**Hardware Implementation Of Finite Field Arithmetic Electronic Engineering**

Circuits and Systems for Security and Privacy begins by introducing the basic theoretical concepts and arithmetic used in algorithms for security and cryptography, and by reviewing the fundamental building blocks of cryptographic systems. It then analyzes the advantages and disadvantages of real-world implementations that not only optimize power, area, and throughput but also resist side-channel attacks. Merging the perspectives of experts from industry and academia, the book provides valuable insight and necessary background for the design of security-aware circuits and systems as well as efficient accelerators used in security applications.

This book constitutes the refereed proceedings of the Third International Workshop on the Arithmetic of Finite Fields, WAIFI 2010, held in Istanbul, Turkey, in June 2010. The 15 revised full papers presented were carefully reviewed and selected from 33 submissions. The papers are organized in topical sections on efficient finite field arithmetic, pseudo-random numbers and sequences, Boolean functions, functions, Equations and modular multiplication, finite field arithmetic for pairing based cryptography, and finite field, cryptography and coding.

These are the proceedings of the 7th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005) held in Edinburgh, Scotland from August 29 to September 1, 2005.

This book constitutes the refereed proceedings of the 17th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2015, held in Saint Malo, France, in September 2015. The 34 full papers included in this volume were carefully reviewed and selected from 128 submissions. They are organized in the following topical sections: processing techniques in side-channel analysis; cryptographic hardware implementations; homomorphic encryption in hardware; side-channel attacks on public key cryptography; cipher design and cryptanalysis; true random number generators and entropy estimations; side-channel analysis and fault injection attacks; higher-order side-channel attacks; physically unclonable functions and hardware trojans; side-channel attacks in practice; and lattice-based implementations.

This book constitutes the thoroughly refereed post-proceedings of the International Conference on Information Networking, ICOIN 2003, held at Cheju Island, Korea in February 2003. The 100 revised full papers presented were carefully selected during two rounds of reviewing and revision. The papers are organized in topical sections on high-speed network technologies, enhanced Internet protocols, QoS in the Internet, mobile Internet, network security, network management, and network performance.

This book constitutes the refereed proceedings of the 4th International Conference on Cryptology in India, INDOCRYPT 2003, held in New Delhi, India in December 2003. The 29 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 101 submissions. The papers are organized in topical sections on stream ciphers, block ciphers, Boolean functions, secret sharing, bilinear pairings, public key cryptography, signature schemes, protocols, elliptic curve cryptography and algebraic geometry, implementation and digital watermarking, and authentication.

The refereed post-proceedings of the International Conference on Computational Intelligence and Security are presented in this volume. The 116 papers were submitted to two rounds of careful review. Papers cover bio-inspired computing, evolutionary computation, learning systems and multi-agents, cryptography, information processing and intrusion detection, systems and security, image and signal processing, and pattern recognition.

The process of Integrated Circuits (IC) started its era of VLSI (Very Large Scale Integration) in 1970's when thousands of transistors were integrated into one single chip. Nowadays we are able to integrate more than a billion transistors on a single chip. However, the term "VLSI" is still being used, though there was some effort to coin a new term ULSI (Ultra-Large Scale Integration) for fine distinctions many years ago. VLSI technology has brought tremendous benefits to our everyday life since its occurrence. VLSI circuits are used everywhere, real applications include microprocessors in a personal computer or workstation, chips in a graphic card, digital camera or camcorder, chips in a cell phone or a portable computing device, and embedded processors in an automobile, et al. VLSI covers many phases of design and fabrication of integrated circuits. For a commercial chip design, it involves system definition, VLSI architecture design and optimization, RTL (register transfer language) coding, (pre- and post-synthesis) simulation and verification, synthesis, place and route, timing analyses and timing closure, and multi-step semiconductor device fabrication including wafer processing, die preparation, IC packaging and testing, et al. As the process technology scales down, hundreds or even thousands of millions of transistors are integrated into one single chip. Hence, more and more complicated systems can be integrated into a single chip the so-called System-on-chip (SoC), which brings to VLSI engineers ever increasingly challenges to master techniques in various phases of VLSI design. For modern SoC design, practical applications are usually speed hungry. For instance, Ethernet standard has evolved from 10Mbps to 10Gbps. Now the specification for 100Mbps Ethernet is on the way. On the other hand, with the popularity of wireless and portable computing devices, low power consumption has become extremely critical. To meet these contradicting requirements, VLSI designers have to perform optimizations at all levels of design. This book is intended to cover a wide range of VLSI design topics. The book can be roughly partitioned into four parts. Part I is mainly focused on algorithmic level and architectural level VLSI design and optimization for image and video signal processing systems. Part II addresses VLSI design optimizations for cryptography and error correction coding. Part III discusses general SoC design techniques as well as other application-specific VLSI design optimizations. The last part will cover generic nano-scale circuit-level design techniques.
August 2000. The 25 revised full papers presented together with two invited contributions were carefully reviewed and selected from 51 submissions. The papers are organized in topical sections on implementation of elliptic curve cryptosystems, power and timing analysis attacks, hardware implementation of block ciphers, hardware architectures, power analysis attacks, arithmetic architectures, physical security and cryptanalysis, and new schemes and algorithms.

