Transactions on Computational Science and Computational Intelligence

Kevin Daimi · Hamid R. Arabnia
Leonidas Deligiannidis
Min-Shiang Hwang
Fernando G. Tinetti *Editors*

Advances in Security, Networks, and Internet of Things

Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20

Springer

Transactions on Computational Science and Computational Intelligence

Series Editor
Hamid Arabnia
Department of Computer Science
The University of Georgia
Athens, GA, USA

Computational Science (CS) and Computational Intelligence (CI) both share the same objective: finding solutions to difficult problems. However, the methods to the solutions are different. The main objective of this book series, "Transactions on Computational Science and Computational Intelligence", is to facilitate increased opportunities for cross-fertilization across CS and CI. This book series publishes monographs, professional books, contributed volumes, and textbooks in Computational Science and Computational Intelligence. Book proposals are solicited for consideration in all topics in CS and CI including, but not limited to, Pattern recognition applications; Machine vision; Brain-machine interface; Embodied robotics; Biometrics; Computational biology; Bioinformatics; Image and signal processing; Information mining and forecasting; Sensor networks; Information processing; Internet and multimedia; DNA computing; Machine learning applications; Multi-agent systems applications; Telecommunications; Transportation systems; Intrusion detection and fault diagnosis; Game technologies; Material sciences; Space, weather, climate systems, and global changes; Computational ocean and earth sciences; Combustion system simulation; Computational chemistry and biochemistry; Computational physics; Medical applications; Transportation systems and simulations; Structural engineering; Computational electro-magnetic; Computer graphics and multimedia; Face recognition; Semiconductor technology, electronic circuits, and system design; Dynamic systems; Computational finance; Information mining and applications; Biometric modeling; Computational journalism; Geographical Information Systems (GIS) and remote sensing; Ubiquitous computing; Virtual reality; Agent-based modeling; Computational psychometrics; Affective computing; Computational economics; Computational statistics; and Emerging applications. For further information, please contact Mary James, Senior Editor, Springer, mary.james@springer.com.

More information about this series at http://www.springer.com/series/11769

Kevin Daimi • Hamid R. Arabnia
Leonidas Deligiannidis • Min-Shiang Hwang
Fernando G. Tinetti
Editors

Advances in Security, Networks, and Internet of Things

Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20

Springer

Editors
Kevin Daimi
Electrical and Computer Engineering, and Computer Science
University of Detroit Mercy
Detroit, MI, USA

Hamid R. Arabnia
Department of Computer Science
University of Georgia
Athens, GA, USA

Leonidas Deligiannidis
School of Computing and Data Sciences
Wentworth Institute of Technology
Boston, MA, USA

Min-Shiang Hwang
Computer Science and Information Engineering
Asian University
Taichung City, Taiwan

Fernando G. Tinetti
Facultad de Informática – CIC PBA
Universidad Nacional de La Plata
La Plata, Argentina

ISSN 2569-7072 ISSN 2569-7080 (electronic)
Transactions on Computational Science and Computational Intelligence
ISBN 978-3-030-71016-3 ISBN 978-3-030-71017-0 (eBook)
https://doi.org/10.1007/978-3-030-71017-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

It gives us great pleasure to introduce this collection of papers that were presented at the following international conferences: Security and Management (SAM 2020); Wireless Networks (ICWN 2020); Internet Computing & IoT (ICOMP 2020); and Embedded Systems, Cyber-physical Systems, and Applications (ESCS 2020). These four conferences were held simultaneously (same location and dates) at Luxor Hotel (MGM Resorts International), Las Vegas, USA, July 27–30, 2020. This international event was held using a hybrid approach, that is, "in-person" and "virtual/online" presentations and discussions.

This book is composed of seven parts. Parts 1 through 4 (composed of 33 chapters) include articles that address various challenges with security and management (SAM). Part 5 (composed of 8 chapters) presents novel methods and applications in the areas of wireless networks (ICWN). Part 6 (composed of 8 chapters) discusses advancements in Internet computing and Internet of Things (ICOMP). Lastly, Part 7 (composed of 11 chapters) presents emerging trends in the areas of embedded systems and cyber-physical systems (ESCS).

An important mission of the World Congress in Computer Science, Computer Engineering, and Applied Computing, CSCE (a federated congress to which this event is affiliated with), includes *"Providing a unique platform for a diverse community of constituents composed of scholars, researchers, developers, educators, and practitioners. The Congress makes concerted effort to reach out to participants affiliated with diverse entities (such as: universities, institutions, corporations, government agencies, and research centers/labs) from all over the world. The congress also attempts to connect participants from institutions that have* ***teaching*** *as their main mission with those who are affiliated with institutions that have* ***research*** *as their main mission. The congress uses a quota system to achieve its institution and geography diversity objectives."* By any definition of diversity, this congress is among the most diverse scientific meetings in the USA. We are proud to report that this federated congress had authors and participants from 54 different nations, representing variety of personal and scientific experiences that arise from differences in culture and values.

