Rfid Mifare And Contactless Cards In Application

In the past several years, there has been an increasing trend in the use of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) as well as in the integration of both systems due to their complementary nature, flexible combination, and the demand for ubiquitous computing. As always, adequate security remains one of the open areas of concern before wide deployment of RFID and WSNs can be achieved. Security in RFID and Sensor Networks is the first book to offer a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and integrated RFID and WSNs, providing an essential reference for those who regularly interface with these versatile technologies. Exposes Security Risks The book begins with a discussion of current security issues that threaten the effective use of RFID technology. The contributors examine multi-tag systems, relay attacks, authentication protocols, lightweight cryptography, and host of other topics related to RFID safety. The book then shifts the focus to WSNs, beginning with a background in sensor network security before moving on to survey intrusion detection, malicious node detection, jamming, and other issues of concern to WSNs and their myriad of applications. Offers Viable Solutions In each chapter, the contributors propose effective solutions to the plethora of security challenges that confront users, offering practical examples to aid in intuitive understanding. The last part of the book reviews the security problems inherent in integrated RFID & WSNs. The book ends with a glimpse of the future possibilities in these burgeoning technologies and provides recommendations for the proactive design of secure wireless embedded systems.

This groundbreaking text examines the problem of user authentication from a completely new viewpoint. Rather than describing the requirements, technologies and implementation issues of designing point-of-entry authentication, the book introduces and investigates the technological requirements of implementing transparent user authentication – where authentication credentials are captured during a user’s normal interaction with a system. This approach would transform user authentication from a binary point-of-entry decision to a continuous identity confidence measure. Topics and features: discusses the need for user authentication; reviews existing authentication approaches; introduces novel behavioural biometrics techniques; examines the wider system-specific issues with designing large-scale multimodal authentication systems; concludes with a look to the future of user authentication.

The most comprehensive book on state-of-the-art smart card technology available Updated with new international standards and specifications, this essential fourth edition now covers all aspects of smart card in a completely revised structure. Its enlarged coverage now includes smart cards for passports and ID cards, health care cards, smart cards for public transport, and Java Card 3.0. New sub-chapters cover near field communication (NFC), single wire protocol (SWP), and multi megabyte smart cards (microcontroller with NAND-Flash). There are also extensive revisions to chapters on smart card production, the security of smart cards (including coverage of new attacks and protection methods), and contactless card data transmission (ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693). This edition also features: additional views to the future development of smart cards, such as USB, MMU, SWP, HCI, Flash memory and their usage; new internet technologies for smart cards; smart card web server, HTTP-Protocol, TCP/IP, SSL/TSL; integration of the new flash-based microcontrollers for smart cards (until now the usual ROM-based microcontrollers), and; a completely revised glossary with explanations of all important smart card subjects (600 glossary terms). Smart Card Handbook is firmly established as the definitive reference to every aspect of smart card technology, proving an invaluable resource for security systems development engineers. Professionals and microchip designers working in the smart card industry will continue to benefit from this essential guide. This book is also ideal for newcomers to the field. The Fraunhofer Smart Card Award was presented to the authors for the Smart Card Handbook, Third Edition in 2008.

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 most interesting talks given at ISSE 2011 – the forum for the inter-disciplinary discussion of how to adequately secure electronic business processes. The topics include: - Cloud Computing & Enterprise Security Services - Awareness, Education, Privacy & Trustworthiness - Smart Grids, Mobile & Wireless Security - Security Management, Identity & Access Management - eID & eGovernment - Device & Network Security Adequate information security is one of the basic requirements of all electronic business processes. It is crucial for effective solutions that the possibilities offered by security technology can be integrated with the commercial requirements of the applications. The reader may expect state-of-the-art: best papers of the Conference ISSE 2011.

"This set of books represents a detailed compendium of authoritative, research-based entries that define the contemporary state of knowledge on technology"--Provided by publisher.

"This book addresses security risks involved with RFID technologies, and gives insight on some possible solutions and preventions in dealing with these developing technologies"--

This volume constitutes the refereed proceedings of the 8th IFIP WG 11.2 International Workshop on Information Security Theory and Practices, WISTP 2014, held in Heraklion, Crete, Greece, in June/July 2014. The 8 revised full papers and 6 short papers presented together with 2 keynote talks were carefully reviewed and selected from 33 submissions. The papers have been organized in topical sections on cryptography and cryptanalysis, smart cards and embedded devices, and privacy.

