Aes Vhdl Code

As recognized, adventure as with ease as experience approximately lesson, amusement, as without difficulty as harmony can be gotten by just checking out a book **Aes Vhdl Code** with it is not directly done, you could understand even more regarding this life, a propos the world.

We allow you this proper as well as simple showing off to get those all. We pay for Aes Vhdl Code and numerous book collections from fictions to scientific research in any way. among them is this Aes Vhdl Code that can be your partner.

Innovative Security Solutions for Information Technology and Communications - Diana Maimut 2021-02-03
This book constitutes the thoroughly refereed post-conference proceedings of the 13th International Conference on Security for Information Technology and Communications, SecITC 2020, held in Bucharest, Romania, in November 2020. The 17 revised full papers presented together with 2 invited talks were carefully reviewed and selected from 41 submissions. The conference covers topics from cryptographic algorithms, to digital forensics and cyber security and much more.
ICCWS 2022 17th International Conference on Cyber Warfare and Security - 2022-03-17

International Conference on Multi disciplinary Technologies and challenges in Industry 4.0 - Dr. Prakash s, dr. Silvia liberataullo, dr. Yogesh g s, dr. I manimozhi, prof. Shilpa patil.

Topics in Cryptology - CT-RSA 2001 - David Naccache 2003-06-29
You are holding the rst in a hopefully long and successful series of RSA Cr- tographers' Track proceedings. The Cryptographers' Track (CT-RSA) is one of the many parallel tracks of the yearly RSA Conference. Other sessions deal with government projects, law and policy issues, freedom and privacy news, analysts' opinions, standards, ASPs, biotech and healthcare, nance, telecom and wireless security, developers, new products, implementers, threats, RSA products, VPNs, as well as cryp- graphy and enterprise tutorials. RSA Conference 2001 is expected to continue the tradition and remain the largest computer security event ever staged: 250 vendors, 10,000 visitors and 3,000 class-going attendees are expected in San Francisco next year. I am very grateful to the 22 members of the program committee for their hard work. The program committee received 65 submissions (one of which was later withdrawn) for which review was conducted electronically; almost all papers had at least two reviews although most had three or more. Eventually, we accepted the 33 papers that appear in these proceedings. Revisions were not checked on their scienti c aspects and some authors will write nal versions of their papers for publication in refereed journals. As is usual, authors bear full scienti c and paternity responsibilities for the contents of their papers.
Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems - Yeliz Karaca 2022-07-01
Multi-Chaos, Fractal and Multi-Fractional Artificial Intelligence of Different Complex Systems addresses different uncertain processes inherent in the complex systems, attempting to provide global and robust optimized solutions distinctively through multifarious methods, technical analyses, modeling, optimization processes, numerical simulations, case studies as well as applications including theoretical aspects of

complexity. Foregrounding Multi-chaos, Fractal and Multi-fractional in the era of Artificial Intelligence (AI), the edited book deals with multi-chaos, fractal, multifractional, fractional calculus, fractional operators, quantum, wavelet, entropy-based applications, artificial intelligence, mathematics-informed and data driven processes aside from the means of modelling, and simulations for the solution of multifaceted problems characterized by nonlinearity, non-regularity and self-similarity, frequently encountered in different complex systems. The fundamental interacting components underlying complexity, complexity thinking, processes and theory along with computational processes and technologies, with machine learning as the core component of AI demonstrate the enabling of complex data to augment some critical human skills. Appealing to an interdisciplinary network of scientists and researchers to disseminate the theory and application in medicine, neurology, mathematics, physics, biology, chemistry, information theory, engineering, computer science, social sciences and other far-reaching domains, the overarching aim is to empower out-of-the-box thinking through multifarious methods, directed towards paradoxical situations, uncertain processes, chaotic, transient and nonlinear dynamics of complex systems. Constructs and presents a multifarious approach for critical decision-making processes embodying paradoxes and uncertainty. Includes a combination of theory and applications with regard to multi-chaos, fractal and multi-fractional as well as AI of different complex systems and many-body systems. Provides readers with a bridge between application of advanced computational mathematical methods and AI based on comprehensive analyses and broad theories.

Cryptology and Network Security - Sara Foresti 2016-10-30

This book constitutes the refereed proceedings of the 15th International Conference on Cryptology and Network Security, CANS 2016, held in Milan, Italy, in November 2016. The 30 full papers presented together with 18 short papers and 8 poster papers were carefully reviewed and selected from 116 submissions. The papers are organized in the following topical sections: cryptanalysis of symmetric key; side channel attacks and implementation; lattice-based cryptography, virtual private network; signatures and hash; multi party computation; symmetric cryptography and authentication; system security, functional and homomorphic encryption; information theoretic security; malware and attacks; multi party computation and functional encryption; and network security, privacy, and authentication.

