Advances in Intelligent Systems and Computing 1262

Debasis Giri · Rajkumar Buyya · S. Ponnusamy · Debashis De · Andrew Adamatzky · Jemal H. Abawajy *Editors*

Proceedings of the Sixth International Conference on Mathematics and Computing

ICMC 2020

Springer

Advances in Intelligent Systems and Computing

Volume 1262

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing such as: computational intelligence, soft computing including neural networks, fuzzy systems, evolutionary computing and the fusion of these paradigms, social intelligence, ambient intelligence, computational neuroscience, artificial life, virtual worlds and society, cognitive science and systems, Perception and Vision, DNA and immune based systems, self-organizing and adaptive systems, e-Learning and teaching, human-centered and human-centric computing, recommender systems, intelligent control, robotics and mechatronics including human-machine teaming, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, knowledge management, intelligent agents, intelligent decision making and support, intelligent network security, trust management, interactive entertainment, Web intelligence and multimedia.

The publications within "Advances in Intelligent Systems and Computing" are primarily proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Indexed by SCOPUS, DBLP, EI Compendex, INSPEC, WTI Frankfurt eG, zbMATH, Japanese Science and Technology Agency (JST), SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at http://www.springer.com/series/11156

Debasis Giri · Rajkumar Buyya ·
S. Ponnusamy · Debashis De ·
Andrew Adamatzky · Jemal H. Abawajy
Editors

Proceedings of the Sixth International Conference on Mathematics and Computing

ICMC 2020

Springer

Editors
Debasis Giri
Department of Information Technology
Maulana Abul Kalam Azad University
of Technology
Haringhata, West Bengal, India

S. Ponnusamy
Department of Mathematics
Indian Institute of Technology Madras
Chennai, India

Andrew Adamatzky
Unconventional Computing Laboratory
Department of Computer Science
and Creative Technologies
University of the West of England
Bristol, UK

Rajkumar Buyya
School of Computing
and Information Systems
University of Melbourne
Melbourne, VIC, Australia

Debashis De
Department of Computer
Science and Engineering
Maulana Abul Kalam Azad
University of Technology
Haringhata, West Bengal, India

Jemal H. Abawajy
Faculty of Science
Engineering and Built Environment
Deakin University Geelong
Geelong, VIC, Australia

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-981-15-8060-4 ISBN 978-981-15-8061-1 (eBook)
https://doi.org/10.1007/978-981-15-8061-1

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Committee

Chief Patron

Prof. Avinash Khare, Honorable Vice Chancellor, Sikkim University, India

Patron

Prof. Rajkumar Buyya, University of Melbourne, Australia

General Co-chairs

Dr. P. K. Saxena, Former Director, DRDO, SAG, Delhi, India
Prof. P. D. Srivastava, IIT Bhilai, India
Prof. Debashis De, Maulana Abul Kalam Azad University of Technology, WB, India

Program Co-chairs

Dr. Debasis Giri, Maulana Abul Kalam Azad University of Technology, WB, India
Prof. S. Ponnusamy, IIT Madras, India
Dr. Satish Narayana Srirama, University of Tartu, Estonia
Prof. Jemal Hussien, Deakin University, Australia
Prof. Andrew Adamatzky, University of West of England, UK

Publicity Chair

Dr. Nilanjan Dey, Techno India College of Technology, Kolkata, India

Organizing Chair

Partha Pratim Ray, Department of CA, Sikkim University, India

Organizing Committee

Dr. Swarup Roy, Department of CA, Sikkim University, India
Dr. Mohan Pratap Pradhan, Department of CA, Sikkim University, India
Mrs. Chunnu Khawas, Department of CA, Sikkim University, India

Dr. Rebika Rai, Department of CA, Sikkim University, India
Mrs. Lekhika Chettri, Department of CA, Sikkim University, India
Dr. Thoudam Roshan Singh, Department of Mathematics, Sikkim University, India
Dr. Namita Behera, Department of Mathematics, Sikkim University, India
Dr. Bipul Pal, Department of Mathematics, Sikkim University, India
Ms. Rinkila Bhutia, Department of Mathematics, Sikkim University, India

Technical Program Committee

TPC for Computing (Alphabetically)

Abderrahmen Mtibaa, New Mexico State University, Mexico
Amlan Chakrabarti, Calcutta University, India
Anand Kumar M, NIT Karnataka, India
Andrew Adamatzky, University of the West of England, UK
Andy Adamatzky University of the West of England, UK
Anilkumar Devarapu, Albany State University, USA
Anirban Mondal, Ashoka University, India
Arif Ahmed Sk, University of Tromsø, Norway
Ashok Kumar Das, IIIT Hyderabad, India
Athanasios V. Vasilakos, Luleå University of Technology, Sweden
Bidyut Patra, NIT Rourkela, India
Bivas Mitra, IIT Kharagpur, India
Chandan Kumar Chanda, IIEST, India
Chandrashekhar Y. Meshram, Rani Durgavati University, India
Christina Boura, Université de Versailles Saint-Quentin-en-Yvelines, France
Christine Fernandez, University of Poitiers, UMR CNRS, France
Dhananjoy Dey, SAG, DRDO, India
Debashis De, Maulana Abul Kalam Azad University of Technology, WB, India
Debasis Giri, Maulana Abul Kalam Azad University of Technology, WB, India
Debiao He, Wuhan University, China
Debi Prosad Dogra IIT Bhubaneswar, India
Dhananjoy Dey, SAG, DRDO, India
Dinesh Dash, NIT Patna, India
Dipanwita Roy Chowdhury, IIT kharagpur, India
Dung Hoang Duong, University of Wollongongm, Australia
Fagen Li, Univ. of Electronic Science and Technology of China, China
Fahreddïn Abdullaye, v Kyrgyz Turkey Manas University, Turkey
Fernando Velez, Universidade da Beira Interior, Portugal
Gerardo Pelosi, Politecnico di Milano, Italy
Goutham Reddy Alavalapati, NIT Andhra Pradesh, India
Indivar Gupta, SAG, DRDO, India
Janka Chlebikova, University of Portmouth, UK