This work provides an assessment of the current state of near field communication (NFC) security, it reports on new attack scenarios, and offers concepts and solutions to overcome any unresolved issues. The work describes application-specific security aspects of NFC based on exemplary use-case scenarios and uses these to focus on the interaction with NFC tags and on card emulation. The current security architectures of NFC-enabled cellular phones are evaluated with regard to the identified security aspects.

This book constitutes the refereed proceedings of the 5th International Conference on Ubiquitous Computing, UbiComp 2003, held in Seattle, WA, USA in Ocotber 2003. The 16 revised full papers and 11 technical note papers presented were carefully reviewed and selected from a total of 153 submissions. The papers are organized in topical sections on location and space, modeling and inference, context awareness, new devices and technologies, domestic environments and healthcare, social aspects and privacy, and new interfaces.

Electronic Access Control introduces the fundamentals of electronic access control through clear, well-illustrated explanations. Access Control Systems are difficult to learn and even harder to master due to the different ways in which manufacturers approach the subject and the myriad complications associated with doors, door frames, hardware, and electrified locks. This book consolidates this information, covering a comprehensive yet easy-to-read list of subjects that every Access Control System Designer, Installer, Maintenance Tech or Project Manager needs to know in order to develop quality and profitable Alarm/Access Control System installations. Within these pages, Thomas L. Norman - a master at electronic security and risk management consulting and author of the industry reference manual for the design of Integrated Security Systems - describes the full range of EAC devices (credentials, readers, locks, sensors, wiring, and computers), showing how they work, and how they are installed. A comprehensive introduction to all aspects of electronic access control Provides information in short bursts with ample illustrations Each chapter begins with outline of chapter contents and ends with a quiz May be used for self-study, or as a professional reference guide

This book constitutes the thoroughly refereed post-worksop proceedings of the 7th International Workshop Radio Frequency Identification: Security and Privacy Issues. RFIDSec 2011, held in Amherst, Massachusetts, USA, in June 2011. The 12 revised full papers presented were carefully reviewed and selected from 21 initial submissions for inclusion in the book. The papers focus on minimalism in cryptography, on-tag cryptography, securing RFID with physics, and protocol-level security in RFID.

Extend the range of your Arduino skills, incorporate the new developments in both hardware and software, and understand how the electronic applications function in everyday life. This project-based book extends the Arduino Uno starter kits and increases knowledge of microcontrollers in electronic applications. Learn how to build complex Arduino projects, break them down into smaller ones, and then enhance them, thereby broadening your understanding of each topic.You'll use the Arduino Uno in a range of applications such as a blinking LED, route mapping with a mobile GPS system, and uploading information to the internet. You'll also apply the Arduino Uno to sensors, collecting and displaying information, Bluetooth and wireless communications, digital image captures, route tracking with GPS, controlling motors, color and sound, building robots, and internet access. With Arduino Applied, prior knowledge of electronics is not required, as each topic is described and illustrated with examples using the Arduino Uno. What You'll Learn Set up the Arduino Uno and its programming environment Understand the application of electronics in every day systems Build projects with a microcontroller and readily available electronic components Who This Book Is For Readers with an Arduino starter-kit and little-to-no programming experience and those interested in "how electronic appliances work."

This is the third revised edition of the established and trusted RFID Handbook; the most comprehensive introduction to radio frequency identification (RFID) available. This essential new edition contains information on electronic product code (EPC) and the EPC global network, and explains near-field communication (NFC) in depth. It includes revisions on chapters devoted to the physical principles of RFID systems and microprocessors, and supplies up-to-date details on relevant standards and regulations. Taking into account critical modern concerns, this handbook provides the latest information on: the use of RFID in ticketing and electronic passports; the security of RFID systems, explaining attacks on RFID systems and other security matters, such as transponder emulation and cloning, defence using cryptographic methods, and electronic article surveillance; frequency ranges and radio licensing regulations. The text explores schematic circuits of simple transponders and readers, and includes new material on active and passive transponders, ISO/IEC 18000 family, ISO/IEC 15691 and 15692. It also describes the technical limits of RFID systems. A unique resource offering a complete overview of the large and varied world of RFID, Klaus Finkenzeller's volume is useful for end-users of the technology as well as practitioners in auto ID and IT designers of RFID products. Computer and electronics engineers in security system development, microchip designers, and materials handling specialists benefit from this book, as do automation, industrial and transport engineers. Clear and thorough explanations also make this an excellent introduction to the topic for graduate level students in electronics and industrial engineering design. Klaus Finkenzeller was awarded the Fraunhofer-Smart Card Prize 2008 for the second edition of this publication, which was celebrated for being an outstanding contribution to the smart card field.

