. In this proceedings volume you will ?nd the revised versions of the 39 papers that were presented at the conference. The submissions represent the current state of work in the cryptographic community worldwide, covering all areas of cryptologic research. In fact, many high-quality works (that surely will be published elsewhere) could not be accepted. This is due to the competitive nature of the conference and the challenging task of selecting a program. I wish to thank the authors of all submitted papers. Indeed, it is the authors of all papers who have made this conference possible, regardless of whether or not their papers were accepted. The conference program was also immensely bene?ted by two plenary talks.

Advances in Cryptology — CRYPTO ’93 - Douglas R. Stinson 2003-05-15

The CRYPTO ’93 conference was sponsored by the International Association for Cryptologic Research (IACR) and Bell-Northern Research (a subsidiary of Northern Telecom), in co-operation with the IEEE Computer Society Technical Committee. It took place at the University of California, Santa Barbara, from August 22-26, 1993. This was the thirteenth annual CRYPTO conference, all of which have been held at UCSB. The conference was very enjoyable and ran very of the General Chair, Paul Van Oorschot. smoothly, largely due to the efforts It was a pleasure working with Paul throughout the months leading up to the conference. There were 136 submitted papers which were considered by the Program Committee. Of these, 38 were selected for presentation at the conference. There was also one invited talk at the conference, presented by Miles Smid, the title of which was “A Status Report On the Federal Government Key Escrow System.” The conference also included the customary Rump Session, which was presided over by Whit Diffie in his usual inimitable fashion. Thanks again to Whit for organizing and running the Rump session. This year, the Rump Session included an interesting and lively panel discussion on issues pertaining to key escrowing. Those taking part were W. Diffie, J. Gilmore, S. Goldwasser, M. Hellman, A. Herzberg, S. Micali, R. Rueppel, G. Simmons and D. Weitzner.

Advances in Cryptology - CRYPTO '99 - Michael Wiener 2003-07-31

Crypto ’99, the Nineteenth Annual Crypto Conference, was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department, University of California, Santa Barbara (UCSB). The General Chair, Donald Beaver, was responsible for local organization and registration. The Program Committee considered 167 papers and selected 38 for presentation. This year’s conference program also included two invited lectures. I was pleased to include in the program UeliM aurer’s presentation “Information Theoretic Cryptography” and Martin Hellman’s presentation “The Evolution of Public Key Cryptography.” The program also incorporated the traditional Rump Session for informal short presentations of new results, run by Stuart Haber. These proceedings include the revised versions of the 38 papers accepted by the Program Committee. These papers were selected from all the submissions to the conference based on originality, quality, and relevance to the field of cryptology. Revisions were not checked, and the authors bear full responsibility for the contents of their papers.

Advances in Cryptology - CRYPTO '97 - Burton S.Jr. Kaliski 1997-08-06

This book constitutes the refereed proceedings of the 17th Annual International Cryptology Conference, CRYPTO'97, held in Santa Barbara, California, USA, in August 1997 under the sponsorship of the International Association for Cryptologic Research (IACR). The volume presents 35 revised full papers selected from 160 submissions received. Also included are two invited presentations. The papers are organized in sections on complexity theory, cryptographic primitives, lattice-based cryptography, digital signatures, cryptanalysis of public-key cryptosystems, information theory, elliptic curve implementation, number-theoretic systems, distributed cryptography, hash functions, cryptanalysis of secret-key cryptosystems.