Jaydeb Bhaumik, Jadavpur University, India
Jemal Hussien, Deakin University, Australia
Jiqiang Lu, Institute for Infocomm Research, Singapore
Jorge Sa Silva, University of Coimbra, Portugal
Junwei Zhou, Wuhan University of Technology, China
Kanesaraj Ramasamy, Multimedia University, Malaysia
Keshav Dahal, University of the West of Scotland, UK
Kolin Paul, IIT Delhi, India
Kouichi Sakurai, Kyushu University, Japan
Kuheli Sai, University of Pittsburgh, Pennsylvania
Marko Hölbl, University of Maribor, Slovenia
Michal Choras, ITTI Ltd., Poland
Meng Yu, Roosevelt University, USA
Mohd Helmy Abd Wahab, Universiti Tun Hussein Onn Malaysia, Malaysia
Nai-Wei Lo, NTU of Science and Technology, Taiwan
Niladri Puhan, IIT Bhubaneswar, India
Nilanjan Dey, Techno India College of Technology, Kolkata, India
Noboru Kunihiro, The University of Tokyo, Japan
Olivier, Blazy, Université de Limoges, France
Oscar Castillo, Tijuana Institute of Technology, Mexico
P. K. Saxena, SCCS & Former Director, SAG DRDO, India
Philippe Gaborit, University of Limoges, France
Prasanna Mishra, DRDO, India
Rajendra Prasath, IIIT Sricity, India
Rajkumar Buyya, University of Melbourne, Australia
Ranbir Sanasam, IIT Guwahati, India
Raviraj Pandian, Kalaignar Karunanidhi Institute of Technology, India
Saibal Pal, DRDO, India
Samiran Chattopadhyay Jadavpur University, India
Sandip Karmakar, IIIT Kalyani, India
Sarmistha Neogy, Jadavpur University, India
Satish Narayana Srirama, University of Tartu, Estonia
Seonghan Shin, NIAIST, Japan
Sharma Chakravarthy, The University of Texas at Arlington, USA
Shehzad Ashraf Chaudhry, International Islamic University, Pakistan
Sherali Zeadally, University of Kentucky, USA
Siddhartha Bhattacharyya, RCC IIT, India
Sk Hafizul Islam, IIIT Kalyani, India
Sokratis Katsikas, NTNU, Norway
Somitra Sanadhya, IIT Ropar, India
Subhankar Joardar, Haldia Institute of Technology, India
Subrata Dutta, NIT Jamshedpur, India
Sudip Misra, IIT Kharagpur, India
Svetla Nikova, KU Leuven, Belgium
Tanmoy Maitra, KIIT University, India

Thoudam Doren Singh, CDAC, Mumbai, India
Valentina Emilia Balas, Aurel Vlaicu University of Arad, Romania
Vasudha Bhatnagar, Delhi University, India
Yao Zhao, Beijing Jiaotong University, China

TPC for Mathematics (Alphabetically)

Abdullah M. Rababah, Jordan University of S & T, Jordan
Ameeya Nayak, IIT Roorkee, India
Anirban Banerjee, IISER, Kolkata, India
Arya Kumar Bedabrata Chand, IIT Madras, India
Avishek Adhikari, University of Calcutta, India
B. N. Mandal, ISI, Kolkata, India
Bapan Ghosh, NIT Meghalaya, India
Binod Chandra Tripathy, Tripura University, India
Diana Mendes, ISCTE-IUL, Portugal
Dipak Jana, Haldia Institue of Technology, India
Debjani Chakraborty, IIT Kharagpur, India
Don Hong, Middle Tennessee State University, USA
Duan Li, The Chinese University of Hong Kong, Hong Kong
Edgar Martinez-Moro, Universidad de Valladolid, Spain
Emel Aşıcı, Karadeniz Technical University, Turkey
Geetanjali Panda, Indian Institute of Technology Kharagpur, India
Gennadii Demidenko, Sobolev Institute of Mathematics, Russia
Heinrich Begehr, Free University Berlin, Germany
Inessa Matveeva, Sobolev Institute of Mathematics, Russia
Junzo Watada Waseda University, Japan
Kinkar Das, Sungkyunkwan University, South Korea
Konstantin Volkov, Kingston University, London
Lakshmi Kanta Patra, IIIT Ranchi, India
Leopoldo Eduardo, Cárdenas-Barrón Tecnológico de Monterrey, Mexico
Ljubisa Kocinac, University of Nis, Serbia
Madhumangal Pal, Vidyasagar University, India
Margareta Heilmann, University of Wuppertal, Germany
María A. Navascués, Universidad de Zaragoza, Spain
Manoranjan Maiti Vidyasagar University, India
Muhammad Noor, COMSATS IIT, Pakistan
Mujahid Abbas, University of Pretoria, South Africa
Pamini Thangarajah, Mount Royal University, Canada
P. D. Srivastava, IIT Bhilai, India
Praveen Kumar Gupta, NIT Silchar, India
Ravi P. Agarwal, Texas A & M University, USA
S. Ponnusamy, IIT Madras, India
Santanu Sarkar, IIT Madras, India
Saru Kumari, Ch. Charan Singh University, India

Shanta Laishram Indian Statistical Institute, New Delhi, India
Shay Gueron, University of Haifa, Israel
Shuang Li, NIAST, China
Soumen Maity, IISER Pune, India
Srinivas Jangirala, O. P. Jindal Global University, India
Subhas Khajanchi, IIT Roorkee, India
Subhash Bhalla University of Aizu, Japan
Suchandan Kayal, NIT Rourkela, India
Susanta Maity, NIT Arunachal Pradesh, India
Takeshi Koshiba, Waseda University, Japan
Teodor Bulboaca, Babes-Bolyai University, Cluj-Napoca, Romania
Tian-Xiao He, Illinois Wesleyan University, USA
Vilem Novak, University of Ostrava, Czech Republic
Weizhi Meng, Technical Universtiy of Denmark, Denmark
Zakia Hammouch, FST Errachidia Moulay Ismail University, Morocco
Zhisheng Shuai, University of Central Florida, USA

Additional Reviewers

Gopal Shit, Amit Kumar Verma, Partha Pratim Ray, Buddhananda Banerjee, Subhabrata Barman, Tanmoy Chakraborty, Sanjay Chatterji, Barun Das, Manju Khan, Dilip Maity, Amit Maji, Mousumi Mandal, Sourav Mandal, Tufan Naiya, Saroj Padhan, Pratima Panigrahi, Soumen Pati, Suparna Saha, Kuheli Sai.