The program committees (refer to subsequent pages for the list of the members of committees) would like to thank all those who submitted papers for consideration. About 50% of the submissions were from outside the USA. Each submitted paper was peer reviewed by two experts in the field for originality, significance, clarity, impact, and soundness. In cases of contradictory recommendations, a member of the conference program committee was charged to make the final decision; often, this involved seeking help from additional referees. In addition, papers whose authors included a member of the conference program committee were evaluated using the double-blind review process. One exception to the above evaluation process was for papers that were submitted directly to chairs/organizers of pre-approved sessions/workshops; in these cases, the chairs/organizers were responsible for the evaluation of such submissions. The Congress (the joint conferences) received many good submissions. The overall acceptance rate for regular papers was 20%; 18% of the remaining papers were accepted as short and/or poster papers.

We are grateful to the many colleagues who offered their services in preparing this book. In particular, we would like to thank the members of the Program Committees of individual research tracks as well as the members of the Steering Committees of SAM 2020, ICWN 2020, ICOMP 2020, and ESCS 2020; their names appear in the subsequent pages. We would also like to extend our appreciation to over 500 referees.

As sponsors-at-large, partners, and/or organizers, each of the following (separated by semicolons) provided help for at least one research track: Computer Science Research, Education, and Applications (CSREA); US Chapter of World Academy of Science; American Council on Science and Education & Federated Research Council; and Colorado Engineering Inc. In addition, a number of university faculty members and their staff, several publishers of computer science and computer engineering books and journals, chapters and/or task forces of computer science associations/organizations from three regions, and developers of high-performance machines and systems provided significant help in organizing the event as well as providing some resources. We are grateful to them all.

We express our gratitude to all authors of the articles published in this book and the speakers who delivered their research results at the congress. We would also like to thank the following: UCMSS (Universal Conference Management Systems & Support, California, USA) for managing all aspects of the conference; Dr. Tim Field of APC for coordinating and managing the printing of the programs; the staff at Luxor Hotel (MGM Convention) for the professional service they provided; and Ashu M. G. Solo for his help in publicizing the congress. Last but not least, we would like to thank Ms. Mary James (Springer Senior Editor in New York) and Arun Pandian KJ (Springer Production Editor) for the excellent professional service they provided for this book project.

Book Co-editors and Chapter Co-editors: SAM 2020, ICWN 2020, ICOMP 2020, ESCS 2020

Detroit, MI, USA Kevin Daimi

Athens, GA, USA Hamid R. Arabnia

Boston, MA, USA Leonidas Deligiannidis

La Plata, Argentina Fernando G. Tinetti

Security and Management

SAM 2020 – Program Committee

- Dr. Jacques Bou Abdo, Computer Science Department, Notre Dame University – Louaize, Lebanon
- Dr. Hanaa Ahmed, Computer Science Department, University of Technology, Iraq
- Dr. Mohammed Akour, Department of Computer and Information Systems, Yarmouk University, Jordan
- Professor Emeritus Nizar Al Holou, Department of Electrical and Computer Engineering, University of Detroit Mercy, USA
- Professor Nadia Alsaidi, Department of Applied Mathematics & Computing, University of Technology, Iraq
- Allen Ashourian, ZRD Technology, USA
- Professor Emeritus Hamid Arabnia, (Vice Chair and Coordinator, SAM'20), Department of Computer Science, University of Georgia, USA
- Dr. David Arroyo, Researcher, Spanish National Research Council (CSIC), Spain
- Dr. Shadi Banitaan, (Sessions/Workshops Co-Chair, SAM'20), Computer Science and Software Engineering, University of Detroit Mercy, USA
- Dr. Clive Blackwell, Innovation Works, Airbus Group, United Kingdom
- Dr. Violeta Bulbenkiene, Department of Informatics Engineering, Klaipeda University, Lithuania
- Dr. María Calle, Department of Electrical and Electronics Engineering, Universidad del Norte, Barranquilla, Colombia
- Eralda Caushaj, School of Business Administration, Oakland University, USA
- Dr. Feng Cheng, Internet Technologies and Systems, Hasso-Plattner-Institute, University of Potsdam, Germany
- Professor Emeritus Kevin Daimi, (Conference Chair, SAM'20), Computer Science and Software Engineering, University of Detroit Mercy, USA
- Dr. Ioanna Dionysiou, Department of Computer Science, University of Nicosia, Cyprus