Modern cryptosystems, used in numerous applications that require secrecy or privacy - electronic mail, financial transactions, medical-record keeping, government affairs, social media etc. - are based on sophisticated mathematics and algorithms that in implementation involve much computer arithmetic. And for speed it is necessary that the arithmetic be realized at the hardware (chip) level. This book is an introduction to the implementation of cryptosystems at that level. The aforementioned arithmetic is mostly the arithmetic of finite fields, and the book is essentially one on the arithmetic of prime fields and binary fields in the context of cryptography. The book has three main parts. The first part is on generic algorithms and hardware architectures for the basic arithmetic operations: addition, subtraction, multiplication, and division. The second part is on the arithmetic of prime fields. And the third part is on the arithmetic of binary fields. The mathematical fundamentals necessary for the latter two parts are included, as are descriptions of various types of cryptosystems, to provide appropriate context. This book is intended for advanced-level students in Computer Science, Computer Engineering, and Electrical and Electronic Engineering. Practitioners too will find it useful, as will those with a general interest in "hard" applications of mathematics.

This book constitutes the refereed proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems, CHES'99, held in Worcester, MA, USA in August 1999. The 27 revised papers presented together with three invited contributions were carefully reviewed and selected from 42 submissions. The papers are organized in sections on cryptographic hardware, hardware architectures, smartcards and embedded systems, arithmetic algorithms, power attacks, true random numbers, cryptographic algorithms on FPGAs, elliptic curve implementations, new cryptographic schemes and modes of operation.

This book constitutes the refereed proceedings of the 6th International Algorithmic Number Theory Symposium, ANTS 2004, held in Burlington, VT, USA, in June 2004. The 30 revised full papers presented together with 3 invited papers were carefully reviewed and selected for inclusion in the book. Among the topics addressed are zeta functions, elliptic curves, hyperelliptic curves, GCD algorithms, number field computations, complexity, primality testing, Weil and Tate pairings, cryptographic algorithms, function field sieve, algebraic function field mapping, quartic fields, cubic number fields, lattices, discrete logarithms, and public key cryptosystems.

This book constitutes the thoroughly refereed post-workshop proceedings of the 6th International Workshop on the Arithmetic of Finite Field, WAIFI 2016, held in Ghent, Belgium, in July 2016. The 14 revised full papers and 3 invited talks presented were carefully reviewed and selected from 38 submissions. The papers are organized in topical sections on invited talks; elliptic curves; applications; irreducible polynomials; applications to cryptography; Boolean functions; cryptography; cryptography and Boolean functions.

This book constitutes the refereed proceedings of the Third International Workshop on Applied Reconfigurable Computing, ARC 2007, held in Manara, Brazil, in March 2007. The 27 full papers and 10 short papers presented together with a late-corner contribution from ARC 2006 are organized in topical sections on architectures, mapping techniques and tools, arithmetic, and applications.

After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible techniques for efficiently implementing finite-field and elliptic curve arithmetic.