The Theory of Hash Functions and Random Oracles - Arno Mittelbach 2021-01-19

Hash functions are the cryptographer’s Swiss Army knife. Even though they play an integral part in today’s cryptography, existing textbooks discuss hash functions only in passing and instead often put an emphasis on other primitives like encryption schemes. In this book the authors take a different approach and place hash functions at the center. The result is not only an introduction to the theory of hash functions and the random oracle model but a comprehensive introduction to modern cryptography. After motivating their unique approach, in the first chapter the authors introduce the concepts from computability theory, probability theory, information theory, complexity theory, and information-theoretic security that are required to understand the book content. In Part I they introduce the foundations of hash functions and modern cryptography. They cover a number of schemes, concepts, and proof techniques, including computational security, one-way functions, pseudorandomness and pseudorandom functions, game-based proofs, message authentication codes, encryption schemes, signature schemes, and collision-resistant (hash) functions. In Part II the authors explain the random oracle model, proof techniques used with random oracles, random oracle constructions, and examples of real-world random oracle schemes. They also address the limitations of random oracles and the random oracle controversy, the fact that uninstantiable schemes exist which are provably secure in the random oracle model but which become insecure with any real-world hash function. Finally in Part III the authors focus on constructions of hash functions. This includes a treatment of iterative hash functions and generic attacks against hash functions, constructions of hash functions based on block ciphers and number-theoretic assumptions, a discussion of privately keyed hash functions including a full security proof for HMAC, and a presentation of real-world hash functions. The text is supported with exercises, notes, references, and pointers to further reading, and it is a suitable textbook for undergraduate and graduate students, and researchers of cryptology and information security.

Rethinking Public Key Infrastructures and Digital Certificates - Stefan Brands 2000-08-30

Stefan Brands proposes cryptographic building blocks for the design of digital certificates that preserve privacy without sacrificing security. As paper-based communication and transaction mechanisms are replaced by automated ones, traditional forms of security such as photographs and handwritten signatures are becoming outdated. Most security experts believe that digital certificates offer the best technology for safeguarding electronic communications. They are already widely used for authenticating and encrypting email and software, and eventually will be built into any device or piece of software that must be able to communicate securely. There is a serious problem, however, with this unavoidable trend: unless drastic measures are taken, everyone will be forced to communicate via what will be the most pervasive electronic surveillance tool ever built. There will also be abundant opportunity for misuse of digital certificates by hackers, unscrupulous employees, government agencies, financial institutions, insurance companies, and so on.In this book Stefan Brands proposes cryptographic building blocks for the design of digital certificates that preserve privacy without sacrificing security. Such certificates function in much the same way as cinema tickets or subway tokens: anyone can establish their validity and the data they specify, but no more than that. Furthermore, different actions by the same person cannot be linked. Certificate holders have control over what information is disclosed, and to whom. Subsets of the proposed cryptographic building blocks can be used in combination, allowing a cookbook approach to the design of public key infrastructures. Potential applications include electronic cash, electronic postage, digital rights management, pseudonyms for online chat rooms, health care information storage, electronic voting, and even electronic gambling.

Advances in Cryptology — CRYPTO '96 - Neal Koblitz 2003-05-15

Crypto '96, the Sixteenth Annual Crypto Conference, is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and P- vacy and the Computer Science Department of the University of California at Santa Barbara (UCSB). It takes place at UCSB from August 18 to 22, 1996. The General Chair, Richard Graveman, is responsible for local organization and registration. The scientific program was organized by the 16-member Program C- mittee. We considered 115 papers. (An additional 15 submissions had to be summarily rejected because of lateness or major noncompliance with the c- ditions in the Call for Papers.) Of these, 30 were accepted for presentation. In addition, there will be five invited talks by Ernest Brickell. Andrew Clark, Whitfield Diffie, Ronald Rivest, and Cliff Stoll. A Rump Session will be chaired by Stuart Haber. These proceedings contain the revised versions of the 30 contributed talks. least three com- The submitted version of each paper was examined by at mittee members and/or outside experts, and their comments were taken into account in the revisions. However, the authors (and not the committee) bear full responsibility for the content of their papers.