With the rapid technological development of information technology, computer systems and especially embedded systems are becoming more mobile and ub- uitous. Ensuring the security of these complex and yet resource-constraineds- temshasemergedasoneofthemostpressingchallengesforresearchers.Although there are a number of information security conferences that look at particular aspects of the challenge, we decided to create the Workshop in Information - curity Theory and Practices (WISTP) to consider the problem as a whole. In additiontheworkshopaimsto bringtogetherresearchersandpractitionersin- lated disciplines and encourage interchange and practical co-operation between academia and industry. Although this is the ?rst ever WISTP event, the response from researchers wassuperbwithover68paperssubmittedforpotentialinclusionintheworkshop and proceedings. The submissions were reviewed by at least three reviewers, in most cases by four, and for program committee (PC) papers at least ?ve reviewers. This long and rigorous process was only possible thanks to the hard work of the PC members and additional reviewers, listed in the following pages. We would like to express our gratitude to the PC members, who were very supportive from the very beginning of this project. Thanks are also due to the additional expert reviewers who helped the PC to select the ?nal 20 workshop papers for publication in the proceedings. Of course we highly appreciate the e?orts of all the authors who submitted papers to WISTP 2007. We hope they will contribute again to a future edition and encourage others to do so.

Internet of Things: Connecting Objects puts forward the technologies and the networking architectures which make it possible to support the Internet of Things. Amongst these technologies, RFID, sensor and PLC technologies are described and a clear view on how they enable the Internet of Things is given. This book also provides a good overview of the main issues facing the Internet of Things such as the issues of privacy and security, application and usage, and standardization.

This book constitutes the proceedings of the 9th Workshop on RFID Security and Privacy, RFIDsec 2013, held in Graz, Austria, in July 2013. The 11 papers presented in this volume were carefully reviewed and selected from 23 submissions. RFIDsec deals with topics of importance to improving the security and privacy of RFID, NFC, contactless technologies, and the Internet of Things. RFIDsec bridges the gap between cryptographic researchers and RFID developers.

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.

This book presents the proceedings of the 3rd International Conference of Reliable Information and Communication Technology 2018 (IRICT 2018), which was held in Kuala Lumpur, Malaysia, on July 23–24, 2018. The main theme of the conference was “Data Science, AI and IoT Trends for the Fourth Industrial Revolution.” A total of 158 papers were submitted to the conference, of which 103 were accepted and considered for publication in this book. Several hot research topics are covered, including Advances in Data Science and Big Data Analytics, Artificial Intelligence and Soft Computing, Business Intelligence, Internet of Things (IoT) Technologies and Applications, Intelligent Communication Systems, Advances in Computer Vision, Health Informatics, Reliable Cloud Computing Environments, Recent Trends in Knowledge Management, Security Issues in the Cyber World, and Advances in Information Systems Research, Theories and Methods.

2011 Updated Reprint. Updated Annually. Czech Republic Starting Business (Incorporating) in....Guide

by Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp and Christopher Wolf. The purpose of the award is to formally acknowledge excellence in research. We would like to c-gratulate the authors of these two papers.

How RFID, a ubiquitous but often invisible mobile technology, identifies tens of billions of objects as they move through the world. RFID (Radio Frequency Identification) is ubiquitous but often invisible, a mobile technology used by more people more often than any flashy smartphone app. RFID systems use radio waves to communicate identifying information, transmitting data from a tag that carries data to a reader that accesses the data. RFID tags can be found in credit cards, passports, key fobs, car windshields, subway passes, consumer electronics, tunnel walls, and even human and animal bodies—identifying tens of billions of objects as they move through the world. In this book, Jordan Frith looks at RFID technology and its social impact, bringing into focus a technology that was designed not to be noticed. RFID, with its ability to collect unique information about almost any material object, has been hyped as the most important identification technology since the bar code, the linchpin of the Internet of Things—and also seen (by some evangelical Christians) as a harbinger of the end times. Frith views RFID as an infrastructure of identification that simultaneously functions as an infrastructure of communication. He uses RFID to examine such larger issues as big data, privacy, and surveillance, giving specificity to debates about societal trends. Frith describes how RFID can monitor hand washing in hospitals, change supply chain logistics, communicate wine vintages, and identify rescued pets. He offers an accessible explanation of the technology, looks at privacy concerns, and pushes back against alarmist accounts that exaggerate RFID's capabilities. The increasingly granular practices of identification enabled by RFID and other identification technologies, Frith argues, have become essential to the working of contemporary networks, reshaping the ways we use information.