Topics in Cryptology – CT-RSA 2017 - Helena Handschuh 2017-01-09

This book constitutes the refereed proceedings of the Cryptographer's Track at the RSA Conference 2017, CT-RSA 2017, held in San Francisco, CA, USA, in February 2017. The 25 papers presented in this volume were carefully reviewed and selected from 77 submissions. CT-RSA has become a major publication venue in cryptography. It covers a wide variety of topics from public-key to symmetric key cryptography and from cryptographic protocols to primitives and their implementation security. This year selected topics such as cryptocurrencies and white-box cryptography were added to the call for papers.

Advances in Electrical and Computer Technologies - Thangaprakash Sengodan 2020-09-07

The book comprises select proceedings of the first International Conference on Advances in Electrical and Computer Technologies 2019 (ICAECT 2019). The papers presented in this book are peer reviewed and cover wide range of topics in Electrical and Computer Engineering fields. This book contains the papers presenting the latest developments in the areas of Electrical, Electronics, Communication systems and Computer Science such as smart grids, soft computing techniques in power systems, smart energy management systems, power electronics, feedback control systems, biomedical engineering, geo informative systems, grid computing, data mining, image and signal processing, video processing, computer vision, pattern recognition, cloud computing, pervasive computing, intelligent systems, artificial intelligence, neural network and fuzzy logic, broad band communication, mobile and optical communication, network security, VLSI, embedded systems, optical networks and wireless communication. This book will be of great use to the researchers and students in the areas of Electrical and Electronics Engineering, Communication systems and Computer Science.

Field Programmable Logic and Application - Jürgen Becker 2004-08-19
This book constitutes the refereed proceedings of the 13th International Conference on Field-Programmable Logic and Applications, FPL 2003, held in Lisbon, Portugal in September 2003. The 90 revised full papers and 56 revised poster papers presented were carefully reviewed and selected from 216 submissions. The papers are organized in topical sections on technologies and trends, communications applications, high level design tools, reconfigurable architecture, cryptographic applications, multi-context FPGAs, low-power issues, run-time reconfiguration, compilation tools, asynchronous techniques, bio-related applications, codesign, reconfigurable fabrics, image processing applications, SAT techniques, application-specific architectures, DSP applications, dynamic reconfiguration, SoC architectures, emulation, cache design, arithmetic, bio-inspired design, SoC design, cellular applications, fault analysis, and network applications.
Advanced FPGA Design - Steve Kilts 2007-06-18
This book provides the advanced issues of FPGA design as the underlying theme of the work. In practice, an engineer typically needs to be mentored for several years before these principles are appropriately utilized. The topics that will be discussed in this book are essential to designing FPGA's beyond moderate complexity. The goal of the book is to present practical design techniques that are otherwise only available through mentorship and real-world experience.
FCCM 2004 - Jeffrey M. Arnold 2004
FCCM presents recent work on the use of reconfigurable logic as computing elements. The proceedings focuses on topics such as device architecture, system architecture, compilation and programming tools, run time environments, nano technology, and applications.
MIPS Pipeline Cryptoprocessor - Kirat Pal Singh 2012-11-01
The design and implementation of a crypto processor based on Cryptographic algorithms can be used in wide range of electronic devices, include PCs, PDAs, hardware security modules, web servers etc. The growing problem of breaches in information security in recent years has created a demand for earnest efforts towards ensuring security in electronic processors. The successful deployment of these electronic processors for ecommerce, Internet banking, government online services, VPNs, mobile commerce etc., are dependent on the effectiveness of the security solutions. These security concerns are further compounded when resource-constrained environments and real-time speed requirements have to be considered in next generation applications. Consequently, these IT and Network security issues have been a subject of intensive research in areas of computing, networking and cryptography these last few years. Computational methodologies, computer arithmetic, and encryption algorithms need deep investigation and research to obtain efficient integrations of crypto-processors, with desirable improvements and optimizations. Approaches on silicon achieve high values of speed and bandwidth.
Computer and Network Security - Jaydip Sen 2020-06-10
In the era of Internet of Things (IoT), and with the explosive worldwide growth of electronic data volume and the associated needs of processing, analyzing, and storing this data, several new challenges have emerged. Particularly, there is a need for novel schemes of secure authentication, integrity protection, encryption, and non-repudiation to protect the privacy of sensitive data and to secure systems. Lightweight symmetric key cryptography and adaptive network security algorithms are in demand for mitigating these challenges. This book presents state-of-the-art research in the fields of cryptography and security in computing and communications. It covers a wide range of topics such as machine learning, intrusion detection, steganography, multi-factor authentication, and more. It is a valuable reference for researchers, engineers, practitioners, and graduate and doctoral students working in the fields of cryptography, network security, IoT, and machine learning.
Security of Internet of Things Nodes - Chinmay Chakraborty 2021-08-31
The book Security of Internet of Things Nodes: Challenges, Attacks, and Countermeasures® covers a wide range of research topics on the security of the Internet of Things nodes along with the latest research development in the domain of Internet of Things. It also covers various