Message from General Co-chairs

It gives me a great pleasure to welcome you to ICMC 2020, the 6th edition of the premier annual conference on Mathematics and Computing. This year, ICMC will be held in the Department of Computer Applications, Sikkim University, Gangtok, Sikkim, India, where advanced technology infrastructure and collection of creative talents are gathered, making it an excellent position to develop advanced Computing. ICMC has been the most impactful conference on all aspects of Mathematics and Computing. Papers published in this impactful conference represent the hard work of many outstanding researchers from around the world. We are very delighted to report that ICMC remains at the forefront of computer networks. This year, the main conference embodies a set of 45 papers out of 172 submissions, selected through careful and rigorous peer review by TPC members as best of the best submissions, and organized around 2 tracks and 18 keynote sessions. It is our honour to have invited most prominent scholars as our conference: Prof. Dipanwita Roy Chowdhury, IIT Kharagpur, India; Prof. P. D. Srivastava, IIT Bhilai, India; Dr. P. K. Saxena, DRDO, India; Prof. S. Ponnusamy, IIT Madras, India; Prof. Samiran Chattopadhyay, Jadavpur University, India; Dr. Ashok Kumar Das, IIIT Hyderabad; Dr. Sanasam Ranbir Singh, IIT Guwahati, India; Dr. Biswapati Jana, Vidyasagar University, India; Prof. Ekrem SAVAS, Usak University, Usak/Turkey; Mr. Aninda Bose, Springer, India; Prof. Duan Li, City University of Hong Kong, Hong Kong; Prof. Bidyut B. Chaudhuri, Techno India University, Kolkata, and ISI Kolkata, India; Prof. Neeraj Kumar, Thapar Institute of Engineering and Technology, India; Mr. Giovanni BluMitolo, Italy; Dr. Bidyut Kr. Patra, NIT Rourkela, Dr. Debasis Giri, MAKAUT, WB, India; Prof. Debashis De, MAKAUT, WB, India; and Dr. Swadesh Kumar Sahoo, Indian Institute of Technology Indore, India.

First, we would like to thank to all program members and organizing committee members who have done an outstanding job in carrying out the paper review tasks. In particular, we would like to express our appreciation to Dr. Debasis Giri and Mr. Partha Pratim Ray who spent great effort to develop the review system. We would like to thank Honourable Vice-Chancellor of Sikkim University, Sikkim, for his support for providing Excellent Venue. Last but not least, we thank our patrons

and sponsors for their warm support. We must thank IEEE Fellow Prof. Rajkumar Buyya for his tireless effort and constant support of ICMC 2020 for his guidance and direction.

Finally, we thank all the conference participants for making ICMC a success.

P. K. Saxena
P. D. Srivastava
Debashis De

Message from Program Co-chairs

It is a great pleasure for us to organize the Sixth International Conference on Mathematics and Computing 2020 held from March 18–20, 2020, at Gangtok, Sikkim, India. Our main goal is to provide an opportunity to the participants to learn about contemporary research in Mathematics and Computing, and exchange ideas among themselves and with experts present in the conference as tutorial presenters and the plenary as well as invited speakers.

Sixteen speakers from India and abroad agreed to deliver their talks and some of them acted as session chairs. After an initial call for papers, 172 papers were submitted at the conference. All submitted papers were sent to external referees and, after refereeing, 45 papers were recommended for publication for the conference proceedings that will be published by Springer series: Advances in Intelligent Systems and Computing.

ICMC 2020 has come up as an international platform to deliver and share novel knowledge in various fields on applied mathematics and computing of interest.

We are grateful to the chief patron, patron, general co-chairs, program co-chairs, publicity chair, speakers, participants, referees, organizers, sponsors, and funding agencies for their support and help without which it would have been impossible to organize the conference. We owe our gratitude to the volunteers who work behind the scene tirelessly in taking care of the details in making this conference a success.

Debasis Giri
S. Ponnusamy
Satish Narayana Srirama
Jemal Hussien
Andrew Adamatzky

Preface

In the last two decades, scientific computing has become an important contributor to all scientific research programs. It is particularly important for the solution of research problems that are unsolvable by traditional theory and experimental approaches, hazardous to study in the laboratory, or time-consuming or expensive to be solved by traditional means. With mathematical modeling and computational algorithms, many more problems from the realm of science, commerce as well as other walks of life can be solved efficiently. The International Conference on Mathematics and Computing (ICMC) is such a premier forum for the presentation of new advances and research results in the fields of Cryptography, Network Security, Cybersecurity, Internet of Things, Due & Edge Computing, Mathematics, Statistics and Scientific Computing. The conference will bring together leading academic scientists, experts from industry, and researchers in their domains of expertise from around the world. Earlier, ICMC was organized in 2013, 2015, 2017, 2018, and 2019.

The 6th ICMC 2020 aims to bring together both novice and experienced scientists with developers, to meet new colleagues, collect new ideas, and establish new cooperation between research groups and provide a platform for researchers from academic and industry to present their original work and exchange ideas, information, techniques, and applications in the field of Computational Applied Mathematics, including, but not limited to the broad topics of Operations Research, Soft Computing, Cryptology, Network Security, Cybersecurity, Internet of Things, Due & Edge Computing, Image Processing, Pure and Applied Mathematics, and other emerging areas of research.