#HashtagActivism - Sarah J. Jackson 2020-03-10

How marginalized groups use Twitter to advance counter-narratives, preempt political spin, and build diverse networks of dissent. The power of hashtag activism became clear in 2011, when #IranElection served as an organizing tool for Iranians protesting a disputed election and offered a global audience a front-row seat to a nascent revolution. Since then, activists have used a variety of hashtags, including #JusticeForTrayvon, #BlackLivesMatter, #YesAllWomen, and #MeToo to advocate, mobilize, and communicate. In this book, Sarah Jackson, Moya Bailey, and Brooke Foucault Welles explore how and why Twitter has become an important platform for historically disenfranchised populations, including Black Americans, women, and transgender people. They show how marginalized groups, long excluded from elite media spaces, have used Twitter hashtags to advance counternarratives, preempt political spin, and build diverse networks of dissent. The authors describe how such hashtags as #MeToo, #SurvivorPrivilege, and #WhyIStayed have challenged the conventional understanding of gendered violence; examine the voices and narratives of Black feminism enabled by #FastTailedGirls, #YouOKSis, and #SayHerName; and explore the creation and use of #GirlsLikeUs, a network of transgender women. They investigate the digital signatures of the “new civil rights movement”—the online activism, storytelling, and strategy-building that set the stage for #BlackLivesMatter—and recount the spread of racial justice hashtags after the killing of Michael Brown in Ferguson, Missouri, and other high-profile incidents of killings by police. Finally, they consider hashtag created by allies, including #AllMenCan and #CrimingWhileWhite.

Embedded and Ubiquitous Computing - EUC 2005 Workshops - Tomoya Enokido 2005-11-25

This book constitutes the refereed proceedings of the EUC 2005 workshops held in conjunction with the IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2005, in Nagasaki, Japan in December 2005. The 132 revised full papers presented were carefully reviewed and selected from 352 submissions. Topics covered by the five workshops are ubiquitous intelligence and smart worlds (UISW 2005), network-centric ubiquitous systems (NCUS 2005), security in ubiquitous computing systems (SecUbiq 2005), RFID and ubiquitous sensor networks (USN 2005), and trusted and autonomic ubiquitous and embedded systems (TAUES 2005).

Mining of Massive Datasets - Jure Leskovec 2014-11-13

Now in its second edition, this book focuses on practical algorithms for mining data from even the largest datasets.

Computer Science Handbook - Allen B. Tucker 2004-06-28

When you think about how far and fast computer science has progressed in recent years, it's not hard to conclude that a seven-year old handbook may fall a little short of the kind of reference today's computer scientists, software engineers, and IT professionals need. With a broadened scope, more emphasis on applied computing, and more than 70 chap

Hashing in Computer Science - Alan G. Konheim 2010-12-07

Written by one of the developers of the technology, Hashing is both a historical document on the development of hashing and an analysis of the applications of hashing in a society increasingly concerned with security. The material in this book is based on courses taught by the author, and key points are reinforced in sample problems and an accompanying instructor s manual. Graduate students and researchers in mathematics, cryptography, and security will benefit from this overview of hashing and the complicated mathematics that it requires.

Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management - Hossein Bidgoli 2006-03-13

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Mathematical Writing - Donald E. Knuth 1989

This book will help those wishing to teach a course in technical writing, or who wish to write themselves.

STACS 2007 - Wolfgang Thomas 2007-05-24

This book constitutes the refereed proceedings of the 24th Annual Symposium on Theoretical Aspects of Computer Science, STACS 2007, held in Aachen, Germany in February 2007. The 56 revised full papers presented together with 3 invited papers address the whole range of theoretical computer science as well as current challenges like biological computing, quantum computing, and mobile and net computing.

High Performance Python - Micha Gorelick 2020-04-30

Your Python code may run correctly, but you need it to run faster. Updated for Python 3, this expanded edition shows you how to locate performance bottlenecks and significantly speed up your code in high-data-volume programs. By exploring the fundamental theory behind design choices, High Performance Python helps you gain a deeper understanding of Python’s implementation. How do you take advantage of multicore architectures or clusters? Or build a system that scales up and down without losing reliability? Experienced Python programmers will learn concrete solutions to many issues, along with war stories from companies that use high-performance Python for social media analytics, productionized machine learning, and more. Get a better grasp of NumPy, Cython, and profilers Learn how Python abstracts the underlying computer architecture Use profiling to find bottlenecks in CPU time and memory usage Write efficient programs by choosing appropriate data structures Speed up matrix and vector computations Use tools to compile Python down to machine code Manage multiple I/O and computational operations concurrently Convert multiprocessing code to run on local or remote clusters Deploy code faster using tools like Docker