algorithms, techniques, and schemes in the field of computer science with state-of-the-art tools and technologies. This book mainly focuses on the security challenges of the Internet of Things devices and the countermeasures to overcome security vulnerabilities. Also, it highlights trust management issues on the Internet of Things nodes to build secured Internet of Things systems. The book also covers the necessity of a system model for the Internet of Things devices to ensure security at the hardware level.

Cryptography: Breakthroughs in Research and Practice - Management Association, Information Resources 2019-12-06

Advances in technology have provided numerous innovations that make people's daily lives easier and more convenient. However, as technology becomes more ubiquitous, corresponding risks also increase. The field of cryptography has become a solution to this ever-increasing problem. Applying strategic algorithms to cryptic issues can help save time and energy in solving the expanding problems within this field. Cryptography: Breakthroughs in Research and Practice examines novel designs and recent developments in cryptographic security control procedures to improve the efficiency of existing security mechanisms that can help in securing sensors, devices, networks, communication, and data. Highlighting a range of topics such as cyber security, threat detection, and encryption, this publication is an ideal reference source for academicians, graduate students, engineers, IT specialists, software engineers, security analysts, industry professionals, and researchers interested in expanding their knowledge of current trends and techniques within the cryptology field.

CASES 2004 - International Conference on Compilers, Architectures and Synthesis for Embedded Systems 2004

The Design of Rijndael - Joan Daemen 2013-03-09

An authoritative and comprehensive guide to the Rijndael algorithm and Advanced Encryption Standard (AES). AES is expected to gradually replace the present Data Encryption Standard (DES) as the most widely applied data encryption technology. This book, written by the designers of the block cipher, presents Rijndael from scratch. The underlying mathematics and the wide trail strategy as the basic design idea are explained in detail and the basics of differential and linear cryptanalysis are reworked. Subsequent chapters review all known attacks against the Rijndael structure and deal with implementation and optimization issues. Finally, other ciphers related to Rijndael are presented.

Advanced Machine Learning Technologies and Applications - Aboul Ella Hassanien 2012-12-03

This book constitutes the refereed proceedings of the First International Conference on Advanced Machine Learning Technologies and Applications, AMLTA 2012, held in Cairo, Egypt, in December 2012. The 58 full papers presented were carefully reviewed and selected from 99 intial submissions. The papers are organized in topical sections on rough sets and applications, machine learning in pattern recognition and image processing, machine learning in multimedia computing, bioinformatics and cheminformatics, data classification and clustering, cloud computing and recommender systems.

Financial Cryptography and Data Security - Radu Sion 2010-07-16

This book constitutes the thoroughly refereed post-conference proceedings of the 14th International Conference on Financial Cryptography and Data Security, FC 2010, held in Tenerife, Canary Islands, Spain in January 2010. The 19 revised full papers and 15 revised short papers presented together with 1 panel report and 7 poster papers were carefully reviewed and selected from 130 submissions. The papers cover all aspects of securing transactions and systems and feature current research focusing on both fundamental and applied real-world deployments on all aspects surrounding commerce security.