The 6th ICMC 2020 is organized by the Department of Computer Applications, Sikkim University, Gangtok, Sikkim, India. This conference received 172 papers from different parts of India as well as world. This book of abstracts contains 45 full papers which fall under mathematics and computing tracks. We would like to thank the Vice-Chancellor and officials of Sikkim University, patron, respected general co-chairs, publicity chair, organizing committee members, volunteers, sponsors,

attendees, and authors who attended and made this conference a success. ICMC 2020 proceedings will be published in the Springer series: Advances in Intelligent Systems and Computing.

Haringhata, India — Debasis Giri
Melbourne, Australia — Rajkumar Buyya
Chennai, India — S. Ponnusamy
Haringhata, India — Debashis De
Bristol, UK — Andrew Adamatzky
Geelong, Australia — Jemal Hussien

Contents

About the Editors

Dr. Debasis Giri is currently working as an Associate Professor in the Department of Information Technology, Maulana Abul Kalam Azad University of Technology (formerly known as West Bengal University of Technology), West Bengal, India. Prior to this, he also held academic positions as the Professor in the Department of Computer Science and Engineering and Dean in the School of Electronics, Computer Science and Informatics, Haldia Institute of Technology, Haldia, India. He did his masters (M.Tech. and M.Sc.) both from IIT Kharagpur, India, and also completed his Ph.D. from IIT Kharagpur, India. He is tenth all India rank holder in Graduate Aptitude Test in Engineering (GATE) in 1999. He received a certificate from All India Science Teachers' Association in Science Aptitude & Talent Search Test in 1988. His current research interests include cryptography, information security, e-commerce security, and design and analysis of algorithms. He has authored more than 75 research papers in reputed international journals and conference proceedings. He is serving as an Associate Editorial of the Journal of (i) Information Security and Applications (Elsevier), (ii) Security and Privacy Journal (Wiley), (iii) International Journal of Communication Systems (Wiley), (iv) Security and Communication Networks, (v) Electrical and Computer Engineering Innovations, and (vi) Azerbaijan Journal of High Performance Computing. He has been involved as a Technical Program Committee member of several international conferences in repute. He is the Founder of the International Conference on Mathematics and Computing. He is also a program committee member of several international conferences. He is a member of IEEE, and a life member of Cryptology Research Society of India, and the International Society for Analysis, its Applications and Computation (ISAAC).

Dr. Rajkumar Buyya is a Redmond Barry Distinguished Professor and Director of the Cloud Computing and Distributed Systems (CLOUDS) Laboratory at the University of Melbourne, Australia. He is also serving as the founding CEO of Manjrasoft, a spin-off company of the university, commercializing its innovations in cloud computing. He served as a Future Fellow of the Australian Research

Council during 2012–2016. He has authored over 625 publications and 7 textbooks including "Mastering Cloud Computing" published by McGraw Hill, China Machine Press, and Morgan Kaufmann for Indian, Chinese, and international markets, respectively. He also edited several books including "Cloud Computing: Principles and Paradigms" (Wiley Press, USA, February 2011). He is one of the highly cited authors in computer science and software engineering worldwide (h-index = 132, g-index = 294, 92,500+ citations). "A Scientometric Analysis of Cloud Computing Literature" by German scientists ranked him as the World's Top-Cited (#1) Author and the World's Most-Productive (#1) Author in Cloud Computing. He is recognized as a "Web of Science Highly Cited Researcher" for four consecutive years since 2016, a Fellow of IEEE, and Scopus Researcher of the Year 2017 with Excellence in Innovative Research Award by Elsevier and recently (2019) received "Lifetime Achievement Awards" from two Indian universities for his outstanding contributions to cloud computing and distributed systems. Software technologies for grid and cloud computing developed under his leadership have gained rapid acceptance and are in use at several academic institutions and commercial enterprises in 40 countries around the world. He served as the founding Editor-in-Chief of the IEEE Transactions on Cloud Computing. He is currently serving as the Co-Editor-in-Chief of Journal of Software: Practice and Experience, which was established 50 years ago.

Dr. S. Ponnusamy is a Institute Chair Professor in the Department of Mathematics of IIT Madras. He has earned his B.Sc. (1980) and M.Sc. (1992) from the University of Madras. He completed his Ph.D. (1989) at IIT Kanpur. His current research interest includes complex analysis, quasiconformal and harmonic mappings, special functions, and functions spaces. He is the founding "Fellow of the Forum de Analystes, Chennai, India," 1992. He was elected as a "Fellow of The National Academy of Sciences, India" in the year 2002. He served 5 years as the Head of the Indian Statistical Institute, Chennai Centre (October 2012–October 2017). He is the currently the President of the Ramanujan Mathematical Society, India. He has been associated with a number of organizations for popularization of science and serves on the editorial boards of several peer-reviewed international journals. He is often invited to give plenary talks at international conferences and to give lectures in universities all over the world. He took part as a researcher in many funded projects in India and Abroad. He has been refereeing for more than 100 journals. He has written four books and another book with Herb Sivlerman. One of his books won the Best Selling Author Award in 2002. He has edited several volumes and international conference proceedings. He has published more than 250 technical articles in reputed international journals (such as Advances in Mathematics, Annales Academia Scientiarum Fennica Mathematica, Applied Mathematics and Computation, Archiv der Mathematik, Bulletin des Sciences Mathematiques, Bulletin/Journal of the Australian Mathematical Society, Complex Variables and Elliptic Equations, Complex Analysis and Operator Theory, Computational Methods and Function Theory, Indagationes Mathematicae, Journal

of London Mathematical Society, Integral Equations and Operator Theory, Journal Computational and Applied Mathematics, Journal of Mathematical Analysis and Applications, Mathematika, Mathematishe Annalen, Mathematische Nachrichten, Mathematische Zeitschrift, Monatshefte fuer Mathematik, Nonlinear Analysis, Potential Analysis, Proceedings of American Mathematical Society, Results in Mathematics, Rocky Mountain Journal of Mathematics The Journal of Geometric Analysis) and has solved several long-standing open problems and conjectures. He has been a Visiting Professor of a number of universities in abroad (e.g., Hengyang Normal University and Hunan Normal University, China; Kazan Federal University and Petrozavodsk State University, Russia; University Sains Malaysia, Malaysia; the University of Aalto, the University of Turku, and the University of Helsinki, Finland; Texas Tech University, Lubbock, USA).

