Vhdl Implementation Of Aes 128 Smanticscholar

This book constitutes the proceedings of the 19th International Conference on Cryptographic Hardware and Embedded Systems, CHES 2017, held in Taipei, Taiwan, in September 2017. The 33 full papers presented in this volume were carefully reviewed and selected from 130 submissions. The annual CHES conference highlights new results in the design and analysis of cryptographic hardware and soft- ware implementations. The workshop builds a valuable bridge between the research and cryptographic engineering communities and attracts participants from industry, academia, and government organizations.

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.

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.

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.

Proceedings of the 2nd International Conference on Communications and Cyber Physical Engineering

17th International Conference, CARDIS 2018, Montpellier, France, November 12–14, 2018, Revised Selected Papers

4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019

22nd International Symposium, VDAT 2018, Madurai, India, June 28-30, 2018, Revised Selected Papers

Architectures, Design Methods and Applications

International Joint Conference, ICETE 2013, Reykjavik, Iceland, July 29-31, 2013, Revised Selected Papers

Proceedings of Fifth International Conference on Soft Computing for Problem Solving

E-Business and Telecommunications

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 proceedings of SocProS 2015 will serve as an academic bonanza for scientists and researchers working in the field of Soft Computing. This book contains theoretical as well as practical aspects using fuzzy logic, neural networks,

evolutionary algorithms, swarm intelligence algorithms, etc., with many applications under the umbrella of 'Soft Computing'. The book will be beneficial for young as well as experienced researchers dealing across complex and intricate real world problems for which finding a solution by traditional methods is a difficult task. The different application areas covered in the proceedings are: Image Processing, Cryptanalysis, Industrial Optimization, Supply Chain Management, Newly Proposed Nature Inspired Algorithms, Signal Processing, Problems related to Medical and Health Care, Networking Optimization Problems, etc.

Advances in Computing, Communication, Automation and Biomedical Technology aims to bring together leading academic, scientists, researchers, industry representatives, postdoctoral fellows and research scholars around the world to share their knowledge and research expertise, to advances in the areas of Computing, Communication, Electrical, Civil, Mechanical and Biomedical Systems as well as to create a prospective collaboration and networking on various areas. It also provides a premier interdisciplinary platform for researchers, practitioners, and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered, and solutions adopted in the fields of innovation.

This book constitutes the refereed proceedings of the 10th International Joint Conference on E-Business and Telecommunications, ICETE 2013, held in Reykjavik, Iceland, in July 2013. ICETE is a joint international conference integrating four major areas of knowledge that are divided into six corresponding conferences: International Conference on Data Communication Networking, DCNET; International Conference on E-Business, ICE-B; International Conference on Optical Communication Systems, OPTICS; International Conference on Security and Cryptography, SECRYPT; International Conference on Wireless Information Systems, WINSYS; and International Conference on Signal Processing and Multimedia, SIGMAP. The 24 full papers presented were carefully reviewed and selected from 341 submissions. The papers cover the following key areas of e-business and telecommunications: data communication networking, e-business, optical communication systems, security and cryptography, signal processing and multimedia applications, wireless information networks and systems.

Topics in Cryptology – CT-RSA 2017
14th International Conference, FC 2010, Tenerife, Canary Islands, January 25-28, 2010, Revised Selected Papers
Innovative Security Solutions for Information Technology and Communications
Proceedings of the 5th International Workshop on Reconfigurable Communication-centric Systems on Chip 2010 - ReCoSoC'10
4th International Conference, EuroMed 2012, Lemessos, Cyprus, October 29 -- November 3, 2012, Proceedings
Cryptographic Hardware and Embedded Systems – CHES 2017
System-on-Chip Architectures and Implementations for Private-Key Data Encryption
Towards Hardware-Intrinsic Security

This book const í tutes the thoroughly refereed postproceedings of the 4th International Conference on the Advanced Encryption Standard, AES 2004, held in Bonn, Germany in May 2004. The 10 revised full papers presented together with an introductory survey and 4 invited papers by leading researchers were carefully selected during two rounds of reviewing and improvement. The papers are organized in topical sections on cryptanalytic attacks and related topics, algebraic attacks and related results, hardware implementations, and other topics. All in all, the papers constitute a most up-to-date assessment of the state of the art of data encryption using the Advanced Encryption Standard AES, the de facto world standard for data encryption.
MobiSec 2010 was the second ICST conference on security and privacy in mobile information and communication systems. With the vast area of mobile technology research and application, the intention behind the creation of MobiSec was to make a small, but unique contribution to build a bridge between top-level research and large scale application of novel kinds of information security for mobile devices and communication.
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.
This six-volume-set (CCIS 231, 232, 233, 234, 235, 236) constitutes the refereed proceedings of

the International Conference on Computing, Information and Control, ICCIC 2011, held in Wuhan, China, in September 2011. The papers are organized in two volumes on Innovative Computing and Information (CCIS 231 and 232), two volumes on Computing and Intelligent Systems (CCIS 233 and 234), and in two volumes on Information and Management Engineering (CCIS 235 and 236).