Distills complex mathematics and algorithms for easy understanding * Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools * This comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security.

This book constitutes the refereed proceedings of the 4th International Workshop on the Arithmetic of Finite Field, WAIFI 2012, held in Bochum, Germany, in July 2012. The 14 revised full papers and 4 invited talks presented were carefully reviewed and selected from 29 submissions. The papers are organized in topical sections on coding theory and code-based cryptography, Boolean functions, finite field arithmetic, equations and functions, and polynomial factorization and permutation polynomial.

This book constitutes the refereed proceedings of the Cryptographers' Track at the RSA Conference 2003, CT-RSA 2003, held in San Francisco, CA, USA, in April 2003. The 26 revised full papers presented together with abstracts of 3 invited talks were carefully reviewed and selected from 97 submissions. The papers are organized in topical sections on key self-protection, message authentication, digital signatures, pairing based cryptography, multivariate and lattice problems, cryptographic architectures, new RSA-based cryptosystems, chosen-ciphertext security, broadcast encryption and PRF sharing, authentication structures, elliptic curves and pairings, threshold cryptography, and implementation issues.

This book constitutes the thoroughly refereed post-workshop proceedings of the 8th International Workshop on the Arithmetic of Finite Field, WAIFI 2020, held in Rennes, France in July 2020. Due to the COVID-19, the workshop was held online. The 12 revised full papers and 2 invited talks presented were carefully reviewed and selected from 22 submissions. The papers are organized in topical sections on invited talks, Finite Field Arithmetic, Coding Theory, Network Security and much more.

Modern cryptography, which is the basis of information security techniques, started in the late 70's and developed in the 80's. As communication networks were spreading deep into society, the need for secure communication greatly promoted cryptographic research. The need for fast but secure cryptographic systems is growing bigger. Therefore, dedicated systems for cryptography are becoming a key issue for designers. With the spread of reconfigurable hardware such as FPGAs, hardware implementations of cryptographic algorithms become cost-effective. The focus of this book is on all aspects of embedded cryptographic hardware. Of special interest are contributions that describe new secure and fast hardware implementations and new efficient algorithms, methodologies and protocols for secure communications. This book is organised in two parts. The first part is dedicated to embedded hardware of cryptosystems while the second part focuses on new algorithms for cryptography, design methodologies and secure protocols.

Elliptic curve cryptography (ECC) offers a viable alternative to Rivest-Shamir-Adleman (RSA) by delivering equivalent security with a smaller key size. This has several advantages, including smaller
bandwidth demands, faster key exchange, and lower latency encryption and decryption. The fundamental operation for ECC is scalar point multiplication, wherein a point P on an elliptic curve defined over a finite field is multiplied by a scalar k. The complexity of this operation requires a hardware implementation to achieve high performance. The algorithms involved in scalar point multiplication are constantly evolving, incorporating the latest developments in number theory to improve computation time. These competing needs, high performance and flexibility, have caused previous implementations to either limit their adaptability or to incur performance losses. This thesis explores the use of a hybrid-FPGA for scalar point multiplication. A hybrid-FPGA contains a general purpose processor (GPP) in addition to reconfigurable fabric. This allows for a software/hardware co-design with low latency communication between the GPP and custom hardware. The elliptic curve operations and finite field inversion are programmed in C code. All other finite field arithmetic is implemented in the FPGA hardware, providing higher performance while retaining flexibility. The resulting implementation achieves speedups ranging from 24 times to faster than an optimized software implementation executing on a Pentium II workstation. The scalability of the design is investigated in two directions: faster finite field multiplication and increased instruction level parallelism exploitation. Increasing the number of parallel arithmetic units beyond two is shown to be less efficient than increasing the speed of the finite field multiplier.