Prof. Debashis De earned his M.Tech. from the University of Calcutta in 2002 and his Ph.D. (Engineering) from Jadavpur University in 2005. He is the Professor and Director in the Department of Computer Science and Engineering of the Maulana Abul Kalam Azad University of Technology, West Bengal (Former West Bengal University of Technology), India, and Adjunct Research Fellow at the University of Western Australia, Australia. He is a senior member of the IEEE, life member of CSI, and member of the International Union of Radio science. He was awarded the prestigious Boyscast Fellowship by the Department of Science and Technology, Government of India, to work at the Herriot-Watt University, Scotland, UK. He received the Endeavour Fellowship Award during 2008–2009 by DEST Australia to work at the University of Western Australia. He received the Young Scientist Award both in 2005 at New Delhi and in 2011 at Istanbul, Turkey, from the International Union of Radio Science, Head Quarter, Belgium. His research interests include mobile cloud computing and Green mobile networks. He has published in more than 250 peer-reviewed international journals and 200 international conference papers, 6 research monographs, and 10 textbooks. His h-index is 26 and i10 index is 91. Total citation is 3330. He is an Associate Editor of journal IEEE ACCESS, Editor Hybrid computational intelligence, Journal Array, Elsevier.

Dr. Andrew Adamatzky is the Professor of Unconventional Computing and Director of the Unconventional Computing Laboratory, Department of Computer Science, University of the West of England, Bristol, UK. He does research in molecular computing, reaction-diffusion computing, collision-based computing, cellular automata, slime mould computing, massive parallel computation, applied mathematics, complexity, nature-inspired optimization, collective intelligence and robotics, bionics, computational psychology, nonlinear science, novel hardware, and future and emergent computation. He authored 7 books, mostly notable are "Reaction-Diffusion Computing," "Dynamics of Crow Minds," and "Physarum Machines" and edited 22 books in computing, most notable are "Collision Based Computing," "Game of Life Cellular Automata," and "Memristor Networks"; he also produced a series of influential artworks published in the atlas "Silence of Slime Mould". He is the founding Editor-in-Chief of "Journal of Cellular

Automata" and "Journal of Unconventional Computing" and Editor-in-Chief of "Journal of Parallel, Emergent, Distributed Systems" and "Parallel Processing Letters."

Dr. Jemal H. Abawajy (SM'11) is a Full Professor at the Faculty of Science, Engineering and Built Environment, Deakin University, Australia. He has delivered more than 60 keynote sessions and seminars worldwide and has been involved in the organization of more than 300 international conferences in various capacity including chair and general co-chair. He has also served on the editorial board of numerous international journals including IEEE Transaction on Cloud Computing. He is the author/co–author of more than 400 refereed articles and supervised numerous Ph.D. students to completion.

Preventing Differential Fault Analysis Attack on AEGIS Family of Ciphers

Swapan Maiti and Dipanwita Roy Chowdhury

Abstract AEGIS, a dedicated authenticated encryption algorithm is one of the winners of the CAESAR portfolio. In literature, there exist fault attacks on AEGIS family of ciphers. Fault attack is one of the most efficient forms of side-channel attacks against implementations of cryptographic algorithms, and the protection against fault attack is vital for security-related devices. In this paper, we propose countermeasures for AEGIS family of ciphers. The proposed countermeasures show that the state of the ciphers can not be recovered faster than exhaustive search because it needs 2^{128} time to recover a state of each cipher.

Keywords Authenticated encryption · Fault attack · Countermeasures · CAESAR · AES

1 Introduction

Authenticated encryption (AE) and authenticated encryption with associated data (AEAD) are forms of encryption which simultaneously assure the confidentiality and authenticity of data. CAESAR [1], a competition for authenticated encryption was started in 2013, which targets to identify a portfolio of AEAD. AEGIS [2], a dedicated AES [3]-based authenticated encryption algorithm is a one of the winners of the CAESAR competition.

Fault attack is one of the most efficient forms of side-channel attack against implementations of cryptographic algorithms. In this kind of attack, faults are injected during cipher operations. The attacker then analyzes the fault-free and faulty ciphertexts or keystreams to deduce partial or full information of the secret key.

S. Maiti (✉) · D. Roy Chowdhury
Indian Institute of Technology Kharagpur, Kharagpur, India
e-mail: swapankumar_maiti@yahoo.co.in

D. Roy Chowdhury
e-mail: drc@cse.iitkgp.ac.in

D. Giri et al. (eds.), *Proceedings of the Sixth International Conference on Mathematics and Computing*, Advances in Intelligent Systems and Computing 1262,
https://doi.org/10.1007/978-981-15-8061-1_1

In literature, there exist some fault attacks on authenticated encryption stream ciphers and the countermeasures [4–6]. AEGIS is also susceptible to Differential Fault Attack (DFA) [7].

The main contribution of this work can be summarized below:

- Proposed countermeasures against differential fault attack for each of the ciphers of AEGIS family.
- Furnished a comparison of the modified AEGIS with AEGIS family

The organization of the rest of the paper is as follows. Section 2 discusses AEGIS family of ciphers. The differential fault analysis on each of the ciphers is briefly described in this section. Section 3 presents the countermeasures against fault attack on each of the ciphers. A comparison of the modified AEGIS with AEGIS family is shown in Sect. 4. Finally, the paper is concluded in Sect. 5.