- Dr. Hiroshi Dozono, Faculty of Science and Engineering, Saga University, Japan
- Dr. Luis Hernandez Encinas, (Program Co-Chair, SAM'20), Department of Information Technologies and Communications, Institute of Physical and Information Technologies (ITEFI-CSIC), Spain
- Professor Levent Ertaul, Department of Computer Science, California State University East Bay, USA
- Dr. Ken Ferens, Department of Electrical and Computer Engineering, University of Manitoba, Canada
- Professor Guillermo Francia, Center for Cybersecurity, University of West Florida, USA
- Steffen Fries, Siemens AG, Corporate Technology, CT RDA ITS, Germany
- Dr. Víctor Gayoso Martínez, Spanish National Research Council (CSIC), Spain
- Dr. Bela Genge, University of Medicine, Pharmacy, Science and Technology of Tg. Mures, Romania
- Professor Danilo Gligoroski, Norwegian University of Science and Technology (NTNU), Norway
- Dr. Michael R. Grimaila, Department of Systems Engineering and Management, Center for Cyberspace Research, Air Force Institute of Technology, USA
- Dr. Diala Abi Haidar, Management Information Systems Department, Dar Al Hekma University, Saudi Arabia
- Dr. Hicham H. Hallal, College of Engineering, American University of Sharjah, UAE
- Dr. Hanady Hussein Issa, Arab Academy for Science, Technology and Maritime Transport (ASTMT), Egypt
- Christian Jung, Security Engineering Department, Fraunhofer IESE, Germany
- Nesrine Kaaniche, University of Sheffield, United Kingdom
- Dr. Marie Khair, Computer Science Department, Notre Dame University – Louaize, Lebanon
- Professor Hiroaki Kikuchi, (Program Co-Chair, SAM'20), Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences, Meiji University, Japan
- Professor Irene Kopaliani, Princeton University Research Computing, USA
- Dr. Arash Habibi Lashkari, Canadian Institute for Cybersecurity (CIC), University New Brunswick (UNB), Canada
- Dr. Flaminia Luccio, (Sessions/Workshops Co-Chair, SAM'20), Department of Environmental Sciences, Informatics and Statistics, Ca' Foscari University of Venice, Italy
- Dr. Giovanni L. Masala, Computing, Mathematics & Digital Technology, Manchester Metropolitan University, UK
- Dr. Wojciech Mazurczyk, Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland
- Dr. Suzanne Mello-Stark, Rhode Island College, USA
- Dr. Sherry Michael, Enterprise Partners, Bahrain
- Dr. Alexandra Michota, Open University of Cyprus, Cyprus

- Dr. Esmiralda Moradian, (Posters Co-Chair, SAM'20), Department of Computer and Systems Sciences, Stockholm University, Sweden
- Dr. Nader M Nassar, Innovation for Security and Compliance Group, IBM Corp, USA
- Dr. Ana Nieto, Computer Science Department, University of Malaga, Spain
- Dr. Mais Nijim, Department of Electrical Engineering and Computer Science, Texas A&M University-Kingsville, USA
- Dr. Eugenia Nikolouzou, Internet Application Department, Hellenic Authority for Communication Security and Privacy, Greece
- Dr. Saibal K. Pal, DRDO & University of Delhi, India
- Dr. Cathryn Peoples, (Posters Co-Chair, SAM'20), School of Computing and Communications, Faculty of Science, Technology, Engineering & Mathematics, The Open University, United Kingdom
- Dr. Junfeng Qu, Deptartment of Information Technology, Clayton State University, USA
- Dr. Peter Schartner, System Security Research Group, Alpen-Adria-Universität Klagenfurt, Austria
- Dr. Karpoor Shashidhar, Computer Science Department, Sam Houston State University, USA
- Dr. Nicolas Sklavos, Computer Engineering & Informatics Department, University of Patras, Greece
- Ashu M.G. Solo, (Publicity Chair, SAM'20) Maverick Technologies America, USA.
- Dr. Cristina Soviany, (Program Co-Chair, SAM'20), Features Analytics SA, Belgium
- Professor Hung-Min Sun, Information Security, Department of Computer Science, National Tsing Hua University, Taiwan
- Professor Woei-Jiunn Tsaur, Department of Computer Science, National Taipei University, Taiwan
- Professor Shengli Yuan, Department of Computer Science and Engineering Technology, University of Houston-Downtown, USA