RFID (Radio Frequency Identification) is used in all areas of automatic data capture allowing contactless identification of objects using RF. With applications ranging from secure internet payment systems to industrial automation and access control, RFID technology solutions are receiving much attention in the research and development departments of large corporations. RFID is a major growth are in auto ID, allowing emergency vehicles to safely trip traffic signals, and providing the technology behind contactless smart cards, "autopiloting" cars, and production automation. Fully revised and updated to include all the latest information on industry standards and applications, this new edition provides a standard reference for people working with RFID technology. Expanded sections explain exactly how RFID systems work, and provide up-to-date information on the development of new tags such as the smart label. Updated coverage of RFID technologies, including electron data carrier architecture and common algorithms for anticollision Details the latest RFID applications, such as the smartlabel, e-commerce and the electronic purse, document tracking and e-ticketing Detailed appendix providing up-to-date information on relevant ISO standards and regulations, including descriptions of ISO 14443 for contactless ticketing and ISO 15693 covering the smartlabel A leading edge reference for this rapidly evolving technology, this text is of interest to practitioners in auto ID and IT designing RFID products and end-users of RFID technology, computer and electronics engineers in security system development and microchip designers, automation, industrial and transport engineers and materials handling specialists. Also a valuable resource for graduate level students in electronics and industrial engineering design.

This book constitutes the thoroughly refereed post-conference proceedings of the 13th International Conference on Information Security and Cryptology, held in Seoul, Korea, in December 2010. The 28 revised full papers presented were carefully selected from 99 submissions during two rounds of reviewing. The conference provides a forum for the presentation of new results in research, development, and applications in the field of information security and cryptology. The papers are organized in topical sections on cryptanalysis, cryptographic algorithms, implementation, network and mobile security, symmetric key cryptography, cryptographic protocols, and side channel attack.

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You’ll develop a security testing methodology, discover the art of

passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Workshop on Information Security Applications, WISA 2009, held in Busan, Korea, during August 25-27, 2009. The 27 revised full papers presented were carefully reviewed and selected from a total of 79 submissions. The papers are organized in topical sections on mutlimedia security, device security, HW implementation security, applied cryptography, side channel attacks, cryptograptanalysis, anonymity/authentication/access controll, and network security.

Discusses the main issues, challenges, opportunities, and trends related to this explosive range of new developments and applications, in constant evolution, and impacting every organization and society as a whole. This two volume handbook supports post-graduate students, teachers, and researchers, as well as IT professionals and managers.

Software Networks describe new concepts for the Internet's next generation. This architecture is based on virtual networking using Cloud and datacenter facilities. The main problems to be dealt with are the placement of virtual resources for opening a new network on the fly, and the urbanization of virtual resources implemented on physical network equipment. The digital architecture also deals with mechanisms capable of automatically controlling the placement of all virtual resources within the physical network. This book describes how to create and delete virtual networks on the fly. Indeed, the system is able to create any new network with any kind of virtual resource (e.g. switches, routers, LSRs, optical paths, firewalls, SIP-based servers, devices, servers, access points, etc.). Software Networks shows how this architecture is compatible with new advances in SDN (Software Defined Networking), new high-speed transport protocols such as TRILL (Transparent Interconnection of Lots of Links) and LISP (Locator/Identifier Separation Protocol), NGN, IMS, new generation Wi-Fi, and 4G/5G networks. Finally, the author introduces Clouds of security and the virtualization of secure elements (smartcards) that could certainly transform how to secure the Internet. For this second edition, the author addresses in five new chapters the importance of open source software for networks, mobile edge computing, fog networking, tactile internet – a network environment allowing remote access, and security – the use of Cloud of security, secure elements and the emergence of the blockchain.

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.

This book constitutes the thoroughly refereed post-conference proceedings of the 14th International Conference on Smart Card Research and Advanced Applications, CARDIS 2015, held in Bochum, Germany, in November 2015. The 17 revised full papers presented in this book were carefully reviewed and selected from 40 submissions. The focus of the conference was on all aspects of the design, development, deployment, validation, and application of smart cards and secure elements in secure platforms or systems.

The book covers many topics, including unconditionally secure RFID systems, dynamic RFID tag authentication, RFID ownership transfer, fingerprinting RFID tags, and secure RFID-supported supply chains.