This book contains the proceedings of the NATO-Russia Advanced Study Institute (ASI) 'Boolean Functions in Cryptology and Information Security,' which was held in Zvenigorod, Moscow region, Russia. These proceedings consist of three parts. The first part contains survey lectures on various areas of Boolean function theory that are of primary importance for cryoptology. These lectures were delivered by leading researchers from many countries and contain both classic and recent results. The second part contains research papers written by graduate and postgraduate students of Lomonosov University, Moscow. The third part contains a list of open problems in Boolean function theory. The book includes lectures and papers concerning the following areas: cryptographic properties of Boolean functions and mappings; algebraic and combinatorial constructions of Boolean functions and mappings with prescribed cryptographic properties; Boolean functions and mappings in cryptosynthesis; classification of Boolean functions; cryptanalysis of ciphers; and efficient computations in finite fields.

Software-based cryptography can be used for security applications where data traffic is not too large and low encryption rate is tolerable. But hardware methods are more suitable where speed and real-time encryption are needed. Until now, there has been no book explaining how cryptographic algorithms can be implemented on reconfigurable hardware devices. This book covers computational methods, computer arithmetic algorithms, and design improvement techniques needed to implement efficient cryptographic algorithms in FPGA reconfigurable hardware platforms. The author emphasizes the practical aspects of reconfigurable hardware design, explaining the basic mathematics involved, and giving a comprehensive description of state-of-the-art implementation techniques.

This book contains the papers presented at the 14th International Conference on Field Programmable Logic and Applications (FPL) held during August 30th- September 1st 2004. The conference was hosted by the Interuniversity Micro- Electronics Center (IMEC) in Leuven, Belgium. The FPL series of conferences was founded in 1991 at Oxford University (UK), and has been held annually since: in Oxford (3 times), Vienna, Prague, Darmstadt, London, Tallinn, Glasgow, Villach, Belfast, Montpellier and Lisbon. It is the largest and oldest conference in reconfigurable computing and brings together academic researchers, industry experts, users and newcomers in an informal, welcoming atmosphere that encourages productive exchange of ideas and knowledge between the delegates. The fast and exciting advances in field programmable logic are increasing steadily with more and more application potential and need. New ground has been broken in architectures, design techniques, (partial) run-time reconfiguration and applications of field programmable devices in several different areas. Many of these recent innovations are reported in this volume. The size of the FPL conferences has grown significantly over the years. FPL in 2003 saw 216 papers submitted. The interest and support for FPL in the programmable logic community continued this year with 285 scientific papers submitted, demonstrating a 32% increase when compared to the year before. The technical program was assembled from 78 selected regular papers, 45 additional short papers and 29 posters, resulting in this volume of proceedings. The program also included three invited plenary keynote presentations from Xilinx, Guilder Technology Report and Altera, and three embedded tutorials from Xilinx, the Universit ? at Karlsruhe (TH) and the University of Oslo.

This book constitutes the refereed proceedings of the 4th International Workshop on Post-Quantum Cryptography, PQCrypto 2011, held in Taipei, Taiwan, in November/December 2011. The 18 revised full papers presented were carefully reviewed and selected from 38 submissions. The papers cover a wide range of topics in the field of post-quantum public key cryptosystems such as cryptosystems that have the potential to resist possible future quantum computers, classical and quantum attacks, and security models for the post-quantum era..

This book contains extended and revised versions of the best papers presented at the 26th IFIP WG 10.5/IEEE International Conference on Very Large Scale Integration, VLSI-SoC 2018, held in Verona, Italy, in October 2018. The 13 full papers included in this volume were carefully reviewed and selected from the 27 papers (out of 106 submissions) presented at the conference. The papers discuss the latest academic and industrial results and developments as well as future trends in the field of System-on-Chip (SoC) design, considering the challenges of nano-scale, state-of-the-art and emerging manufacturing technologies. In particular, they address cutting-edge research fields like heterogeneous, neuromorphic and brain-inspired, biologically-inspired, approximate computing systems.

This book constitutes the thoroughly refereed post-workshop proceedings of the 7th International Workshop on the Arithmetic of Finite Field, WAIFI 2018, held in Bergen, Norway, in June 2018. The 14 revised full papers and six invited talks presented were carefully reviewed and selected from 26 submissions. The papers are organized in topical sections on invited talks; elliptic curves; hardware implementations; arithmetic and applications of finite fields and cryptography.

