

prof. dr hab. Mirosław Kutylowski

Curriculum Vitae

Mirosław Kutylowski

I agree to process the personal data contained in the CV for the purpose of ESCAPE project proposal evaluation.

Personal:

- born in Wrocław, Poland
- nationality: Polish, citizenship: Polish
- foreign languages spoken: German, English, some knowledge of Russian and Chinese

Education:

- 1976-1980, graduate studies: Institute of Mathematics, University of Wrocław, individual program in foundations of mathematics 1977-1980,
- 1980, Master degree in Mathematics,
- 1984-1985, Graduate School, City University of New York, Ph.D. studies in computer science,
- 1985, Ph.D. in mathematical sciences, area: theory of computing, Institute of Mathematics University of Wrocław, supervisor prof. L. Pacholski, Dissertation: *"Small Grzegorzczuk classes and relations defined by simultaneous recursion and iteration"*
- 1992, Habilitation in mathematical sciences, Institute of Mathematics, University of Wrocław, Dissertation: *"Computational complexity of one-way multihead automata"*
- 1998, Professor title in mathematical sciences

Occupation:

- 1980 – 1986, research and teaching assistant, Institute of Computer Science, University of Wrocław, on a leave 1984 – 1985
- 16.09.1984 – 30.05.1985, Research Assistant, Graduate Center CUNY, USA
- 01.01.1985 – 30.05.1985, Adjunct Lecturer, Brooklyn College CUNY, USA
- 01.10.86 – 30.04.95, assistant professor in Institute of Computer Science, University of Wrocław, on a leave 01.04.1988 – 31.08.1989, 1.02.1991 – 31.01.92 and since 1.03.1994
- 01.04.1988 – 31.08.1989 and 26.05.1990 – 26.06.1990, Humboldt Fellow at Institut für Theoretische Informatik, Technische Hochschule Darmstadt, Germany
- 1.02.1991 – 31.01.92, Wiss. Angestellter in the project DFG Me 872/1-4 lead by Prof. Meyer auf der Heide, Fachbereich Mathematik–Informatik, Universität-GH Paderborn
- 1.09.1992 – 30.09.92, Wiss. Angestellter in the project DFG Di 412/2-1, Fachbereich Mathematik–Informatik, Universität-GH Paderborn
- 01.09.92–15.03.1994, leader of Theoretical Computer Science Division at Institute of Computer Science, University of Wrocław,
- 1.09.1993 – 30.09.93, visiting professor, Fachbereich Mathematik–Informatik, Universität-GH Paderborn

- 1.04.94 – 30.12.1997, Fachbereich Mathematik–Informatik, Universität-GH Paderborn
 - professor of applied computer science (C3, Vertretung), Spring term 1994
 - Hochschuldozent 1994-1997
- since 1.01.98-30.09.2000, extraordinary professor in the Institute of Computer Science, University of Wrocław, leader of "Computational Complexity and Algorithms" Division at Institute of Computer Science, University of Wrocław,
- 1.10.98-30.09.2002, extraordinary professor at Poznań University (part time), Department of Mathematics and Computer Science
- since 1.10.2000, full professor at Wrocław University of Technology, Institute of Mathematics and Computer Science, leader of Computer Science research group
- 2001-2005, Chairman of Scientific Board of TP Internet company,
- since 01.2007 member of Scientific Board of Institute of Foundations of Computer Science, Polish Academy of Sciences (elected for the third term)
- 2018-ongoing, Hua Shan Professor at Xidian University, School of Cyber Engineering (gast professor status)

Teaching in the following areas: theory of computing and automata theory, computer science logic, descriptive programming, functional programming, parallel programming, design of programming languages, formal languages, translation techniques and compilers, computational complexity theory, Boolean circuits, parallel algorithms, distributed algorithms, ad hoc systems, communication complexity, randomized algorithms, VLSI design, embedded systems, P2P systems, information theory, error correcting codes, data compression, digital image coding, cryptography, computer security, privacy protection, smart cards, embedded systems for security applications
law for IT professionals

Work at foreign scientific institutions:

- foreign expert in Base 111 Project Secure Mobile Internet at Xidian University
- member of editorial board of *Fundamenta Informaticae* (2006-2012)
- co-editor of „Towards Trustworthy Election Systems“, Springer Verlag
- co-organizer of Dagstuhl Seminars (Leibniz Zentrum für Informatik, Germany):
 - „Frontiers in Electronic Voting“(2007)
 - „Democracy in a Network Society“(2009)
- member of Steering Committee of ESORICS (European Symposium on Research in Computer Security) and of SOFSEM (Current Trends in Theory and Practice of Computer Science)
- PC co-chairman of NSS'2020 , Melbourne
- PC co-chairman of FCT (17th International Symposium on Fundamentals of Computation Theory, Wrocław, 2009)
- chairman of Frontiers in Electronic Elections Workshop (2006)
- PC co-chairman of ALGOSENSORS, Wrocław (2007),
- PC co-chairman of INSCRYPT (International Conference on Information Security and Cryptology, Beijing, 2012)

- PC co-chairman of SNFC (Secure Networking and Forensic Computing, workshop in conjunction with IEEE ICC, Sydney, 2014)
- PC co-chairman and organizer of ESORICS (European Symposium on Research on Computer Security, Wroclaw, 2014)
- PC co-chairman of IEEE SOCIALSEC (Fiji, 2016)
- PC co-chairman of IFIP SEC (Poznan, 2018)
- Program Committee member of major international conferences (since 2005 till 2019):
 - NSS'2019 (Saporro, 2019)
 - ML4CS'2019 (Xi'an, 2019)
 - CECC'2019 (Brno, 2019)
 - PriCom'2019 (Canterbury, 2019)
 - ISPEC'2019 (Kuala Lumpur, 2019)
 - ACNS'2019 (Colombia, 2019)
 - Asia PKC'2017, (Abu Dhabi, 2017)
 - 2nd Singapore Cyber Security R&D Conference, (Singapore, 2016)
 - Secitc'2017, (Bucharest, Romania, 2017)
 - ACISP'2017, (Auckland, New Zealand, 2017)
 - ISPEC'2016, (Zhangjiajie, China, 2016)
 - Secitc'2016 (Bucharest, Romania, 2016)
 - ACM CPSS'2016 (Cyber-Physical System Security Workshop, Xi'an, 2016)
 - Asia PKC 2016, (Xi'an, 2016)
 - ASIACCS' 2016 (ACM Symposium on Information, Computer and Communications Security, Xi'an, 2016)
 - IEEE CCNC'2016 (Annual Consumer Communications and Networking Conference , Las Vegas, 2016)
 - International Workshop on Secure Internet of Things 2015, (ESORICS workshop)
 - PROVSEC 2015 (Kanazawa, Japan)
 - IWCC 2015 (International Workshop on Cyber Crime, Toulouse, France)
 - NSS'2015 (9th International Conference on Network and System Security , New York City)
 - ISPEC 2015 (11st International Conference on Information Security Practice and Experience, Beijing, 2015)
 - ASIACCS' 2015 (ACM Symposium on Information, Computer and Communications Security , Singapore, 2015)
 - 1st Cyber-Physical System Security Workshop (CPSS, Singapore, 2015)
 - IEEE CCNC'2015 (12nd Annual Consumer Communications and Networking Conference , Las Vegas, 2015)
 - PROVSEC 2014 (Hong Kong 2014)
 - IEEE CSC (International Conference on Cloud and Service Computing, Beijing 2013)
 - ICDCN (International Conference on Distributed Computing and Networking, Mumbai 2014)
 - ISPEC (Information Security Practice & Experience Conference, Fuzhou 2014)
 - ESORICS (European Symposium on Research in Computer Security, Royal Holloway, 2013)
 - IEEE IWCC (International Workshop on Cyber Crime, San Francisco, 2013)