Since1994,CARDIShasbeentheforemostinternationalconferencededicatedto smart card research and applications. Every two years, the scienti?c community congregates to present new ideas and discuss recent developments with both an academicandindustrialfocus.Followingtheincreasedcapabilitiesofsmartcards anddevices,CARDIS has becomea majoreventfor the discussionofthe various issuesrelatedtotheuseofsmallelectronictokensintheprocessofhuman-machine interactions.Thescopeoftheconferenceincludesnumeroussub?eldssuchasn- working,e?cientimplementations,physicalsecurity,biometrics,andso on. This year's CARDIS was held in London, UK, on September 8–11, 2008. It was organized by the Smart Card Centre, Information Security Group of the Royal Holloway, University of London. Thepresentvolumecontainsthe21papersthatwereselectedfromthe51s- missions to the conference. The 22 members of the program committee worked hard in order to evaluate each submission with at least three reviews and agree on a high quality ?nal program. Additionally, 61 external reviewers helped the committee with their expertise. Two invited talks completed the technical p- gram. The ?rst one, given by Ram Banerjee and Anki Nelaturu, was entitled "Getting Started with Java Card 3.0 Platform". The second one, given by Aline Gouget, was about "Recent Advances in Electronic Cash Design" and was c- pleted by an abstract provided in these proceedings.

This book discusses the security issues in a wide range of wireless devices and systems, such as RFID, Bluetooth, ZigBee, GSM, LTE, and GPS. It collects the findings of recent research by the UnicornTeam at 360 Technology, and reviews the state-of-the-art literature on wireless security. The book also offers detailed case studies and theoretical

treatments – specifically it lists numerous laboratory procedures, results, plots, commands and screenshots from real-world experiments. It is a valuable reference guide for practitioners and researchers who want to learn more about the advanced research findings and use the off-the-shelf tools to explore the wireless world.

An insightful and practical guide to the use of RFID. The author's professional experience is used to great effect to de-mystify RFID, which is becoming one of the fastest growing sectors of the radio technology industry. Building on Paret's previous technical guide it covers a variety of topics in an accessible manner.

This book provides a broad overview of the many card systems and solutions that are in practical use today. This new edition adds content on RFIDs, embedded security, attacks and countermeasures, security evaluation, javacards, banking or payment cards, identity cards and passports, mobile systems security, and security management. A step-by-step approach educates the reader in card types, production, operating systems, commercial applications, new technologies, security design, attacks, application development, deployment and lifecycle management. By the end of the book the reader should be able to play an educated role in a smart card related project, even to programming a card application. This book is designed as a textbook for graduate level students in computer science. It is also as an invaluable post-graduate level reference for professionals and researchers. This volume offers insight into benefits and pitfalls of diverse industry, government, financial and logistics aspects while providing a sufficient level of technical detail to support technologists, information security specialists, engineers and researchers.

With Smart Card Programming the reader will have the expert guidance he need to work with smart cards. The book offers a comprehensive guide, to the technological aspects related to smart cards, providing an high level overview of the technological panorama and giving an in-depth technical coverage about the related architectures, programming paradigms and APIs. The first part of the book introduces the smart card technologies, the general concepts and a few case studies. It is addressed also to non-technical reader who wishes an high level overview on smart card world. The second part of the book is a technical guide to smart card specifications and programming paradigms. It dives into technical topics about smart card programming and applications development in C/C++, C#, Visual Basic and Java. Key features include: - Contact and Contactless Cards - ISO 7816 - NFC - JavaCard Framework - PC/SC - PKCS#11 - OpenCard Framework - Java - Smart Card I/O - GlobalPlatform - EMV

This book constitutes the refereed proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2007. The 31 revised full papers cover side channels, low resources, hardware attacks and countermeasures, special purpose hardware, efficient algorithms for embedded processors, efficient hardware, trusted computing.

These proceedings contain the papers selected for presentation at the 13th European Symposium on Research in Computer Security—ESORICS 2008—held October 6–8, 2008 in Torremolinos (Malaga), Spain, and hosted by the University of Malaga, C- puter Science Department. ESORICS has become the European research event in computer security. The symposium started in 1990 and has been organized on alternate years in different European countries. From 2002 it has taken place yearly. It attracts an international audience from both the academic and industrial communities. In response to the call for papers, 168 papers were submitted to the symposium. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the Program Comm- tee. The Program Committee meeting was held electronically, holding intensive d- cussion over a period of two weeks. Finally, 37 papers were selected for presentation at the symposium, giving an acceptance rate of 22%.