Wireless Networks

ICWN 2020 – Program Committee

- Prof. Emeritus Nizar Al-Holou (Congress Steering Committee); ECE Department; Vice Chair, IEEE/SEM-Computer Chapter; University of Detroit Mercy, Detroit, Michigan, USA
- Prof. Emeritus Hamid R. Arabnia (Congress Steering Committee); The University of Georgia, USA; Editor-in-Chief, Journal of Supercomputing (Springer); Fellow, Center of Excellence in Terrorism, Resilience, Intelligence & Organized Crime Research (CENTRIC).
- Dr. Travis Atkison; Director, Digital Forensics and Control Systems Security Lab, Department of Computer Science, College of Engineering, The University of Alabama, Tuscaloosa, Alabama, USA
- Prof. Dr. Juan-Vicente Capella-Hernandez; Universitat Politecnica de Valencia (UPV), Department of Computer Engineering (DISCA), Valencia, Spain
- Prof. Emeritus Kevin Daimi (Congress Steering Committee); Department of Mathematics, Computer Science and Software Engineering, University of Detroit Mercy, Detroit, Michigan, USA
- Prof. Leonidas Deligiannidis (Congress Steering Committee); Department of Computer Information Systems, Wentworth Institute of Technology, Boston, Massachusetts, USA
- Prof. Mary Mehrnoosh Eshaghian-Wilner (Congress Steering Committee); Professor of Engineering Practice, University of Southern California, California, USA; Adjunct Professor, Electrical Engineering, University of California Los Angeles, Los Angeles (UCLA), California, USA
- Prof. Tai-hoon Kim; School of Information and Computing Science, University of Tasmania, Australia
- Prof. Louie Lolong Lacatan; Chairperson, Computer Engineerig Department, College of Engineering, Adamson University, Manila, Philippines; Senior Member, International Association of CS & IT (IACSIT), Singapore; Member, International Association of Online Engineering (IAOE), Austria

- Prof. Dr. Guoming Lai; Computer Science and Technology, Sun Yat-Sen University, Guangzhou, P. R. China
- Dr. Andrew Marsh (Congress Steering Committee); CEO, HoIP Telecom Ltd (Healthcare over Internet Protocol), UK; Secretary General of World Academy of BioMedical Sciences and Technologies (WABT) a UNESCO NGO, The United Nations
- Prof. Salahuddin Mohammad Masum; Computer Engineering Technology, Southwest Tennessee Community College, Memphis, Tennessee, USA
- Prof. Dr., Eng. Robert Ehimen Okonigene (Congress Steering Committee); Department of Electrical & Electronics Engineering, Faculty of Engineering and Technology, Ambrose Alli University, Nigeria
- Prof. James J. (Jong Hyuk) Park (Congress Steering Committee); Department of Computer Science and Engineering (DCSE), SeoulTech, Korea; President, FTRA, EiC, HCIS Springer, JoC, IJITCC; Head of DCSE, SeoulTech, Korea
- Dr. Akash Singh (Congress Steering Committee); IBM Corporation, Sacramento, California, USA; Chartered Scientist, Science Council, UK; Fellow, British Computer Society; Member, Senior IEEE, AACR, AAAS, and AAAI; IBM Corporation, USA
- Ashu M. G. Solo (Publicity), Fellow of British Computer Society, Principal/R&D Engineer, Maverick Technologies America Inc.
- Prof. Fernando G. Tinetti (Congress Steering Committee); School of CS, Universidad Nacional de La Plata, La Plata, Argentina; also at Comision Investigaciones Cientificas de la Prov. de Bs. As., Argentina
- Prof. Hahanov Vladimir (Congress Steering Committee); Vice Rector, and Dean of the Computer Engineering Faculty, Kharkov National University of Radio Electronics, Ukraine and Professor of Design Automation Department, Computer Engineering Faculty, Kharkov; IEEE Computer Society Golden Core Member; National University of Radio Electronics, Ukraine
- Prof. Shiuh-Jeng Wang (Congress Steering Committee); Director of Information Cryptology and Construction Laboratory (ICCL) and Director of Chinese Cryptology and Information Security Association (CCISA); Department of Information Management, Central Police University, Taoyuan, Taiwan; Guest Ed., IEEE Journal on Selected Areas in Communications.
- Dr. Yunlong Wang; Advanced Analytics at QuintilesIMS, Pennsylvania, USA
- Prof. Layne T. Watson (Congress Steering Committee); Fellow of IEEE; Fellow of The National Institute of Aerospace; Professor of Computer Science, Mathematics, and Aerospace and Ocean Engineering, Virginia Polytechnic Institute & State University, Blacksburg, Virginia, USA
- Prof. Hyun Yoe; Director of Agrofood IT Research Center and Vice President of Korea Association of ICT Convergence in the Agriculture and Food Business (KAICAF); Director of Agriculture IT Convergence Support Center (AITCSC); Department of Information and Communication Engineering, Sunchon National University, Suncheon, Republic of Korea (South Korea)
- Prof. Jane You (Congress Steering Committee); Associate Head, Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong

Internet Computing & IoT

ICOMP 2020 – Program Committee

- Prof. Afrand Agah; Department of Computer Science, West Chester University of Pennsylvania, West Chester, PA, USA
- Prof. Emeritus Nizar Al-Holou (Congress Steering Committee); Professor and Chair, Electrical and Computer Engineering Department; Vice Chair, IEEE/SEM-Computer Chapter; University of Detroit Mercy, Detroit, Michigan, USA
- Prof. Emeritus Hamid R. Arabnia (Congress Steering Committee); The University of Georgia, USA; Editor-in-Chief, Journal of Supercomputing (Springer); Fellow, Center of Excellence in Terrorism, Resilience, Intelligence & Organized Crime Research (CENTRIC).
- Prof. Dr. Juan-Vicente Capella-Hernandez; Universitat Politecnica de Valencia (UPV), Department of Computer Engineering (DISCA), Valencia, Spain
- Prof. Emeritus Kevin Daimi (Congress Steering Committee); Department of Mathematics, Computer Science and Software Engineering, University of Detroit Mercy, Detroit, Michigan, USA
- Prof. Zhangisina Gulnur Davletzhanovna; Vice-rector of the Science, Central-Asian University, Kazakhstan, Almaty, Republic of Kazakhstan; Vice President of International Academy of Informatization, Kazskhstan, Almaty, Republic of Kazakhstan
- Prof. Leonidas Deligiannidis (Congress Steering Committee); Department of Computer Information Systems, Wentworth Institute of Technology, Boston, Massachusetts, USA
- Prof. Mary Mehrnoosh Eshaghian-Wilner (Congress Steering Committee); Professor of Engineering Practice, University of Southern California, California, USA; Adjunct Professor, Electrical Engineering, University of California Los Angeles, Los Angeles (UCLA), California, USA
- Prof. Houcine Hassan; Department of Computer Engineering (Systems Data Processing and Computers), Universitat Politecnica de Valencia, Spain

- Prof. Tai-hoon Kim; School of Information and Computing Science, University of Tasmania, Australia
- Prof. Louie Lolong Lacatan; Chairperson, Computer Engineerig Department, College of Engineering, Adamson University, Manila, Philippines; Senior Member, International Association of CS & IT (IACSIT), Singapore; Member, International Association of Online Engineering (IAOE), Austria
- Prof. Dr. Guoming Lai; Computer Science and Technology, Sun Yat-Sen University, Guangzhou, P. R. China
- Dr. Andrew Marsh (Congress Steering Committee); CEO, HoIP Telecom Ltd (Healthcare over Internet Protocol), UK; Secretary General of World Academy of BioMedical Sciences and Technologies (WABT) a UNESCO NGO, The United Nations
- Dr. Ali Mostafaeipour; Industrial Engineering Department, Yazd University, Yazd, Iran
- Prof. Dr., Eng. Robert Ehimen Okonigene (Congress Steering Committee); Department of Electrical & Electronics Engineering, Faculty of Engineering and Technology, Ambrose Alli University, Nigeria
- Prof. James J. (Jong Hyuk) Park (Congress Steering Committee); Department of Computer Science and Engineering (DCSE), SeoulTech, Korea; President, FTRA, EiC, HCIS Springer, JoC, IJITCC; Head of DCSE, SeoulTech, Korea
- Dr. Xuewei Qi; Research Faculty & PI, Center for Environmental Research and Technology, University of California, Riverside, California, USA
- Dr. Akash Singh (Congress Steering Committee); IBM Corporation, Sacramento, California, USA; Chartered Scientist, Science Council, UK; Fellow, British Computer Society; Member, Senior IEEE, AACR, AAAS, and AAAI; IBM Corporation, USA
- Ashu M. G. Solo (Publicity), Fellow of British Computer Society, Principal/R&D Engineer, Maverick Technologies America Inc.
- Prof. Fernando G. Tinetti (Congress Steering Committee); School of CS, Universidad Nacional de La Plata, La Plata, Argentina; also at Comision Investigaciones Cientificas de la Prov. de Bs. As., Argentina
- Prof. Hahanov Vladimir (Congress Steering Committee); Vice Rector, and Dean of the Computer Engineering Faculty, Kharkov National University of Radio Electronics, Ukraine and Professor of Design Automation Department, Computer Engineering Faculty, Kharkov; IEEE Computer Society Golden Core Member; National University of Radio Electronics, Ukraine
- Varun Vohra; Certified Information Security Manager (CISM); Certified Information Systems Auditor (CISA); Associate Director (IT Audit), Merck, New Jersey, USA
- Prof. Shiuh-Jeng Wang (Congress Steering Committee); Director of Information Cryptology and Construction Laboratory (ICCL) and Director of Chinese Cryptology and Information Security Association (CCISA); Department of Information Management, Central Police University, Taoyuan, Taiwan; Guest Ed., IEEE Journal on Selected Areas in Communications.
- Dr. Yunlong Wang; Advanced Analytics at QuintilesIMS, Pennsylvania, USA