These are the proceedings of CHES 2004, the 6th Workshop on Cryptographic Hardware and Embedded Systems. For the first time, the CHES Workshop was sponsored by the International Association for Cryptologic Research (IACR). This year, the number of submissions reached a new record. One hundred and twenty-five papers were submitted, of which 32 were selected for presentation. Each submitted paper was reviewed by at least 3 members of the program committee. We are very grateful to the program committee for their hard and efficient work in assembling the program. We are also grateful to the 108 external referees who helped in the review process in their area of expertise. In addition to the submitted contributions, the program included three invited talks, by Neil Gershenfeld (Center for Bits and Atoms, MIT) about "Physical Information Security," by Issac Chuang (Medialab, MIT) about "Quantum Cryptography," and by Paul Kocher (Cryptography Research) about "Phy- cal Attacks". It also included a rump session, chaired
by Christof Paar, which featured informal talks on recent results. As in the previous years, the workshop focused on all aspects of cryptographic hardware and embedded system security. We sincerely hope that the CHES Workshop series will remain a premium forum for intellectual exchange in this area.

This book constitutes the thoroughly refereed proceedings of the Second International Conference on Pairing-Based Cryptography, Pairing 2008, held in London, UK, in September 2008. The 20 full papers, presented together with the contributions resulting from 3 invited talks, were carefully reviewed and selected from 50 submissions. The contents are organized in topical sections on cryptography, mathematics, constructing pairing-friendly curves, implementation of pairings, and hardware implementation.

Implement Finite-Field Arithmetic in Specific Hardware (FPGA and ASIC) Master cutting-edge electronic circuit synthesis and design with help from this detailed guide. Hardware Implementation of Finite-Field Arithmetic describes algorithms and circuits for executing finite-field operations, including addition, subtraction, multiplication, squaring, exponentiation, and division. This comprehensive resource begins with an overview of mathematics, covering algebra, number theory, finite fields, and cryptography. The book then presents algorithms which can be executed and verified with actual input data. Logic schemes and VHDL models are described in such a way that the corresponding circuits can be easily simulated and synthesized. The book concludes with a real-world example of a finite-field application—elliptic-curve cryptography. This is an essential guide for hardware engineers involved in the development of embedded systems. Get detailed coverage of: Modulo m reduction Modulo m addition, subtraction, multiplication, and exponentiation Operations over GF(p) and GF(pm) Operations over the commutative ring Zp[x]/f(x) Operations over the binary field GF(2m) using normal, polynomial, dual, and triangular

Hardware Implementation of Finite-Field Arithmetic McGraw Hill Professional

This book constitutes the refereed proceedings of the First International Workshop on the Arithmetic of Finite Fields, WAIFI 2007, held in Madrid, Spain in June 2007. The 27 revised full papers presented were carefully reviewed and selected from 94 submissions. The papers are organized in topical sections on structures in finite fields, efficient implementation and architectures, efficient finite field arithmetic, classification and construction of mappings over finite fields, curve algebra, cryptography, codes, and discrete structures.