Proceeding of NCCS 2018

NCC-2005, 28-30 January, 2005

Proceedings of ICTIS 2020

Design Recipes for FPGAs: Using Verilog and VHDL

VHDL Implementation of a Security Co-processor

International Conference on Computer Applications - Telecommunications

Proceedings of ICICCT 2021

Select Proceedings of ICAECT 2019

This book constitutes the thoroughly refereed post-conference proceedings of the 17th International Conference on Smart Card Research and Advanced Applications, CARDIS 2018, held in Monpellier, France, in November 2018. The 13 revised full papers presented in this book were carefully reviewed and selected from 28 submissions. CARDIS has provided a space for security experts from industry and academia to exchange on security of smart cards and related applications.

Author Impact

This book gathers papers addressing state-of-the-art research in the areas of machine learning and predictive analysis, presented virtually at the Fourth International Conference on Information and Communication Technology for Intelligent Systems (ICTIS 2020), India. It covers topics such as intelligent agent and multi-agent systems in various domains, machine learning, intelligent information retrieval and business intelligence, intelligent information system development using design science principles, intelligent web mining and knowledge discovery systems.

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.

From Architectures to Gate-Level Circuits and FPGAs

Dynamically Reconfigurable Systems

First International Conference, AMLTA 2012, Cairo, Egypt, December 8-10, 2012, Proceedings

Report on the Development of the Advanced Encryption Standard (AES)

Architecture, Implementation, and Optimization

Field Programmable Logic and Application

Reconfigurable Computing: Architectures, Tools and Applications

Advanced Machine Learning Technologies and Applications

This book constitutes the refereed proceedings of the 22st International Symposium on VLSI Design and Test, VDAT 2018, held in Madurai, India, in June 2018. The 39 full papers and 11 short papers presented together with 8 poster papers were carefully reviewed and selected from 231 submissions. The papers are organized in topical sections named: digital design; analog and mixed signal design; hardware security; micro bio-fluidics; VLSI testing; analog circuits and devices; network-on-chip; memory; quantum computing and NoC; sensors and interfaces.

"The second edition of The Designer's Guide to VHDL sets a new standard in VHDL texts. I am certain that you will find it a very valuable addition to your library." --From the foreword by Paul Menchini, Menchini & AssociatesSince the publication of the first edition of The Designer's Guide to VHDL in 1996, digital electronic systems have increased exponentially in their complexity, product lifetimes have dramatically shrunk, and reliability requirements have shot through the roof. As a result more and more designers have turned to VHDL to help them dramatically improve productivity as well as the quality of their designs.VHDL, the IEEE standard hardware description language for describing digital electronic systems, allows engineers to describe the structure and specify the function of a digital system as well as simulate and test it before manufacturing. In addition, designers use VHDL to synthesize a more detailed structure of the design, freeing them to concentrate on more strategic design decisions and reduce time to market. Adopted by designers around the world, the VHDL family of standards have recently been revised to address a range of issues, including portability across synthesis tools.This best-selling comprehensive tutorial for the language and authoritative reference on its use in hardware design at all levels--from system to gates--has been revised to reflect the new IEEE standard, VHDL-2001. Peter Ashenden, a member of the IEEE VHDL standards committee, presents the entire description language and builds a modeling methodology based on successful software engineering techniques. Reviewers on Amazon.com have consistently rated the first edition with five stars. This second edition updates the first, retaining the authors unique ability to teach this complex subject to a broad audience of students and practicing professionals.Features: Details how the new standard allows for increased portability across tools. Covers related standards, including the Numeric Synthesis Package and the Synthesis Operability Package, demonstrating how they can be used for digital systems design. Presents four extensive case studies to demonstrate and combine features of the language taught across multiple chapters. Requires only a minimal background in programming, making it an excellent tutorial for anyone in computer architecture, digital systems engineering, or CAD.

This book is a collection research papers and articles from the 2nd International

Conference on Communications and Cyber-Physical Engineering (ICCCE – 2019), held in Pune, India in Feb 2019. Discussing the latest developments in voice and data communication engineering, cyber-physical systems, network science, communication software, image- and multimedia processing research and applications, as well as communication technologies and other related technologies, it includes contributions from both academia and industry.

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.