- Prof. Layne T. Watson (Congress Steering Committee); Fellow of IEEE; Fellow of The National Institute of Aerospace; Professor of Computer Science, Mathematics, and Aerospace and Ocean Engineering, Virginia Polytechnic Institute & State University, Blacksburg, Virginia, USA
- Prof. Hyun Yoe; Director of Agrofood IT Research Center and Vice President of Korea Association of ICT Convergence in the Agriculture and Food Business (KAICAF); Director of Agriculture IT Convergence Support Center (AITCSC); Department of of Information and Communication Engineering, Sunchon National University, Suncheon, Republic of Korea (South Korea)
- Prof. Jane You (Congress Steering Committee); Associate Head, Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong
- Dr. Farhana H. Zulkernine; Coordinator of the Cognitive Science Program, School of Computing, Queen's University, Kingston, ON, Canada

Embedded Systems, Cyber-physical Systems, & Applications

ESCS 2020 – Program Committee

- Prof. Emeritus Nizar Al-Holou (Congress Steering Committee); Professor and Chair, ECE Department; Vice Chair, IEEE/SEM-Computer Chapter; University of Detroit Mercy, Detroit, Michigan, USA
- Prof. Emeritus Hamid R. Arabnia (Congress Steering Committee); The University of Georgia, USA; Editor-in-Chief, Journal of Supercomputing (Springer); Fellow, Center of Excellence in Terrorism, Resilience, Intelligence & Organized Crime Research (CENTRIC).
- Dr. P. Balasubramanian; School of CSE, Nanyang Technological University, Singapore
- Prof. Dr. Juan-Vicente Capella-Hernandez; Universitat Politecnica de Valencia (UPV), Department of Computer Engineering (DISCA), Valencia, Spain
- Prof. Emeritus Kevin Daimi (Congress Steering Committee); Director, Computer Science and Software Engineering Programs, Department of Mathematics, Computer Science and Software Engineering, University of Detroit Mercy, Detroit, Michigan, USA
- Prof. Leonidas Deligiannidis (Congress Steering Committee); Department of Computer Information Systems, Wentworth Institute of Technology, Boston, Massachusetts, USA
- Prof. Mary Mehrnoosh Eshaghian-Wilner (Congress Steering Committee); Professor of Engineering Practice, University of Southern California, California, USA; Adjunct Professor, Electrical Engineering, University of California Los Angeles, Los Angeles (UCLA), California, USA
- Prof. Houcine Hassan; Department of Computer Engineering (Systems Data Processing and Computers), Universitat Politecnica de Valencia, Spain
- Prof. Dr. Guoming Lai; Computer Science and Technology, Sun Yat-Sen University, Guangzhou, P. R. China
- Dr. Andrew Marsh (Congress Steering Committee); CEO, HoIP Telecom Ltd (Healthcare over Internet Protocol), UK; Secretary General of World Academy of

BioMedical Sciences and Technologies (WABT) a UNESCO NGO, The United Nations

- Dr. Ali Mostafaeipour; Industrial Engineering Department, Yazd University, Yazd, Iran
- Prof. Dr., Eng. Robert Ehimen Okonigene (Congress Steering Committee); Department of Electrical & Electronics Engineering, Faculty of Engineering and Tech., Ambrose Alli University, Edo State, Nigeria
- Dr. Benaoumeur Senouci; Embedded Systems Department, LACSC Laboratory-Central Electronic Engineering School, ECE, Paris, France
- Ashu M. G. Solo (Publicity), Fellow of British Computer Society, Principal/R&D Engineer, Maverick Technologies America Inc.
- Prof. Fernando G. Tinetti (Congress Steering Committee); School of CS, Universidad Nacional de La Plata, La Plata, Argentina; also at Comision Investigaciones Cientificas de la Prov. de Bs. As., Argentina
- Prof. Hahanov Vladimir (Congress Steering Committee); Vice Rector, and Dean of the Computer Engineering Faculty, Kharkov National University of Radio Electronics, Ukraine and Professor of Design Automation Department, Computer Engineering Faculty, Kharkov; IEEE Computer Society Golden Core Member; National University of Radio Electronics, Ukraine
- Prof. Shiuh-Jeng Wang (Congress Steering Committee); Director of Information Cryptology and Construction Laboratory (ICCL) and Director of Chinese Cryptology and Information Security Association (CCISA); Department of Information Management, Central Police University, Taoyuan, Taiwan; Guest Ed., IEEE Journal on Selected Areas in Communications.
- Prof. Layne T. Watson (Congress Steering Committee); Fellow of IEEE; Fellow of The National Institute of Aerospace; Professor of Computer Science, Mathematics, and Aerospace and Ocean Engineering, Virginia Polytechnic Institute & State University, Blacksburg, Virginia, USA
- Prof. Hyun Yoe; Director of Agrofood IT Research Center and Vice President of Korea Association of ICT Convergence in the Agriculture and Food Business (KAICAF); Director of Agriculture IT Convergence Support Center (AITCSC); Department of of Information and Communication Engineering, Sunchon National University, Suncheon, Republic of Korea (South Korea)
- Prof. Jane You (Congress Steering Committee); Associate Head, Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong

Contents

Part V Wireless Networks, Novel Technologies and Applications

Part VI Internet Computing, Internet of Things, and Applications

Part I
Authentication, Biometrics, and Cryptographic Technologies

Statistical Analysis of Prime Number Generators Putting Encryption at Risk

Aykan Inan

1 Introduction

When it comes down to investigating the security properties of a cryptographic procedure there are different methods to do so, depending on the cryptoscheme itself. This includes inter alia, protocol, side-channel, and mathematical attacks. But the security of a strong cryptographically system is primarily based on the secure management of the secret key. If this key can be easily accessed or even worse guessed by the attacker the system is compromised. No matter how strong the used encryption method itself is. Therefore, it is of great importance that the secret key cannot be revealed in any case. Storing the key securely is one matter but the unpredictability is another [1].

Some cryptoschemes, such as RC4, rely on a random stream. Others, such as RSA need a PNG in order to generate two primes for generating the public and corresponding private key. Therefore, randomness for both "normal" random numbers and primes plays a major role.

Random number and prime number generators (RNGs and PNGs) are typically used when a cryptographic scheme needs a random number or random prime number to some extent. Random prime number generators have additional features as general random number generators: Any number generated needs to be odd and needs to be tested for primality afterwards. The following section gives an overview over the current state of PNGs. Section 3 demonstrates the approach used in this paper to verify the PNGs randomness.Sections 4 and 5 analyze specific outliers

A. Inan (✉)
Ravensburg-Weingarten University, Weingarten, Baden-Württemberg, Germany
e-mail: aykan.inan@hs-weingarten.de

K. Daimi et al. (eds.), *Advances in Security, Networks, and Internet of Things*, Transactions on Computational Science and Computational Intelligence,
https://doi.org/10.1007/978-3-030-71017-0_1

within the randomness spectrum. Section 6 looks for patterns within primes, and Sect. 7 for patterns in the last 32 to 64 bits. The last Sect. 8 concludes and gives an outlook.

2 Related Work and Basics

This section is splitted in two parts: while Sects. 2.1 and 2.2 discusses deterministic (Sect. 2.1) and non-deterministic (Sect. 2.2) random number generators, Sect. 2.3 gives an overview on prime-number generators. A key requirement for both types of random number generators is that their output cannot be reproduced or predicted [2]. There are many mathematical tests such as the chi-square test, which can verify the statistical behavior of RNGs or PNGs sequences.

2.1 *Deterministic RNG*

A deterministic random number generator is always producing the same sequences of random numbers under the same circumstances. That is why they are also called pseudo-random number generators (PRNG). But the produced consecutive numbers appear to be random enough for most applications. The generated sequence of a PRNG is computed recursively from an initial seed value initializing a function $f(s_0)$:

$$\begin{aligned} s_0 &= \text{seed} \\ s_{i+1} &= f(s_i),\ i = 0, 1, \ldots\ i \in \mathbb{N}_0 \end{aligned} \tag{1}$$

In general, the generated sequence can be described as:

$$s_{i+1} = f(s_i, s_{i-1}, \ldots, s_{i-t}) \tag{2}$$

In this case t is representing an integer constant.

Consequently, a PRNG does not generate true random numbers in a proper or true sense because it is computing its random numbers initialized from a starting (seed) value. Thus, it is completely deterministic [2]. According to Manuel Blum and Silvio Micali [3] a polynomial algorithm should not be capable of predicting and computing the next sequence better than 0.5 (50%) chance of success without knowing the initial seed value. For this, different mathematical tests are being used to prove the correctness.

2.2 Non-deterministic RNG

In contrast to the deterministic RNG a non-deterministic random number generator includes external source of randomness (entropy) such as hardware noise or the current time [1]. They are also known as cryptographically secure pseudo-random number generators (CSPRNG) and can be seen as a special type of PRNG which represents an unpredictable PRNG [2].

Assuming we have the following output sequence of n bits, where n is representing some integer:

$$s_i, s_{i+1}, \ldots, s_{i+n-1} \tag{3}$$

Then it must be computationally infeasible to compute the subsequent bits:

$$s_{i+n}, s_{i+n+1} \cdots \tag{4}$$

PNRGs and CSPSRNGs are described and defined as an algorithm that is producing an unpredictable sequence of random numbers in such a way that an attacker is not capable of computing or guessing them. This means that all generated random numbers must have the same likelihood of occurrence.