Advances in Cryptology – EUROCRYPT ’97 - Walter Fumy 2003-05-15

EUROCRYEVr '97, the 15th annual EUROCRYPT conference on the theory and application of cryptographic techniques, was organized and sponsored by the International Association for Cryptologic Research (IACR). The IACR organizes two series of international conferences each year, the EUROCRYPT meeting in Europe and CRWTO in the United States. The history of EUROCRYFT started 15 years ago in Germany with the Burg Feuerstein Workshop (see Springer LNCS 149 for the proceedings). It was due to Thomas Beth's initiative and hard work that the 76 participants from 14 countries gathered in Burg Feuerstein for the first open meeting in Europe devoted to modem cryptography. I am proud to have been one of the participants and still fondly remember my first encounters with some of the celebrities in cryptography. Since those early days the conference has been held in a different location in Europe each year (Udine, Paris, Linz, Linkoping, Amsterdam, Davos, Houthalen, Aarhus, Brighton, Balantonfiired, Lofthus, Perugia, Saint-Malo, Saragossa) and it has enjoyed a steady growth, Since the second conference (Udine, 1983) the IACR has been involved, since the Paris meeting in 1984, the name EUROCRYPT has been used. For its 15th anniversary, EUROCRYPT finally returned to Germany. The scientific program for EUROCRYPT '97 was put together by a 18-member program committee whch considered 104 high-quality submissions. These proceedings contain the revised versions of the 34 papers that were accepted for presentation. In addition, there were two invited talks by Ernst Bovelander and by Gerhard Frey.

Modern Cryptography, Probabilistic Proofs and Pseudorandomness - Oded Goldreich 2013-03-09

Cryptography is one of the most active areas in current mathematics research and applications. This book focuses on cryptography along with two related areas: the study of probabilistic proof systems, and the theory of computational pseudorandomness. Following a common theme that explores the interplay between randomness and computation, the important notions in each field are covered, as well as novel ideas and insights.

Fundamentals of Information Systems Security - David Kim 2021-12-10
Fundamentals of Information Systems Security, Fourth Edition provides a comprehensive overview of the essential concepts readers must know as they pursue careers in information systems security.

Winning Together - Bruno Verdini Trejo 2017-12-15
Strategies for transboundary natural resource management; winner of Harvard Law School's Raiffa Award for best research of the year in negotiation and conflict resolution. Transboundary natural resource negotiations, often conducted in an atmosphere of entrenched mistrust, confrontation, and deadlock, can go on for decades. In this book, Bruno Verdini outlines an approach by which government, private sector, and nongovernmental stakeholders can overcome grievances, break the status quo, trade across differences, and create mutual gains in high-stakes water, energy, and environmental negotiations. Verdini examines two landmark negotiations between the United States and Mexico. The two cases—one involving conflict over shared hydrocarbon reservoirs in the Gulf of Mexico and the other involving disputes over the shared waters of the Colorado River—resulted in groundbreaking agreements in 2012, after decades of deadlock. Drawing on his extensive interviews with more than seventy high-ranking negotiators in the United States and Mexico—from presidents and ambassadors to general managers, technical experts, and nongovernmental advocates—Verdini offers detailed accounts from multiple points of view, on both sides of the border. He unpacks the negotiation, leadership, collaborative decision-making, and political communication strategies that made agreement possible. Building upon the theoretical and empirical findings, Verdini offers advice for practitioners on effective negotiation and dispute resolution strategies that avoid the presumption that there are not enough resources to go around, and that one side must win and the other must inevitably lose. This investigation is the winner of Harvard Law School's Howard Raiffa Award for best research of the year in negotiation, mediation, decision-making, and dispute resolution.

Notes and Queries - 1859

Proceedings of the ... International Joint Conference on Artificial Intelligence - 1981