Progress in Cultural Heritage Preservation

May 17-19, 2010, Karlsruhe, Germany

Disruptive Security Technologies with Mobile Code and Peer-to-Peer Networks

Advanced Encryption Standard - AES

13th International Conference, SecITC 2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers

Advances in Computing, Communication, Automation and Biomedical Technology

Proceedings of the Eleventh National Conference on Communications

Computer and Network Security

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. 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 4th International Conference on Progress in Cultural Heritage Preservation, EuroMed 2012, held in Lemesos, Cyprus, in October/November 2012. The 95 revised full papers were carefully reviewed and selected from 392 submissions. The papers are organized in topical sections on digital data acquisition technologies and data processing in cultural heritage, 2D and 3D data capture methodologies and data processing in cultural heritage, 2D and 3D GIS in cultural heritage, virtual reality in archaeology and historical research, standards, metadata, ontologies and semantic processing in cultural heritage, data management, archiving and presentation of cultural heritage content, ICT assistance in monitoring and restoration, innovative topics related to the current and future implementation, use, development and exploitation of the EU CH identity card, innovative technologies to asses, monitor and adapt to climate change, digital data acquisition technologies and data processing in cultural heritage, 2D and 3D data capture methodologies and data processing in cultural heritage, on-site and remotely sensed data collection, reproduction techniques and rapid prototyping in cultural heritage, 2D and 3D GIS in cultural heritage, innovative graphics applications and techniques, libraries and archives in cultural heritage, tools for education, documentation and training in CH, standards, metadata, ontologies and semantic processing in cultural heritage, damage assessment, diagnoses and monitoring for the preventive conservation and maintenance of CH, information management systems in CH, European research networks in the field of CH, non-destructive diagnosis technologies for the safe conversation and traceability of cultural assets.

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.
International Conference, ICCIC 2011, Wuhan, China, September 17-18, 2011. Proceedings
Second International ICST Conference, MobiSec 2010, Catania, Sicily, Italy, May 27-28, 2010, Revised Selected Papers
SocProS 2015, Volume 2
Communication and Computing Systems
Proceedings of the International Conference on Communication and Computing Systems (ICCCS 2016), Gurgaon, India, 9-11 September, 2016
Advances in Electrical and Computer Technologies
Proceedings
Foundations and Practice

Advances in Electrical and Computer TechnologiesSelect Proceedings of ICAECT 2019Springer Nature

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.

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.

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.

Design based Research

Inventive Communication and Computational Technologies

Top-Down Digital VLSI Design

19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings

The Cryptographers' Track at the RSA Conference 2017, San Francisco, CA, USA, February 14-17, 2017, Proceedings

14th International Conference , FPL 2004, Leuven, Belgium, August 30-September 1, 2004, Proceedings

Smart Card Research and Advanced Applications

4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers

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.

Dynamically Reconfigurable Systems is the first ever to focus on the emerging field of Dynamically Reconfigurable Computing Systems. While programmable logic and design-time configurability are well elaborated and covered by various texts, this book presents a unique overview over the state of the art and recent results for dynamic and run-time reconfigurable computing systems. Reconfigurable hardware is not only of utmost importance for large manufacturers and vendors of microelectronic devices and systems, but also a very attractive technology for smaller and medium-sized companies. Hence, Dynamically Reconfigurable Systems also addresses researchers and engineers actively working in the field and provides them with information on the newest developments and trends in dynamic and run-time reconfigurable systems.

This book is a collection of accepted papers that were presented at the International Conference on Communication and Computing Systems

(ICCCS-2016), Dronacharya College of Engineering, Gurgaon, September 9–11, 2016. The purpose of the conference was to provide a platform for interaction between scientists from industry, academia and other areas of society to discuss the current advancements in the field of communication and computing systems. The papers submitted to the proceedings were peer-reviewed by 2-3 expert referees. This volume contains 5 main subject areas: 1. Signal and Image Processing, 2. Communication & Computer Networks, 3. Soft Computing, Intelligent System, Machine Vision and Artificial Neural Network, 4. VLSI & Embedded System, 5. Software Engineering and Emerging Technologies.
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.
AES - The Advanced Encryption Standard
Internet of Things and Connected Technologies
The Designer's Guide to VHDL
Academic Publications and Citations
Security and Privacy in Mobile Information and Communication Systems
The Design of Rijndael
5th International Workshop, ARC 2009, Karlsruhe, Germany, March 16-18, 2009, Proceedings
Nanoelectronics, Circuits and Communication Systems

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

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.

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 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.

VLSI Design and Test

Financial Cryptography and Data Security

Machine Learning for Predictive Analysis

Innovative Computing and Information

Advanced FPGA Design

ICCCE 2019

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