- ICALP (International Colloquium on Algorithms Languages and Programming, Riga, 2013)
- RFID Sec Asia (Guangzhou, 2013)
- PKC (Public Key Cryptography, Darmstadt, 2012)
- ACNS (Applied Cryptography and Network Security, Singapore, 2012)
- INSCRYPT (China International Conference on Information Security and Cryptology, Beijing, 2011)
- IMACC (IMA International Conference on Cryptography and Coding, Oxford, 2011)
- 1st IEEE International Workshop on Security in Computers, Networking and Communications, Shanghai (2011)
- RFIDSec Asia (Workshop on RFID Security, Wuxi, 2011)
- NMITS (International Conference on New Technologies, Mobility and Security, Paris, 2011)
- WISTP (Workshop in Information Security Theory and Practice, Iraklion, 2011)
- IEEE CCNC (Consumer Communication & Networking Conference, Las Vegas, 2011)
- ATC (International Conference on Autonomic and Trusted Computing, Xián, 2010)
- Securecomm (Singapore, 2010)
- ICALP (37 International Colloquium on Automata, Languages and Programming, Bordeaux, 2010)
- CT RSA (RSA Conference, Cryptographers Track, San Francisco, 2010)
- IEEE IPDPS (26th IEEE International Parallel & Distributed Processing Symposium, Atlanta, 2010)
- RFIDSec Asia (Workshop on RFID Security, Singapore, 2010)
- ATC (6th International Conference on Autonomic and Trusted Computing, Brisbane, 2009)
- ISPEC (The 5th Information Security Practice and Experience Conference, Xi'an, 2009)
- INSCRYPT (International Conference on Information Security and Cryptology, Beijing, 2009)
- INSCRYPT (International Conference on Information Security and Cryptology, Beijing, 2008)
- ProvSec (Provable Security, Shanghai, 2008)
- ALGOSENSORS, Reykjavik 2008)
- ACM/IEEE DCOSS (IEEE International Conference on Distributed Computing in Sensor Systems, Santorini Island, 2008)
- ESORICS (European Symposium on Research in Computer Security, Dresden, 2007)
- ALGOSENSORS (Venice 2006)
- IASTED PDCN (The IASTED International Conference on Parallel and Distributed Computing and Networks, Innsbruck, 2006)
- Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (Denver, 2005)
- IASTED PDCN (The IASTED International Conference on Parallel and Distributed Computing and Networks, 2005)

Public service:

- expert of Ministry of Digitalization - electronic personal identity document
- expert of Polish Election Committee, problems of IT systems supporting the election process,
- served as a member of a commission in Polish Ministry of Justice, preparation legislation for the project on electronic court (Elektroniczne Postępowanie Upominawcze, the solution has been successfully implemented,

- former member of of Commission for IT Infrastructure for Science in Polish Ministry of Science and Higher Education,
- served as an expert in Polish Ministry of Interior and Administration concerning security and cryptography issues, 2009-2010, 2016
- member of Award Commission in Ministry of Science and Higher Education (2012-2015)
- delegate of Poland to Council of Europe for a work group on electronic voting procedures,
- expert work for diverse public institutions in Poland concerning problems of computer security technology, includes work for Polish Parliament and political parties
- member of *Centralna Komisja ds Stopni i Tytułów* (Central Committee for Academic Degrees and Titles), elected for the period 2013-2016, mathematical sciences, field: computer science, re-elected for the term 2017-2021
- member of Research Council (elected for the third term) of Institute of Computer Science, Polish Academy of Sciences

Industry co-operation and technology transfer work:

- chairman of the scientific board of certification authority SIGNET (terminated)
- scientific advisor of AxIT Poland (terminated)
- technology transfer projects in the scope of:
 - telecommunication (with Siemens)
 - e-voting (project implemented in party elections by Platforma Obywatelska)
 - digital signature for public administration (with Trusted Information Consulting)
 - embedded systems (with Microtech International)
 - telecommunication (with Datax)
 - cloud computing (with IBM)
 - cryptography for microcontrollers (with REC Global)
 - computer security in financial institutions, Association for Polish Banks

Current research areas: ad hoc network communication protocols, self-organization of radio networks, security of cloud computing, RFID technology, anonymity and privacy protection, hardware cryptography, malicious cryptography, e-voting, key management, long time security, legal systems and information technology

Previous research areas: set theory and foundations of mathematics, low Grzegorzczak classes, systems of finite automata and bounded arithmetic, alternating Turing machines, PRAM algorithms, sorting on comparator networks, periodic sorting networks, randomized parallel algorithms, rapid mixing algorithms, lower bounds for parallel communication complexity, communication complexity for finite devices, asynchronous systems

Main awards:

- Alexander von Humboldt-Fellowship, 1987
- Mistrz Award of Foundation for Polish Science 2009
- IBM Faculty Award 2012
- PIIT Award 2013 (The Polish Chamber of Information Technology and Telecommunications), the award given for the impact for the IT market in Poland
- award of the Polish Bank Association (2016)
- Hua Shan Fellow, Xidian University (2018)