2 Background

The authenticated encryption algorithms of AEGIS family of ciphers are introduced in [2]. In this section, we briefly describe the ciphers and the attack strategies on them. The AEGIS family of ciphers extensively uses one keyed round function ($AESRoundFunction$) of AES [3] as follows:

$$AESRoundFunction(A, B) = \tau(A) \oplus B$$

where $\tau(.)$ = MixColumns(ShiftRows(SubBytes(.))), and each of A and B is a 16-byte block. The following operators are used in AEGIS:

$\oplus$: bit-wise exclusive OR
& : bit-wise AND
|| : concatenation

2.1 AEGIS Family of Ciphers

In this section, we briefly describe the ciphers AEGIS-128, AEGIS-256, and AEGIS-128L. The ciphertext and tag generation for each cipher of AEGIS family are done in four phases: (1) The initialization, (2) Processing the associated data, (3) The encryption, and (4) The finalization. Each of the ciphers takes a 128-bit key and a 128-bit nonce.

AEGIS-128 The 80-byte state S_i of AEGIS-128 at round i can be defined as

$$S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}$$

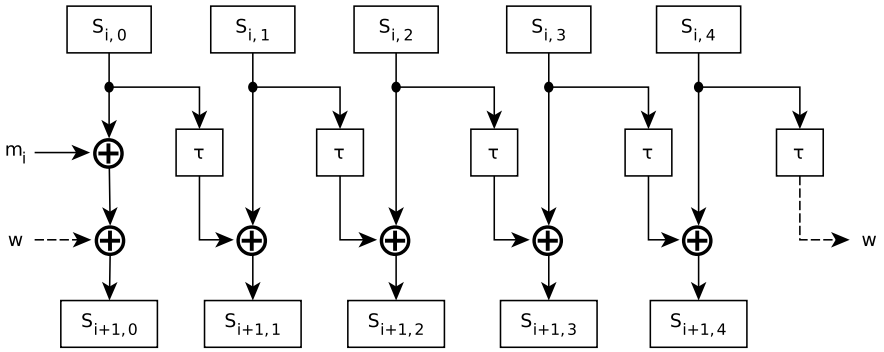

Fig. 1 The state update function of AEGIS-128

where each $S_{i,j}$, $j = 0$ to 4, is a 16-byte block. At each round i, a 16-byte data block m_i is used to update the state S_i. The next state S_{i+1} is computed as follows:

$$\begin{aligned} S_{i+1,0} &= AESRoundFunction(S_{i,4}, S_{i,0} \oplus m_i) \\ S_{i+1,1} &= AESRoundFunction(S_{i,0}, S_{i,1}) \\ S_{i+1,2} &= AESRoundFunction(S_{i,1}, S_{i,2}) \\ S_{i+1,3} &= AESRoundFunction(S_{i,2}, S_{i,3}) \\ S_{i+1,4} &= AESRoundFunction(S_{i,3}, S_{i,4}) \end{aligned}$$

The state update function is shown in Fig. 1. In the encryption (i.e., third phase), a 16-byte plaintext P_i at round i is used to update the state, and P_i is encrypted to a 16-byte ciphertext C_i as $C_i = P_i \oplus Z_i$, where $Z_i = S_{i,1} \oplus S_{i,4} \oplus (S_{i,2} \& S_{i,3})$ is a 16-byte keystream block.

AEGIS-256 The 96-byte state S_i of AEGIS-256 at round i can be defined as

$$S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}||S_{i,5}$$

where each $S_{i,j}$, $j = 0$ to 5, is a 16-byte block. At each round i, a 16-byte data block m_i is used to update the state S_i. The next state S_{i+1} is computed as follows:

$$
\begin{aligned}
S_{i+1,0} &= AESRoundFunction(S_{i,5}, S_{i,0} \oplus m_i) \\
S_{i+1,1} &= AESRoundFunction(S_{i,0}, S_{i,1}) \\
S_{i+1,2} &= AESRoundFunction(S_{i,1}, S_{i,2}) \\
S_{i+1,3} &= AESRoundFunction(S_{i,2}, S_{i,3}) \\
S_{i+1,4} &= AESRoundFunction(S_{i,3}, S_{i,4}) \\
S_{i+1,5} &= AESRoundFunction(S_{i,4}, S_{i,5})
\end{aligned}
$$

In the encryption (i.e., third phase), a 16-byte plaintext P_i at round i is used to update the state, and P_i is encrypted to a 16-byte ciphertext C_i as $C_i = P_i \oplus Z_i$, where $Z_i = S_{i,1} \oplus S_{i,4} \oplus S_{i,5} \oplus (S_{i,2} \& S_{i,3})$ is a 16-byte keystream block.

AEGIS-128L The 128-byte state S_i of AEGIS-128L at round i can be defined as

$$S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}||S_{i,5}||S_{i,6}||S_{i,7}$$

where each $S_{i,j}$, $j = 0$ to 7, is a 16-byte block. At each round i, two 16-byte data blocks m_{2i} and m_{2i+1} are used to update the state S_i. The next state S_{i+1} is computed as follows:

$$
\begin{aligned}
S_{i+1,0} &= AESRoundFunction(S_{i,7}, S_{i,0} \oplus m_{2i}) \\
S_{i+1,1} &= AESRoundFunction(S_{i,0}, S_{i,1}) \\
S_{i+1,2} &= AESRoundFunction(S_{i,1}, S_{i,2}) \\
S_{i+1,3} &= AESRoundFunction(S_{i,2}, S_{i,3}) \\
S_{i+1,4} &= AESRoundFunction(S_{i,3}, S_{i,4} \oplus m_{2i+1}) \\
S_{i+1,5} &= AESRoundFunction(S_{i,4}, S_{i,5}) \\
S_{i+1,6} &= AESRoundFunction(S_{i,5}, S_{i,6}) \\
S_{i+1,7} &= AESRoundFunction(S_{i,6}, S_{i,7})
\end{aligned}
$$

