Aes Vhdl Code

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.

Containing the papers presented at the first International Conference on Data Management and Security with applications in Medicine, Sciences and Engineering, this book focuses on the modern techniques applied in data management and knowledge acquisition with applications in a broad variety of fields. It also discusses recent developments in data security systems. Papers in the book cover such topics as Data and text mining; Ubiquitous devices; Numerical modelling; Expert systems; Databases; Cloud computing; Sensors and optechtronics; Heuristic methods and genetic algorithms; Knowledge discovery; Prediction modelling; Data streaming; Clustering; Decision support systems; Cryptography; Information and codification; Engineering Applications.

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.

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.

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.

This book constitutes the proceedings of the Third International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, held in Uppsala, Sweden, during June 3-5, 2009. The 86 papers contained in this volume were carefully reviewed and selected from numerous submissions. There are 13 main tracks covering the methodology and applications of agent and multi-agent systems and 8 special sessions on specific topics within the field. The papers are divided in topical sections on social and organizational structures of agents; negotiation protocols; mobile agents and robots; agent design and implementation; e-commerce; simulation systems and game systems; agent systems and ontologies; agents for network systems; communication and agent learning systems; Web services and semantic Web; self-organization in multi-agent systems; management and e-business; mobile and intelligent agents for networks and services; engineering interaction protocols; agent-based simulation, decision making and systems optimization; digital economy; agent-based optimization (ABO2009); distributed systems and artificial intelligence applications.

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.

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.

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.

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.

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.

"This proceeding is part of International Conference on Computer Applications 2010 - Telecommunications track which was held in Pondicherry, India from 24 Dec 2010 and 27 Dec 2010"--Pref.

These multiple volumes (LNCS volumes 6016, 6017, 6018 and 6019) consist of the peer-reviewed papers from the 2010 International Conference on Compu- tional Science and Its Applications (ICCSA2010)held in Fukuoka, Japanduring March23–26,2010.ICCSA2010wasasuccessfuleventintheInternationalC- ferences on Computational Science and Its Applications (ICCSA) conference - ries, previouslyheld in Suwon, South Korea (2009), Perugia, Italy (2008), Kuala Lumpur, Malaysia (2007), Glasgow, UK (2006), Singapore (2005), Assisi, Italy (2004), Montreal, Canada (2003), and (as ICCS) Amsterdam, The Netherlands (2002) and San Francisco, USA (2001). Computational science is a main pillar of most of the present research, - dustrial and commercial activities and plays a unique role in exploiting ICT - novative technologies. The ICCSA conference series has been providing a venue to researchers and industry practitioners to discuss new ideas, to share complex problems and their solutions, and to shape new trends in computational science. ICCSA 2010 was celebrated at the host university, Kyushu Sangyo Univ- sity, Fukuoka, Japan, as part of the university’s 50th anniversary.We would like to thank Kyushu Sangyo University for hosting ICCSA this year, and for - cluding this international event in their celebrations. Also for the ?rst time this year, ICCSA organized poster sessions that present on-going projects on various aspects of computational sciences.

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

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.

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

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.

Author Impact

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.

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.

Written for advanced study in digital systems design, Roth/John's DIGITAL SYSTEMS DESIGN USING VHDL, 3E integrates the use of the industry-standard hardware description language, VHDL, into the digital design process. The book begins with a valuable review of basic logic design concepts before introducing the fundamentals of VHDL. The book concludes with detailed coverage of advanced VHDL topics. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Reconfigurable Computing: Architectures, Tools and Applications5th International Workshop, ARC 2009, Karlsruhe, Germany, March 16-18, 2009, ProceedingsSpringer Science & Business Media

This book offers an in-depth study of the design and challenges addressed by a high-level synthesis tool targeting a specific class of cryptographic kernels, i.e. symmetric key cryptography. With the aid of detailed case studies, it also discusses optimization strategies that cannot be automatically undertaken by CRYKET (Cryptographic kernels toolkit. The dynamic nature of cryptography, where newer cryptographic functions and attacks frequently surface, means that such a tool can help cryptographers expedite the very large scale integration (VLSI) design cycle by rapidly exploring various design alternatives before reaching an optimal design option. Features include flexibility in cryptographic processors to support emerging cryptanalytic schemes; area-efficient multinational designs supporting various cryptographic functions; and design scalability on modern graphics processing units (GPUs). These case studies serve as a guide to cryptographers exploring the design of efficient cryptographic implementations.

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.

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

Papers from an October 2002 symposium describe research in areas including algorithms, artificial intelligence, computer graphics, computer networks, databases, evolutionary computation, graph theory, image processing, multimedia technology, software engineering, and software performance engineering. Some specific topics are packet selection in a deflection routing algorithm, honeycomb subdivision, a new image-based lighting method, visualizing transition diagrams of action language programs, and solution stability in evolutionary computation. Other subjects include control of lightpaths in heterogeneous optical networks, exploiting semantic constraints in a database browser, and bandwidth allocation in bluetooth scatternets. There is no subject index. Annotation copyrighted by Book News, Inc., Portland, OR

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.

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.

Tradeoffs of speed vs. area that are inherent in the design of a security coprocessor are explored. Encryption, decryption, and key generation engines for AES in Cipher Block Chaining and Electronic Code Book modes were developed using VHDL. Two designs are discussed. The "space-optimised" design required 1454 FPGA CLB slices for the Cipher implementation (4016 for the complete design) and produced a round delay of - 16.75 ns. The throughput in CBC mode was 636.82 Mbps (depending on the FPGA utilized), which is greater than various published prior works. The Multi-Session Pipelined approach followed a novel architecture that required 13675 CLB slices total and produced a round delay of - 20 ns. The Multi-Session Pipelined AES design can obtain an aggregate throughput of - 6.40 Gbps and is capable of operating in CBC mode. The 1 Ox speedup over the "space-optimised" design required 3.4 ?the total number of FPGA CLB slices.

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.

This book constitutes the carefully refereed post-proceedings of the 6th Symposium on Foundations and Practice of Security, FPS 2013, held in La Rochelle, France, in October 2013. The 25 revised full papers presented together with a keynote address were carefully reviewed and selected from 65 submissions. The papers are organized in topical sections on security protocols, formal methods, physical security, attack classification and assessment, access control, cipher attacks, ad-hoc and sensor networks, resilience and intrusion detection.

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.

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.

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.