International Conference on Computer Applications - Telecommunications -

4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019 - Neeta Nain 2020-02-14

This book presents the proceedings of the 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), held on

May 9–10, 2019, at Malaviya National Institute of Technology (MNIT), Jaipur, India. The Internet of Things (IoT) promises to usher in a revolutionary, fully interconnected “smart” world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet could fundamentally change how people think about what it means to be “online”. The ICIotCT 2019 conference provided a platform to discuss advances in Internet of Things (IoT) and connected technologies, such as various protocols and standards. It also offered participants the opportunity to interact with experts through keynote talks, paper presentations and discussions, and as such stimulated research. With the recent adoption of a variety of enabling wireless communication technologies, like RFID tags, BLE, ZigBee, embedded sensor and actuator nodes, and various protocols such as CoAP, MQTT and DNS, IoT has moved on from its infancy. Today smart sensors can collaborate directly with machines to automate decision-making or to control a task without human involvement. Further, smart technologies, including green electronics, green radios, fuzzy neural approaches, and intelligent signal processing techniques play an important role in the development of the wearable healthcare devices.

Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks - R.R. Brooks 2004-11-29

The traditional fortress mentality of system security has proven ineffective to attacks by disruptive technologies. This is due largely to their reactive nature. Disruptive security technologies, on the other hand, are proactive in their approach to attacks. They allow systems to adapt to incoming threats, removing many of the vulnerabilities explo

Design based Research - Kirat Pal SIngh

Author Impact

Design Recipes for FPGAs: Using Verilog and VHDL - Peter Wilson 2011-02-24

Design Recipes for FPGAs: Using Verilog and VHDL provides a rich toolbox of design techniques and templates to solve practical, every-day problems using FPGAs. Using a modular structure, the book gives ‘easy-to-find’ design techniques and templates at all levels, together with functional code. Written in an informal and ‘easy-to-grasp’ style, it goes beyond the principles of FPGA s and hardware description languages to actually demonstrate how specific designs can be synthesized, simulated and downloaded onto an FPGA. This book's ‘easy-to-find’ structure begins with a design application to demonstrate the key building blocks of FPGA design and how to connect them, enabling the experienced FPGA designer to quickly select the right design for their application, while providing the less experienced a ‘road map’ to solving their specific design problem. The book also provides advanced techniques to create ‘real world’ designs that fit the device required and which are fast and reliable to implement. This text will appeal to FPGA designers of all levels of experience. It is also an ideal resource for embedded system development engineers, hardware and software engineers, and undergraduates and postgraduates studying an embedded system which focuses on FPGA design. A rich toolbox of practical FGPA design techniques at an engineer's finger tips Easy-to-find structure that allows the engineer to quickly locate the information to solve their FGPA design problem, and obtain the level of detail and understanding needed

Top-Down Digital VLSI Design - Hubert Kaeslin 2014-12-04

Top-Down VLSI Design: From Architectures to Gate-Level Circuits and FPGAs represents a unique approach to learning digital design. Developed from more than 20 years teaching circuit design, Doctor Kaeslin’s approach follows the natural VLSI design flow and makes circuit design accessible for professionals with a background in systems engineering or digital signal processing. It begins with hardware architecture and promotes a system-level view, first considering the type of intended application and letting that guide your design choices. Doctor Kaeslin presents modern considerations for handling circuit complexity, throughput, and energy efficiency while preserving functionality. The book focuses on application-specific integrated circuits (ASICs), which along with FPGAs are increasingly used to develop products with applications in telecommunications, IT security,

biomedical, automotive, and computer vision industries. Topics include field-programmable logic, algorithms, verification, modeling hardware, synchronous clocking, and more. Demonstrates a top-down approach to digital VLSI design. Provides a systematic overview of architecture optimization techniques. Features a chapter on field-programmable logic devices, their technologies and architectures. Includes checklists, hints, and warnings for various design situations. Emphasizes design flows that do not overlook important action items and which include alternative options when planning the development of microelectronic circuits.

Cryptographic Hardware and Embedded Systems -- CHES 2010 - Stefan Mangard 2010-08-08

Annotation This book constitutes the refereed proceedings of the 12th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2010, held in Santa Barbara, USA during August 17-20, 2010. This year it was co-located with the 30th International Cryptology Conference (CRYPTO). The book contains 2 invited talks and 30 revised full papers which were carefully reviewed and selected from from 108 submissions. The papers are organized in topical sections on low cost cryptography, efficient implementation, side-channel attacks and countermeasures, tamper resistance, hardware trojans, PUFs and RNGs.