The characteristic of fully randomness can only be fulfilled with a One-time-pad which is, however, unsuitable for practical applications. So, the solution is to use pseudo-random numbers or pseudo-random sequences which are based on a deterministic process. Despite of this deterministic behavior and the use of an initialization seed value the produced output still must have the property of a truly random sequence [1].

In this context it is important to point out that the key generation in asymmetrical procedures usually requires some more effort than the generation process of pseudo-random numbers used in symmetrical systems. This is because an asymmetric cryptoscheme, such as RSA, requires large primes. Thus, the produced random numbers must fulfill the above-mentioned properties as well as the category of being prime at the same time [1, 4]. For this purpose Prime Number Generators are needed.

2.3 Prime Number Generator

In practice it is common to work with pseudo-prime numbers which fulfill most basic requirements for primes such as producing an odd number. Then a primality test, usually Miller-Rabin [5], is applied as depicted in Fig. 1.

The likelihood that a randomly picked or generated integer p is a prime is of further interest. In case of RSA, e.g., in order to generate a 1024-bit modulus n, the two primes p and q each should have a length of about 512 bits [4]. The chance that

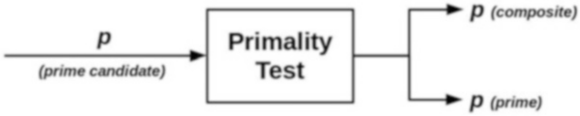

Fig. 1 Approach to generate primes

a random integer of that size is prime is still sufficiently high based on the prime number theorem and is approximately $\frac{1}{\ln(p)}$ as shown below [2, 6]:

$$p \text{ is prime } \approx \frac{2}{\ln(p)} = \frac{2}{\ln(2^{512})} = \frac{2}{512\ln(2)} \approx \frac{1}{177} \tag{5}$$

This means on average that 177 random numbers must be generated and tested before finding a prime. The density of primes, for even much larger bit numbers, is still adequate high [2].

This is relevant if similar prime numbers are generated. Often a value is then added to the result if it fails the primality test until a prime number is finally found. But this can lead to similar generated numbers.

Consequently, a prime used in RSA must be unpredictable. However, if at least one of the primes is easily obtained, RSA would be broken. This paper therefore analyses whether our current process of determining the quality of randomness for primes is still valid.

2.4 Evaluation of PRNG

Every published analysis dealing with PNGs or RNGs such as [3, 7–10] are just focusing on this unpredictability of subsequent sequences. As long as the produced output, e.g., a pair of two primes, is unique compared to the previous one, then the primes are sufficient enough for cryptographical use.

However, by generating more than one billion primes of specific bit lengths, (32, 64, 128, 256, and 512) and displaying the result into different statistics as presented in the following Sects. 3–7. The generated prime numbers show similar characteristics and seem related to each other.

A statistical analysis of the PNG used in LibreSSL was conducted. The results demonstrate suspicious behavior indicating that the numbers are not fully random as they seem.

3 Statistical Analysis

The statistical analysis is based on two essentials aspects:

(a) Prime Numbers
(b) Prime Distances

Each aspect itself is separated into sub-aspects again.

(a.1) Smallest prime number
(a.2) Largest prime number
(a.3) Mean prime number

The exact same statistical approach applies to the generated corresponding distances between prime numbers:

(b.1) Smallest distance
(b.2) Largest distance
(b.3) Maximum distance between (b.1) and (b.2)
(b.4) Mean distance

In general the statistics are showing the following relationship between two consecutive generated primes, as depicted in Fig. 2 and all generated primes in general:

Furthermore a variance analysis and standard deviation will be presented and explained in Sect. 3.3 for the prime numbers and the prime distances in Sect. 3.7. Due to the large amount of data and the large numbers involved the following subsections are going to present the most outstanding properties with regard to the above-mentioned listing in (a) and (b) and the specific bit lengths of 32, 64, 128, 256, and 512 bit because they are most commonly used.

3.1 Largest and Smallest Prime Numbers

The largest and smallest prime numbers that have ever occurred are listed in Tables 1 and 2.

Although these specific numbers did not occur very frequently they give a good reference point to search for boundaries and patterns within and among other primes. This includes, among other properties, the occurrences of numbers near threshold values (see Sects. 4 and 5), such as the largest and smallest prime.

Fig. 2 Distance between p and q

Table 1 Largest prime numbers

Bit	Value	Occurrence
32	4,294,967,291	13
64	18,446 ... 876,649	2
128	340,282 ... 715,813	2
256	115,792 ... 191,919	1
512	13,407 ... 162,089	1