Novel Algorithms and Techniques in Telecommunications and Networking includes a set of rigorously reviewed world-class manuscripts addressing and detailing state-of-the-art research projects in the areas of Industrial Electronics, Technology and Automation, Telecommunications and Networking. Novel Algorithms and Techniques in Telecommunications and Networking includes selected papers from the conference proceedings of the International Conference on Telecommunications and Networking (TeNe 08) which was part of the International Joint Conferences on Computer, Information and Systems Sciences and Engineering (CISSE 2008). Beginning with an introduction to cryptography, Hardware Security: Design, Threats, and Safeguards explains the underlying mathematical principles needed to design complex cryptographic algorithms. It then presents efficient cryptographic algorithm implementation methods, along with state-of-the-art research and strategies for the design of very large scale integrated (VLSI) circuits and symmetric cryptosystems, complete with examples of Advanced Encryption Standard (AES) ciphers, asymmetric ciphers, and elliptic curve cryptography (ECC). Gain a Comprehensive Understanding of Hardware Security—from Fundamentals to Practical Applications Since most implementations of standard cryptographic algorithms leak information that can be exploited by adversaries to gather knowledge about secret encryption keys, Hardware Security: Design, Threats, and Safeguards: Details algorithmic- and circuit-level countermeasures for attacks based on power, timing, fault, cache, and scan chain analysis Describes hardware intellectual property piracy and protection techniques at different levels of abstraction based on watermarking Discusses hardware obfuscation and physically unclonable functions (PUFs), as well as Trojan modeling, taxonomy, detection, and prevention Design for Security and Meet Real-Time Requirements If you consider security as critical a metric for integrated circuits (ICs) as power, area, and performance, you'll embrace the design-for-security methodology of Hardware Security: Design, Threats, and Safeguards. Pairing-based cryptography is at the very leading edge of the current wave in computer cryptography. That makes this book all the more relevant, being as it is the refereed proceedings of the First International Conference on Pairing-Based Cryptography, Pairing 2007, held in Tokyo, Japan in 2007. The 18 revised full papers presented together were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections including those on applications, and certificateless public key encryption. This monograph provides a self-contained presentation of the foundations of finite fields, including a detailed treatment of their algebraic closures. It also covers important advanced topics which are not yet found in textbooks: the primitive normal basis theorem, the existence of primitive elements in affine hyperplanes, and the Niederreiter method for factoring polynomials over finite fields. We give streamlined and/or clearer proofs for many fundamental results and treat some classical material in an innovative manner. In particular, we emphasize the interplay between arithmetical and structural results, and we introduce Berlekamp algebras in a novel way which provides a deeper understanding of Berlekamp's celebrated factorization algorithm. The book provides a thorough grounding in finite field theory for graduate students and researchers in mathematics. In view of its emphasis on applicable and computational aspects, it is also useful for readers working in information and communication engineering, for instance, in signal processing, coding theory, cryptography or computer science.--

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 congratulate the authors of these two papers.
A new approach to the study of arithmetic circuits In Synthesis of Arithmetic Circuits: FPGA, ASIC and Embedded Systems, the authors take a novel approach of presenting methods and examples for the synthesis of arithmetic circuits that better reflects the needs of today's computer system designers and engineers. Unlike other publications that limit discussion to arithmetic units for general-purpose computers, this text features a practical focus on embedded systems. Following an introductory chapter, the publication is divided into two parts. The first part, Mathematical Aspects and Algorithms, includes mathematical background, number representation, addition and subtraction, multiplication, division, other arithmetic operations, and operations in finite fields. The second part, Synthesis of Arithmetic Circuits, includes hardware platforms, general principles of synthesis, adders and subtractors, multipliers, dividers, and other arithmetic primitives. In addition, the publication distinguishes itself with: * A separate treatment of algorithms and circuits—a more useful presentation for both software and hardware implementations * Complete executable and synthesizable VHDL models available on the book’s companion Web site, allowing readers to generate synthesizable descriptions * Proposed FPGA implementation examples, namely synthesizable low-level VHDL models for the Spartan II and Virtex families * Two chapters dedicated to finite field operations This publication is a must-have resource for students in computer science and embedded system designers, engineers, and researchers in the field of hardware and software computer system design and development. An Instructor Support FTP site is available from the Wiley editorial department. This volume contains the proceedings of the 4th International Conference on - formation and Communications Security (ICICS2002). The three previous conferences were held in Beijing (ICICS97), Sydney (ICICS99) and Xian (ICICS01), where we had an enthusiastic and well-attended event. ICICS2002 is sponsored and organized by the Laboratories for Information Technology, Singapore, in co-operation with the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences and the International Communications and Information Security Association (ICISA). During the past five years the conference has placed equal emphasis on the theoretical and practical aspects of information and communications security and has established itself as a forum at which academic and industrial people meet and discuss emerging security challenges and solutions. We hope to uphold this tradition by offering you yet another successful meeting with a rich and interesting program. The response to the Call For Papers was overwhelming, 161 paper submissions were received. Therefore, the paper selection process was very competitive and difficult—only 41 papers were accepted and many good papers had to be rejected. The success of the conference depends on the quality of the program. We are indebted to our program committee members and the external referees for the wonderful job they did.

Copyright: 820f290df4b4fe95acb130b0190e69b