Analysis, Architectures and Modelling of Embedded Systems - Achim Rettberg 2009-09-04

This book presents the technical program of the International Embedded Systems Symposium (IESS) 2009. Timely topics, techniques and trends in embedded system design are covered by the chapters in this volume, including modelling, simulation, verification, test, scheduling, platforms and processors. Particular emphasis is paid to automotive systems and wireless sensor networks. Sets of actual case studies in the area of embedded system design are also included. Over recent years, embedded systems have gained an enormous amount of proce- ing power and functionality and now enter numerous application areas, due to the fact that many of the formerly external components can now be integrated into a single System-on-Chip. This tendency has resulted in a dramatic reduction in the size and cost of embedded systems. As a unique technology, the design of embedded systems is an essential element of many innovations. Embedded systems meet their performance goals, including real-time constraints, through a combination of special-purpose hardware and software components tailored to the system requirements. Both the development of new features and the reuse of existing intellectual property components are essential to keeping up with ever more demanding customer requirements. Furthermore, design complexities are steadily growing with an increasing number of components that have to cooperate properly. Embedded system designers have to cope with multiple goals and constraints simul- neously, including timing, power, reliability, dependability, maintenance, packaging and, last but not least, price.

Inventive Communication and Computational Technologies - G. Ranganathan 2022-01-11

This book gathers selected papers presented at the Inventive Communication and Computational Technologies conference (ICICCT 2021), held on 25–26 June 2021 at Gnanamani College of Technology, Tamil Nadu, India. The book covers the topics such as Internet of things, social networks, mobile communications, big data analytics, bio-inspired computing, and cloud computing. The book is exclusively intended for academics and practitioners working to resolve practical issues in this area.

Effective Coding with VHDL - Ricardo Jasinski 2016-05-27

A guide to applying software design principles and coding practices to VHDL to improve the readability, maintainability, and quality of VHDL code. This book addresses an often-neglected aspect of the creation of VHDL designs. A VHDL description is also source code, and VHDL designers can use the best practices of software development to write high-quality code and to organize it in a design. This book presents this unique set of skills, teaching VHDL designers of all experience levels how to apply the best design principles and coding practices from the software world to the world of hardware. The concepts introduced here will help readers write code that is easier to understand and more likely to be correct, with improved readability, maintainability, and overall

quality. After a brief review of VHDL, the book presents fundamental design principles for writing code, discussing such topics as design, quality, architecture, modularity, abstraction, and hierarchy. Building on these concepts, the book then introduces and provides recommendations for each basic element of VHDL code, including statements, design units, types, data objects, and subprograms. The book covers naming data objects and functions, commenting the source code, and visually presenting the code on the screen. All recommendations are supported by detailed rationales. Finally, the book explores two uses of VHDL: synthesis and testbenches. It examines the key characteristics of code intended for synthesis (distinguishing it from code meant for simulation) and then demonstrates the design and implementation of testbenches with a series of examples that verify different kinds of models, including combinational, sequential, and FSM code. Examples from the book are also available on a companion website, enabling the reader to experiment with the complete source code.

The Designer's Guide to VHDL - Peter J. Ashenden 2010-10-07

VHDL, the IEEE standard hardware description language for describing digital electronic systems, has recently been revised. The Designer's Guide to VHDL has become a standard in the industry for learning the features of VHDL and using it to verify hardware designs. This third edition is the first comprehensive book on the market to address the new features of VHDL-2008. First comprehensive book on VHDL to incorporate all new features of VHDL-2008, the latest release of the VHDL standard Helps readers get up to speed quickly with new features of the new standard Presents a structured guide to the modeling facilities offered by VHDL Shows how VHDL functions to help design digital systems Includes extensive case studies and source code used to develop testbenches and case study examples Helps readers gain maximum facility with VHDL for design of digital systems

Proceedings of the Eleventh National Conference on Communications - 2005

Reconfigurable Computing: Architectures, Tools and Applications - Jürgen Becker 2009-03-09

Recon?gurable computing (RC) technologies o?er the promise of substantial performance gains over traditional architectures by customizing, sometimes at run-time, the topology of the underlying architecture to match the speci?c needs of a given application. Contemporary con?gurable architectures allow for the de?nition of architectures with functional and storage units that match the s- ci?c needs of a given computation, in terms of function, bit-width and control structures. Compared to standard microprocessor architectures, advantages are possible in terms of power consumption on a broad range of di?erent application ?elds. Moreover, the ?exibility enabled by recon?guration is also seen as a basic technique for overcoming transient failures in emerging device structures. Techniques for achieving recon?gurable systems are numerous and require the joint development of recon?gurable hardware systems to support the dynamic behavior, e.g., suitable programming models, tools and languages, to support the recon?guration process during run-time as well as during design-time. This includes veri?cation techniques that can demonstrate formally correct recon?- ration sequences at each stage. While there are many problems, the existence and development of technologies such as recent multi- and many-core processor arc- tectures, dynamically recon?gurable and multi-grain computing architectures, as well as application-speci?c processors suggest that there is a very strong need for adaptive and recon?gurable systems.