In the encryption phase, two 16-byte plaintext P_{2i} and P_{2i+1} at round i are used to update the state, and P_{2i} and P_{2i+1} are encrypted to two 16-byte ciphertext C_{2i} as $C_{2i} = P_{2i} \oplus Z_{2i}$ and C_{2i+1} as C_{2i+1} as $C_{2i+1} = P_{2i+1} \oplus Z_{2i+1}$, respectively, where $Z_{2i} = S_{i,1} \oplus S_{i,6} \oplus (S_{i,2} \& S_{i,3})$ and $Z_{2i+1} = S_{i,2} \oplus S_{i,5} \oplus (S_{i,6} \& S_{i,7})$ are two 16-byte keystream blocks.

2.2 Attack Description for AEGIS Family

Differential Fault Analysis of AEGIS family of ciphers is introduced in [7]. One can find a state of the ciphers by DFA, and eventually, mount forgery attack [8] by the change of one ciphertext and the associated authentication tag. Here, we present the attack description in detail.

2.2.1 *Attack Model*

The attacker can run the cipher with the same secret key, public parameters, and plaintext several times. The attacker is able to inject single-bit faults. The attacker has control on the timing of fault injection, and on the fault location. The plaintext and the corresponding fault-free/faulty ciphertext are available to the attacker.

Attack on AEGIS-128 The states of the cipher at rounds i and $i+1$ are as follows:

$$S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}$$
$$S_{i+1} = S_{i+1,0}||S_{i+1,1}||S_{i+1,2}||S_{i+1,3}||S_{i+1,4}$$

By the encryption, the generated ciphertext C_i at round i, C_{i+1} at round $i+1$ are given by $C_i = P_i \oplus Z_i$ and $C_{i+1} = P_{i+1} \oplus Z_{i+1}$, respectively, where

$$Z_i = S_{i,1} \oplus S_{i,4} \oplus (S_{i,2} \& S_{i,3}) \quad (1)$$
$$Z_{i+1} = S_{i+1,1} \oplus S_{i+1,4} \oplus (S_{i+1,2} \& S_{i+1,3}) \quad (2)$$

The state $S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}$ can be recovered by injecting 3×128 single-bit faults. The state recovery procedure is illustrated in Table 1.

Attack on AEGIS-256 Let the states of the cipher at rounds i, $i+1$, and $i+2$ be S_i, S_{i+1}, and S_{i+2}, respectively. By the encryption, the generated ciphertext C_i at round i, C_{i+1} at round $i+1$, and C_{i+2} at round $i+2$ are given by $C_i = P_i \oplus Z_i$, $C_{i+1} = P_{i+1} \oplus Z_{i+1}$, and $C_{i+2} = P_{i+2} \oplus Z_{i+2}$, respectively, where

Table 1 Recovering the cipher state of AEGIS-128

Steps	Blocks recovered	Recovering procedure
1	$S_{i,2}$	Injecting 128 single-bit faults into $S_{i,3}$ block, and using faulty Z_i and fault-free Z_i by Eq. (1)
2	$S_{i,3}$	Injecting 128 single-bit faults into $S_{i,2}$ block, and using faulty Z_i and fault-free Z_i by Eq. (1)
3	$S_{i+1,2}$	Injecting 128 single-bit faults into $S_{i+1,3}$ block, and using faulty Z_{i+1} and fault-free Z_{i+1} by Eq. (2)
4	$S_{i,1}$	Using $S_{i+1,2} = AESRoundFunction(S_{i,1}, S_{i,2}) = \tau(S_{i,1}) \oplus S_{i,2}$ by the inverse round function
5	$S_{i,4}$	Using Eq. (1)
6	$S_{i+1,3}$	Using $S_{i+1,3} = AESRoundFunction(S_{i,2}, S_{i,3}) = \tau(S_{i,2}) \oplus S_{i,3}$
7	$S_{i+1,4}$	Using $S_{i+1,4} = AESRoundFunction(S_{i,3}, S_{i,4}) = \tau(S_{i,3}) \oplus S_{i,4}$
8	$S_{i+1,1}$	Using Eq. (2)
9	$S_{i,0}$	Using $S_{i+1,1} = AESRoundFunction(S_{i,0}, S_{i,1}) = \tau(S_{i,0}) \oplus S_{i,1}$ by the inverse round function

Table 2 Recovering the cipher state of AEGIS-256

Steps	Blocks recovered	Recovering procedure
1	$S_{i,2}$	Injecting 128 single-bit faults into $S_{i,3}$ block, and using faulty Z_i and fault-free Z_i by Eq. (3)
2	$S_{i,3}$	Injecting 128 single-bit faults into $S_{i,2}$ block, and using faulty Z_i and fault-free Z_i by Eq. (3)
3	$S_{i+1,2}$	Injecting 128 single-bit faults into $S_{i+1,3}$ block, and using faulty Z_{i+1} and fault-free Z_{i+1} by Eq. (4)
4	$S_{i+1,3}$	Using $S_{i+1,3} = AESRoundFunction(S_{i,2}, S_{i,3}) = \tau(S_{i,2}) \oplus S_{i,3}$
5	$S_{i,1}$	Using $S_{i+1,2} = AESRoundFunction(S_{i,1}, S_{i,2}) = \tau(S_{i,1}) \oplus S_{i,2}$ by the inverse round function
6	$S_{i+2,3}$	Using $S_{i+2,3} = AESRoundFunction(S_{i+1,2}, S_{i+1,3})$ $= \tau(S_{i+1,2}) \oplus S_{i+1,3}$
7	$S_{i+2,2}$	Injecting 128 single-bit faults into $S_{i+2,3}$ block, and using faulty Z_{i+2} and fault-free Z_{i+2} by Eq. (5)
8	$S_{i+1,1}$	Using $S_{i+2,2} = AESRoundFunction(S_{i+1,1}, S_{i+1,2})$ $= \tau(S_{i+1,1}) \oplus S_{i+1,2}$ by the inverse round function
9	$S_{i,0}$	Using $S_{i+1,1} = AESRoundFunction(S_{i,0}, S_{i,1}) = \tau(S_{i,0}) \oplus S_{i,1}$ by the inverse round function
10	$(S_{i,4} \oplus S_{i,5})$	Using Eq. (3)
11	$S_{i,4}$	Using Eq. (4) defined as $Z_{i+1} = S_{i+1,1} \oplus \tau(S_{i,3}) \oplus S_{i,4} \oplus \tau(S_{i,4}) \oplus S_{i,5} \oplus (S_{i+1,2} \& S_{i+1,3})$
12	$S_{i,5}$	From known $(S_{i,4} \oplus S_{i,5})$ and $S_{i,4}$