Topics in Cryptology, CT-RSA ... - 2001

System-on-Chip Architectures and Implementations for Private-Key Data Encryption - Máire McLoone 2012-12-06

In System-on-Chip Architectures and Implementations for Private-Key Data Encryption, new generic silicon architectures for the DES and Rijndael symmetric key encryption algorithms are presented. The generic architectures can be utilised to rapidly and effortlessly generate system-on-chip cores, which support numerous application requirements, most importantly, different modes of operation and encryption and decryption

capabilities. In addition, efficient silicon SHA-1, SHA-2 and HMAC hash algorithm architectures are described. A single-chip Internet Protocol Security (IPSec) architecture is also presented that comprises a generic Rijndael design and a highly efficient HMAC-SHA-1 implementation. In the opinion of the authors, highly efficient hardware implementations of cryptographic algorithms are provided in this book. However, these are not hard-fast solutions. The aim of the book is to provide an excellent guide to the design and development process involved in the translation from encryption algorithm to silicon chip implementation.

Nanoelectronics, Circuits and Communication Systems - Vijay Nath 2020-04-01

This book features selected papers presented at the Fourth International Conference on Nanoelectronics, Circuits and Communication Systems (NCCS 2018). Covering topics such as MEMS and nanoelectronics, wireless communications, optical communications, instrumentation, signal processing, the Internet of Things, image processing, bioengineering, green energy, hybrid vehicles, environmental science, weather forecasting, cloud computing, renewable energy, RFID, CMOS sensors, actuators, transducers, telemetry systems, embedded systems, and sensor network applications in mines, it offers a valuable resource for young scholars, researchers, and academics alike.

VHDL-2008 - Peter J. Ashenden 2007-11-26

VHDL-2008: Just the New Stuff, as its title says, introduces the new features added to the latest revision of the IEEE standard for the VHDL hardware description language. Written by the Chair and Technical Editor of the IEEE working group, the book is an authoritative guide to how the new features work and how to use them to improve design productivity. It will be invaluable for early adopters of the new language version, for tool implementers, and for those just curious about where VHDL is headed. * First in the market describing the new features of VHDL 2008; * Just the new features, so existing users and implementers can focus on what's new; * Helps readers to learn the new features soon, rather than waiting for new editions of complete VHDL reference books. * Authoritative, written by experts in the area; * Tutorial style, making it more accessible than the VHDL Standard Language Reference Manual.

Towards Hardware-Intrinsic Security - Ahmad-Reza Sadeghi 2010-11-03

Hardware-intrinsic security is a young field dealing with secure secret key storage. By generating the secret keys from the intrinsic properties of the silicon, e.g., from intrinsic Physical Unclonable Functions (PUFs), no permanent secret key storage is required anymore, and the key is only present in the device for a minimal amount of time. The field is extending to hardware-based security primitives and protocols such as block ciphers and stream ciphers entangled with the hardware, thus improving IC security. While at the application level there is a growing interest in hardware security for RFID systems and the necessary accompanying system architectures. This book brings together contributions from researchers and practitioners in academia and industry, an interdisciplinary group with backgrounds in physics, mathematics, cryptography, coding theory and processor theory. It will serve as important background material for students and practitioners, and will stimulate much further research and development.

Report on the Development of the Advanced Encryption Standard (AES) - James Nechvatal 2001-12-01

In 1997, NIST initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitive (unclass.) Fed. info. In 1998, NIST announced the acceptance of 15 candidate algorithms and requested the assistance of the cryptographic research community in analyzing the candidates. This analysis included an initial exam. of the security and efficiency characteristics for each algorithm. NIST reviewed the results of this research and selected MARS, RC, Rijndael, Serpent and Twofish as finalists. After further public analysis of the finalists, NIST has decided to propose Rijndael as the AES. The research results and rationale for this selection are documented here.

Low Power Design with High-Level Power Estimation and Power-Aware Synthesis - Sumit Ahuja 2011-10-22

This book presents novel research techniques, algorithms, methodologies and experimental results for high level power estimation and power aware high-level synthesis. Readers will learn to apply such techniques

to enable design flows resulting in shorter time to market and successful low power ASIC/FPGA design.

Field-programmable Logic and Applications - 2002