$$Z_i = S_{i,1} \oplus S_{i,4} \oplus S_{i,5} \oplus (S_{i,2} \& S_{i,3}) \tag{3}$$

$$Z_{i+1} = S_{i+1,1} \oplus S_{i+1,4} \oplus S_{i+1,5} \oplus (S_{i+1,2} \& S_{i+1,3}) \tag{4}$$

$$Z_{i+2} = S_{i+2,1} \oplus S_{i+2,4} \oplus S_{i+2,5} \oplus (S_{i+2,2} \& S_{i+2,3}) \tag{5}$$

The state $S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}||S_{i,5}$ can be recovered by 4×128 single-bit faults. The state recovery procedure is illustrated in Table 2.

Attack on AEGIS-128L Let the states of the cipher at rounds i and $i+1$ be S_i and S_{i+1}, respectively. By the encryption, the generated ciphertext C_{2i} and C_{2i+1} at round i, C_{2i+2} and C_{2i+3} at round $i+1$ are given by $C_{2i} = P_{2i} \oplus Z_{2i}$, $C_{2i+1} = P_{2i+1} \oplus Z_{2i+1}$, $C_{2i+2} = P_{2i+2} \oplus Z_{2i+2}$, and $C_{2i+3} = P_{2i+3} \oplus Z_{2i+3}$, respectively, where

$$Z_{2i} = S_{i,1} \oplus S_{i,6} \oplus (S_{i,2} \& S_{i,3}) \tag{6}$$

$$Z_{2i+1} = S_{i,2} \oplus S_{i,5} \oplus (S_{i,6} \& S_{i,7}) \tag{7}$$

$$Z_{2i+2} = S_{i+1,1} \oplus S_{i+1,6} \oplus (S_{i+1,2} \& S_{i+1,3}) \tag{8}$$

$$Z_{2i+3} = S_{i+1,2} \oplus S_{i+1,5} \oplus (S_{i+1,6} \& S_{i+1,7}) \tag{9}$$

Table 3 Recovering the cipher state of AEGIS-128L

Steps	Blocks recovered	Recovering procedure
1	$S_{i,2}$	Injecting 128 single-bit faults into $S_{i,3}$ block, and using faulty Z_{2i} and fault-free Z_{2i} by Eq. (6)
2	$S_{i,3}$	Injecting 128 single-bit faults into $S_{i,2}$ block, and using faulty Z_{2i} and fault-free Z_{2i} by Eq. (6)
3	$S_{i,6}$	Injecting 128 single-bit faults into $S_{i,7}$ block, and using faulty Z_{2i+1} and fault-free Z_{2i+1} by Eq. (7)
4	$S_{i,7}$	Injecting 128 single-bit faults into $S_{i,6}$ block, and using faulty Z_{2i+1} and fault-free Z_{2i+1} by Eq. (7)
5	$S_{i,1}$	Using Eq. (6)
6	$S_{i,5}$	Using Eq. (7)
7	$S_{i+1,2}$	Using $S_{i+1,2} = AESRoundFunction(S_{i,1}, S_{i,2}) = \tau(S_{i,1}) \oplus S_{i,2}$
8	$S_{i+1,3}$	Using $S_{i+1,3} = AESRoundFunction(S_{i,2}, S_{i,3}) = \tau(S_{i,2}) \oplus S_{i,3}$
9	$S_{i+1,6}$	Using $S_{i+1,6} = AESRoundFunction(S_{i,5}, S_{i,6}) = \tau(S_{i,5}) \oplus S_{i,6}$
10	$S_{i+1,7}$	Using $S_{i+1,7} = AESRoundFunction(S_{i,6}, S_{i,7}) = \tau(S_{i,6}) \oplus S_{i,7}$
11	$S_{i+1,1}$	Using Eq. (8)
12	$S_{i+1,5}$	Using Eq. (9)
13	$S_{i,0}$	Using $S_{i+1,1} = AESRoundFunction(S_{i,0}, S_{i,1}) = \tau(S_{i,0}) \oplus S_{i,1}$ by the inverse round function
14	$S_{i,4}$	Using $S_{i+1,5} = AESRoundFunction(S_{i,4}, S_{i,5}) = \tau(S_{i,4}) \oplus S_{i,5}$ by the inverse round function

The state $S_i = S_{i,0}||S_{i,1}||S_{i,2}||S_{i,3}||S_{i,4}||S_{i,5}||S_{i,6}||S_{i,7}$ can be recovered by 4×128 single-bit faults. The state recovery procedure is illustrated in Table 3.

3 Countermeasures

Here, we propose the countermeasures against differential fault attack on AEGIS family by slight modification of the 16-byte block keystream generation in the encryption function. By the modified encryption functions, one can not recover a state of the ciphers of AEGIS family, and hence can not mount a forgery attack on the tag generation.

3.1 Countermeasure for AEGIS-128

We modify the keystream generation function. Under this modification, the keystreams at rounds i and $i + 1$ are as follows: