Wrocław, October 6, 2021

LIST OF PAPERS

Mirosław Kutyłowski

[1] **"Boolean operations over measure algebras"**, coauthor A. Kamburelis, *Coll. Math.*, 50.2 (1986).

[2] **"Restricted comprehension and collection schemata in weak set theories"**, *Zt. math. Log. Grundlag. Math.*, 30.1 (1987).

[3] **"Small Grzegorczyk classes and relations defined by simultaneous recursion and iteration"**, PhD. Dissertation, Instytut Matematyki Uniwersytetu Wrocławskiego, 1984.

[3a] **"Small Grzegorczyk classes"**, journal version of PhD. Dissertation, *the Journal of the London Mathematical Society*, 36.2 (1987), 193–210.

[4] **"A generalized Grzegorczyk hierarchy and low complexity classes"**, *Information and Computation* 72.2 (1987), 133-149.

[5] **"A note about $E_*^0 = E_*^2$? problem"**, coauthor K. Loryś, *Zt. math. Logik und Grundlag. Math.*, 33 (1987).

[6] **"Finite automata, real time processes and counting problem for bounded arithmetics"**, *the Journal of Symbolic Logic*, 53.1 (1988), 243–258.

[7] **"Chains of finite automata with bounded number of states"**, *Fundamenta Informaticae*, 11.3 (1988).

[8] **"Reversal complexity classes for alternating Turing machines"**, coauthors: M. Liśkiewicz and K. Loryś, *SIAM Journal on Computing*, 19.2 (1990), 207-221.

[9] **"MicroProlog - Opis języka programowania"**, textbook in Polish ('MicroProlog - programming language description)" *Wydawnictwo Uniwersytetu Wrocławskiego*, 1989.

[10] **"Multihead one-way finite automata"**, *Theoretical Computer Science*, 85 (1991), 135–153.

[11] **"One-way multihead finite automata and 2-bounded languages"**, *Mathematical Systems Theory*, 23 (1990), 107–139.

[12] **"Remarks on sorting and one-way multihead finite automata"**, *Information Processing Letters*, 36 (1990), 215–218.

[13] **"Time complexity of Boolean functions on CREW PRAMs"**, *SIAM Journal on Computing*, 20 (1991), 824–833.

[14] **"Stack versus sensitivity for one-way automata"**, *Theoretical Computer Science*, 119.2 (1993), 233-246.

[10a],[11a],[12a],[14a] **"Computational power of one-way multihead finite automata"**, surway over results in [11]-[14], *Proceedings of the Symposium on Theoretical Aspects of Computer Science*, (1990), Lecture Notes in Computer Science 415, C. Choffrut and T. Lengauer (eds.), 176-187.

[15] **"Exact time bounds for computing Boolean functions on PRAMs without simultaneous writes"**, coauthors: M. Dietzfelbinger and R. Reischuk, *Proceedings of 2nd ACM Symposium on Parallel Algorithms and Architectures* (1990), 125-135.

[16] **"Broadcasting information by exclusive read PRAMs"**, coauthors: P. Beame and M. Kik, *Parallel Processing Letters*, 4.1&2 (1994), 159–169.

[17] **"Exact lower time bounds for Boolean functions on CREW PRAMs"**, coauthors: M. Dietzfelbinger and R. Reischuk, journal version of the first part of [15], *Journal of Computer and System Sciences*, 48.2 (1994), 231–254.

[18] **"Feasible time-optimal algorithms for Boolean functions on exclusive read PRAMs"**, coauthors: M. Dietzfelbinger and R. Reischuk, journal version of the second part of [15], *SIAM Journal on Computing*, 25.6 (1996), 1196-1230.

[19] **"Limits on the power of parallel random access machines with weak forms of write conflict resolution"**, coauthors: F. Fich, R. Impagliazzo, B. Kapron, and V. King, *STACS 93, 10th Annual Symposium on Theoretical Aspects of Computer Science, Würzburg, Germany, February'93, Proceedings*, Lecture Notes in Computer Science 665 (Springer, Berlin, 1993), 386–397.

[19a] **"Limits on the power of parallel random access machines with weak forms of write conflict resolution"**, coauthors: F. Fich, R. Impagliazzo, B. Kapron, and V. King, full journal version of [19], *Journal of Computer and System Sciences*, 53.1 (1996) 104–111.

[20] **"Fast merging on the EREW PRAM"**, coauthor T. Hagerup, *Proc. of International Coll. on Automata Languages and Programming* '92, Lecture Notes in Computer Science 623 (Springer, Berlin, 1992), 318–329.

[20a] **"Fast merging on the EREW PRAM"**, coauthor T. Hagerup, full journal version of [20], *Algorithmica*, 17.1 (1997), 55–66.

[21] **"Complexity of Boolean functions on PRAMs – lower bound techniques"**, surway paper *Data Structures and Efficient Algorithms*, B. Monien and Th. Ottman (eds.), Lecture Notes in Computer Science 594 (Springer, Berlin, 1992), 309–329.

[22] **"Sorting on 2-dimensional grids"**, coauthor R. Wanka, *Parallel Processing Letters*, 2.2 and 2.3 (1992), 213–220.

[23] **"Retrieval of scattered information by EREW, CREW and CRCW PRAMs"**, coauthors: F. Fich, M. Kowaluk, K. Loryś and P. Ragde, *Algorithm Theory - SWAT'92*, Lecture Notes in Computer Science 621 (Springer, Berlin, 1992), 30-41,

[23a] **"Retrieval of scattered information by EREW, CREW and CRCW PRAMs"**, coauthors: F. Fich, M. Kowaluk, K. Loryś and P. Ragde, full journal version of [23], *Computational Complexity*, 5 (1995), 113–131.

[24] **"Playing Tetris on meshes and multi-dimensional SHEARSORT"**, coauthor R. Wanka, *Algorithms and Computation, 8th International Symposium on Algorithms and Computation, Singapore, December'97, Proceedings*, Lecture Notes in Computer Science 1350 (Springer, Berlin, 1997). 32–41.

[25] **"Periodic constant depth sorting networks"**, coauthors: M. Kik and G. Stachowiak, *STACS 94, 11th Annual Symposium on Theoretical Aspects of Computer Science, Caen, France, February'94, Proceedings*, Lecture Notes in Computer Science 775 (Springer, Berlin, 1994), 201–212.

[26] **"Approximate compaction and padded sorting on exclusive write PRAMs"**, coauthor T. Wierzbicki, *IPPS'96, International Parallel Processing Symposium, IEEE Press*, 174–181.

[27] **"Fast and feasible periodic sorting networks of constant depth"**, coauthors: K. Loryś, B. Oesterdiekhoff, and R. Wanka, *Proceedings 35th IEEE Symposium on Foundations of Computer Science, IEEE Press*, 1994, 369-380.

[27a] **"Constructing sorting networks with constant period**, coauthors: K. Loryś, B.Oesterdiekhoff, and R. Wanka, full journal version of the first part of [27], *Journal of the ACM*, 47(5) (2000), 944–967.

[28] **"Przydatność oceny hematologicznych wykładników infekcji w zapaleniu kości i stawów u noworodków"**, coauthors: Joanna Koralewska and Waldemar Maszkiewicz, poster presentation, 24 Sympozjum Pediatryczne, Gdańsk 1995, poster # 125.

[29] **"Limitations of the QRQW and EREW PRAM models"**, coauthor K. Loryś, *Foundations of Software Technology and Theoretical Computer Science. Proceedings 16th Conf.*, Hyderabad, India, Lecture Notes in Computer Science 1180 (Springer, Berlin, 1996), 310-321.

[30] **"Fast generation of random permutations via network simulation"**, coauthors: A. Czumaj, K. Loryś, and P. Kanarek, *ESA'96, 4th Annual European Symposium on Algorithms, Barcelona, Spain, September'96, Proceedings*, Lecture Notes in Computer Science 1136 (Springer, Berlin, 1996), 246–260.

[30a] **"Fast generation of random permutations via network simulation"**, coauthors: A. Czumaj, K. Loryś, and P. Kanarek, full journal version of [30], *Algorithmica*, 21 (1998), 2–20.

[31] **"Periodic merging networks"**, coauthors: K. Loryś, and B. Oesterdiekhoff, *Algorithms and Computation, 7th International Symposium on Algorithms and Computation, Osaka, Japan, December'96, Proceedings*, Lecture Notes in Computer Science 1178 (Springer, Berlin, 1996), 336–345.

[31a] **"Periodic merging networks"**, coauthors: K. Loryś and B. Oesterdiekhoff, full journal version of [30], *Theory of Computing Systems* 31.5 (1998), 551-578.

[32] **"Distributed stochastic processes for generating random permutations"**, coauthors: A. Czumaj, K. Loryś, and P. Kanarek, *Proc. of 10th ACM-SIAM Symposium on Discrete Algorithms* '99, SIAM, 1999, 271-280.

[32a] **"Generating random permutations and delayed path coupling method for mixing time of Markov chains"**, coauthor : A. Czumaj, full journal version of a part of [32], *Random Structures and Algorithms* 17 (2000), 238-259.

[33] **"Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych", ("Cryptography. Theory and practice for securing computer systems", in Polish)** coauthor Willy-B. Strothmann, READ ME, Warszawa, 1998 ((1999- second edition) ISBN 83-7147-087-9.

[35] **"Towards an efficient parallel minimum spanning tree algorithm"**, coauthors: Micah Adler, Wolfgang Dittrich, Ben Juurlink, and Ingo Rieping, *Proc. of 10th ACM Symposium on Parallel Algorithms and Architectures* '98, 27-38.

[36] **"Power of cooperation and multihead finite systems"**, coauthors: Pavol Duriš, Tomasz Jurdziski, and Krzysztof Loryś, *Proc. of International Coll. on Automata Languages and Programming* '98, Lecture Notes in Computer Science 1443 (Springer, Berlin, 1998), 896-907.

[37] **"Correction networks"**, coauthors: Marcin Kik and Marek Piotrów, *Proc. 1999 International Conference on Parallel Processing*, IEEE Computer Society, Los Alamitos, 1999, ISBN 0-7695-0350-0, 40–47.

[38] **"Multiparty finite computations"**, coauthors: Tomasz Jurdziński and Krzysztof Loryś, *Computing and Combinatorics, Proc. COCOON'99*, Lecture Notes in Computer Science 1627 (Springer, Berlin, 1999), 318–329.

[39] **"Stochastic kleptography detection"**, coauthor : Daniel Kucner, Public-Key Cryptography and Computational Number Theory, Walter de Gruyter, Berlin - New York 2001, 137–149.

[40] **"Communication gap for finite memory devices"**, coauthor : Tomasz Jurdziński, *Automata, Languages and Programming, Proc. ICALP'2001*, Lecture Notes in Computer Science 2076 (Springer, Berlin, 2001), 1052–1064.

[41] **"Switching Networks for Generating Random Permutations"**, coauthors: A. Czumaj, K. Loryś, and P. Kanarek, in *Switching Networks: Recent Advances*, Kluwer Academic Publishers, 2001, ISBN 0-7923-6953-X, .

[42] **"Communication Complexity for Asynchronous Systems of Finite Devices"**, coauthors: Tomasz Jurdziński and Jan Zatopiański, Proc. 15th International Parallel & Distributed Processing Symposium (IPDPS-01), IEEE Computer Society, 2001.

[43] **"Communication Complexity for Multi-speed Cooperting Automata "**, coauthors: Tomasz Jurdziński, Paweł Rzechonek and Jan Zatopiański, Prace Naukowe Instytutu Matematyki Politechniki Wrocawskiej, 24.3, 2001, 17-30.

[43a] **"Efficient simulation of synchronous systems by multi-speed systems"**, coauthors: Tomasz Jurdziński and Jan Zatopiański, RAIRO- Theoretical Informatics and Applications 39 (2005), 403-419.

[44] **"Energy-Efficient Size Approximation for Radio Networks with no Collision Detection"**, coauthors: Tomasz Jurdziński, and Jan Zatopiański, *(Proc. COCOON'2002)*, Lecture Notes in Computer Science 2387 (Springer-Verlag, Berlin, 2002), 279-289.

[45] **"Hamming Weight Attacks on Cryptographic Hardware – Breaking Masking Defense"**, coauthor Marcin Gomułkiewicz, *ESORICS'2002*, Lecture Notes in Computer Science 2502 (Springer-Verlag, Berlin, 2002), 90-103.

[46] **"Efficient algorithms for leader election in radio networks"**, coauthors: Tomasz Jurdziński, and Jan Zatopiański, 21nd ACM Symposium on Principles of Distributed Computing, Monterey, ACM Press, 2002, 51-57.

[47] **"Weak communication in radio networks"**, coauthors: Tomasz Jurdziński, and Jan Zatopiański, *Europar'2002*, Lecture Notes in Computer Science 2400 (Springer-Verlag, Berlin, 2002), 965-972.

[47a] **"Weak communication in single-hop radio networks – adjusting algorithms to industrial standards"**, coauthors: Tomasz Jurdziński and Jan Zatopiański, *Concurrency and Computation: Practice & Experience*, 15 (2003), 1117-1131.

[48] **"Computing average value in ad hoc networks"**, coauthor Daniel Letkiewicz, MFCS'2003, Lecture Notes in Computer Science 2747 (Springer-Verlag, Berlin, 2003) 511-520.

[49] **"Secure data storing in a pool of vulnerable servers"**, coauthor Marcin Gogolewski, Artificial Intelligence and Security in Computing Systems, ISBN 1-4020-7396-8, 217-226.

[50] **"Adversary immune leader election in ad hoc radio networks"**, coauthor Wojciech Rutkowski, ESA'2003, Lecture Notes in Computer Science 2832 (Springer-Verlag, Berlin, 2003), 397-408.

[51] **"Rapid mixing and security of Chaum's visual electronic voting"**, coauthor Marcin Gomułkiewicz, Marek Klonowski, Computer Security- ESORICS 2003, Lecture Notes in Computer Science 2808 (Springer Verlag, Berlin 2003), 132-145.

[52] **"Mobile mixing"**, coauthors: Marcin Gogolewski and Tomasz Łuczak, International Conference on Information Security and Cryptography (ICISC) 2005, Lecture Notes in Computer Science 3506 (Springer Verlag, Berlin 2004), 380-393.

[53] **"How to use untrusty cryptographic devices"**, coauthor Daniel Kucner, TATRACRYPT'03, Tatra Mountains Mathematical Publications, 29 (2004), 57-67.

[54] **"Robust Undetectable Interference Watermarks"**, coauthors: Ryszard Grząślewicz, Jarosław Kutylowski and Wojciech Pietkiewicz, Information Security and Hiding'2005, Lecture Notes in Computer Science 3481, (Springer Verlag, Berlin 2005), 517-526.

[55] **"Provable Unlinkability Against Traffic Analysis already after $O(\log(n))$ steps!"** coauthors: Marcin Gomułkiewicz, Marek Klonowski, Information Security: 7th International Conference (ISC'04). Lecture Notes in Computer Science 3225 (Springer Verlag, Berlin 2004), 354-366.

[56] **"Synchronization Fault Cryptoanalysis for Breaking A5/1"** coauthors: Marcin Gomułkiewicz, Theodor Vierhaus, Paweł Wlaź, 4th International Workshop on Efficient and Experimental Algorithms (WEA'05), Lecture Notes in Computer Science 3503 (Springer Verlag, Berlin 2005), 415-427.

[57] **"Secure initialization in single-hop radio networks"** coauthor Wojciech Rutkowski, ESAS'2004 (1st European Workshop on Security in Ad Hoc and Sensor Networks), Lecture Notes in Computer Science 3313 (Springer Verlag, Berlin 2004), 31-41.

[58] **"Anonymous Distribution of Encryption Keys in Cellular Broadcast Systems"**, coauthors: Jacek Cichoń, Łukasz Krzywiecki, Paweł Wlaź, Secure Mobile Ad-hoc Networks and Sensors 2005 (MADNES), Lecture Notes in Computer Science 4074 (Springer Verlag, Berlin 2006), 96-109.

[59] **"Onions Based on Universal Re-encryption – Anonymous Communication Immune Against Repetitive Attack "** coauthors: Marcin Gomułkiewicz, Marek Klonowski, Workshop on Information Security Applications (WISA) '2004, Lecture Notes in Computer Science 3325, 400-410.

[60] **"DUO–Onions and Hydra–Onions – failure and adversary resistant onion protocols"** coauthors: Jan Iwanik, Marek Klonowski, Communications and Multimedia Security, IFIP, (Springer Verlag, Berlin 2005, ISBN 0-387-24485-9), 1–15).

[61] **"UTRAN Topology Planning Including Point-to-Multipoint Equipment"**, coauthors: M. Gebala, B. Różański, J. Vossnaecker, Th. Winter, M. Zawada, MMB&PGTS'2004 (12th GI/ITG Conference on Measuring, Modelling and Evaluation of Computer and Communication Systems (MMB) together with 3rd Polish-German Teletraffic Symposium (PGTS)), VDE Verlag, Berlin 2004, ISBN 3-8007-2851-6, 87-92.

[62] **"Anonymous communication with on-line and off-line onion encoding"**, coauthors: M. Klonowski, F. Zagórski, SOFSEM'2005, Lecture Notes in Computer Science 3381 (Springer Verlag, Berlin 2004), 229-238.

[63] **"Distributed timestamping with boomerang onions"**, coauthors: Marcin Gogolewski and Tomasz Łuczak, Wartacrypt'2004, proceedings in Tatra Mountains Mathematical Publications 33, 31-40.

[64] **"Universal re-encryption of signatures and controlling anonymous information flow"**, coauthors: M. Klonowski, A. Lauks, F. Zagórski, Wartacrypt'2004, proceedings in Tatra Mountains Mathematical Publications 33, 2006, 179-188.

[65] **"Fault Cryptoanalysis for Breaking A5/1"** coauthors: Marcin Gomułkiewicz, Paweł Wlaź, Wartacrypt'2004, proceedings in Tatra Mountains Mathematical Publications.

[66] **"Provable anonymity for networks of mixes"**, coauthor M. Klonowski, Information Hiding Workshop '2005. Lecture Notes in Computer Science 3727 (Springer Verlag, Berlin 2005), 26-38.

[67] **"Privacy Protection for P2P Publish-Subscribe Networks"**, coauthor M. Klonowski, B. Różański, Security and Protection of Information'2005, Brno University of Defence 2005, ISBN 8085960-99-0, 63-74.

[68] **"A Practical Voting Scheme with Receipts"**, coauthors: M. Klonowski, A. Lauks, F. Zagórski, Information Security: 8th International Conference (ISC'2005), Lecture Notes in Computer Science 3650 (Springer Verlag, Berlin 2005), 490-497.

[69] **"Conditional Digital Signatures and Signing in the Future"**, coauthors: M. Klonowski, A. Lauks, F. Zagórski, TRUSTBUS'2005, Lecture Notes in Computer Science 3592 (Springer Verlag, Berlin 2005), 206-215.

[70] **"Local View Attack on Anonymous Communication"**, coauthors: M. Gogolewski, M. Klonowski, ESORICS'2005, Lecture Notes in Computer Science 3679 (Springer Verlag, Berlin 2005), 475-488.

[71] **"Hiding Data Sources in P2P Networks"**, coauthors: M. Klonowski, B. Różański, 4th International Workshop on Applied PKI (IWAP'2005), IOS Press, Amsterdam, ISBN 1-58603-550-9, 225-239.

[72] **"Intersection Attack and using Dummy Addresses"**, coauthor M. Kabarowski, Tatra Mountains Mathematical Publications 37 (2007), 49-57.

[73] **"Verifiable Internet Voting Solving Secure Platform Problem"**, coauthor F. Zagórski, IWSEC'2007, Lecture Notes in Computer Science 4752, 199-213.

[74] **"How to Protect a Signature from Being Shown to a Third Party"**, coauthors: M. Klonowski, P. Kubiak, A. Lauks, TRUSTBUS'2006, Lecture Notes in Computer Science 4083, 192-202.

[75] **"Adversary Immune Size Approximation of Single-Hop Radio Networks"**, coauthors: M. Kabarowski, W. Rutkowski, Theory and Applications of Models of Computation (TAMC'2006), Lecture Notes in Computer Science 3959, 148-158.

[76] **"Fault Cryptanalysis and Shrinking Generator"**, coauthors: M. Gomułkiewicz, P. Wlaź, WEA'2006, Lecture Notes in Computer Science 4007, 61–72.

[77] **"Kleptographic Attacks on E-voting Schemes"**, coauthors: M. Gogolewski, M. Klonowski, P. Kubiak, A. Lauks, F. Zagórski, ETRICS'2006, Lecture Notes in Computer Science 3995, 494-508.

[78] **"Initialization for Ad Hoc Radio Networks with Carrier Sensing and Collision Detection"**, coauthors: J. Cichoń, M. Zawada, 5th International Conference on AD-HOC Networks & Wireless Networks (AdHocNow'2006), Lecture Notes in Computer Science 4104, 308-320.

[79] **"Kleptographic Attacks on a Cascade of Mix Servers"**, coauthors: P. Kubiak, F. Zagórski, 2007 ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'07), ACM Press, 57-62.

[80] **"General Anonymous Key Broadcasting via Lagrangian Interpolation"**, coauthors: Ł. iecki, M. Nikodem, 1st International Workshop Group-Oriented Cryptographic Protocols, ICALP 2007 Workshop, journal version in IET Information Security, vol. 2.3, 79-84.

[81] **"Stealing Secrets with SSL/TLS and SSH – Kleptographic Attacks"**, coauthors: Z. Gołębiewski, F. Zagórski, The 5th International Conference on Cryptology and Network Security (CANS) 2006, Lecture Notes in Computer Science 4301, 191-202.

[82] **"Adaptive Initialization Algorithm for Ad Hoc Radio Networks with Carrier Sensing"**, coauthors: J. Cichoń, M. Zawada, ALGOSENSORS'2006, Lecture Notes in Computer Science 4240, 35-46,
full version: Theoretical Computer Science, 402(1) (2008), 16-28.

[83] **"Kleptographic Attacks on E-Auction Schemes"**, coauthors: M. Gogolewski, M. Gomułkiewicz, J. Grząślewicz, P. Kubiak, A. Lauks, 5th International Conference on Applied Cryptography and Network Security ACNS'2007, industrial track presentation. Tatra Mountains Mathematical Publications, volume 41, 2008, pp. 47-64

[84] **"Fault Jumping Attacks against Shrinking Generator"**, coauthors: M. Gomułkiewicz, P. Wlaź, preliminary version:Dagstuhl Technical Report, `http://drops.dagstuhl.de/portals/index.php?semnr=06111`, full version under title **"Random Fault Attack against Shrinking Generator"**, ALGOSENSORS'2008, Lecture Notes in Computer Science 5389, 87-99

[85] **"Kleptographic Weaknesses of Benaloh-Tuistra Protocol"**, coauthors: P. Borzęcki, J. Kabarowski, P. Kubiak, F. Zagórski, ICSNC'2006, IEEE Computer Society Press. `http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/icsnc/2006/2699/00/2699toc.xml`

[86] **"A Revocation Scheme Preserving Privacy"**, coauthors: Ł. Krzywiecki, P. Kubiak, INSCRYPT'2006, Lecture Notes in Computer Science 4318, 130-143.

[87] **"Anonymity and k-choice Identities"**, coauthor J.Cichoń, INSCRYPT'2007, Lecture Notes in Computer Science 4990, 283-297.

[88] **"Privacy Protection for Dynamic Systems Based on RFID Tags"**, coauthors: J.Cichoń, M. Klonowski 4th IEEE International Workshop on Pervasive Computing and Communication Security (PERSEC'2007), PERCOM 2007 Workshops, IEEE Computer Society, ISBN 0-7695-2788-4, 235-240.

[89] **"Practical Deniable Encryption"**, coauthors: M. Klonowski, P. Kubiak, SOFSEM'2008, Lecture Notes in Computer Science 4910, 599-609.

[90] **"Forward-secure Key Evolution Protocol in Wireless Sensor Networks"**, coauthors: M. Klonowski, K. Rybarczyk, M. Ren, The 6th International Conference on Cryptology and Network Security (CANS) 2007, Lecture Notes in Computer Science 4856, 102-120.

[91] **"Short Ballot Assumption and Threeballot Voting Protocol"**, coauthors: J. Cichoń, B. Węglorz, SOFSEM'2008, Lecture Notes in Computer Science 4910, 585-598.

[92] **"Step-out Ring Signatures"**, coauthors: M. Klonowski, Ł. Krzywiecki, A. Lauks, MFCS'2008, Lecture Notes in Computer Science 5162, 431-442.

[93] **"Self-stabilizing population of mobile agents"**, coauthors: Z. Gołębiewski, T. Łuczak, F. Zagórski, Proceedings of the 2008 IEEE International Parallel & Distributed Processing Symposium (IPDPS'2008), 29, , IEEE 2008, ISBN 978-1-42441694-3

[94] **"Step-out Group Signature Scheme"**, coauthors: M. Klonowski, Ł. Krzywiecki, A. Lauks, presented at 8th Central European Conference on Cryptography, Graz 2008, journal version: Computing 85(1-2): 137-151 (2009)

[95] **"Distributed Verification of Mixing - Local Forking Proofs Model"**, coauthors: J.Cichoń, M. Klonowski, Australasian Conference on Information Security and Privacy (ACISP 2008), Lecture Notes in Computer Science 5107, 128-140.

[96] **"Privacy Protection for RFID's – Hidden Subset Identifiers"**, coauthors: J.Cichoń, M. Klonowski, PERVASIVE'2008, Lecture Notes in Computer Science 5013, 298-314.

[97] **"Algorithmic Challenges for Sensor Networks - Preface to ALGOSENSORS'2007"**, ALGOSENSORS 2007, Lecture Notes in Computer Science 4837, 2008, 1-5.

[98] **"Repelling Detour Attack against Onions with Re-Encryption"**, coauthors: M. Klonowski, A. Lauks, ACNS'2008, Lecture Notes in Computer Science 5037, 296?-308.

[99] **"Leader Election for Multi-Channel Radio Networks - Dependent versus Independent Trials"**, coauthors: M. Klonowski, M. Koza, Z. Gołębiewski, 1st Asian Conference on Intelligent Information and Database Systems, 477-482, IEEE Computer Society, `http://doi.ieeecomputersociety.org/10.1109/ACIIDS.2009.29`

[100] **"Accessing a Shared Radio Channel"**, coauthors: J. Cichoń, M. Zawada, The European Integrated Project "Dynamically Evolving, Large Scale Information Systems (DELIS)", Proceedings of the Final Workshop, 57-62

[101] **" Key Levels and Securing Key Predistribution against Node Captures"**, coauthors: J. Cichoń, J. Grzaślewicz, ALGOSENSORS'2009, Lecture Notes in Computer Science 5304, 64-75, also presented at ACNS 2009, Industrial Track

[102] **"Power of Discrete Nonuniformity – Optimizing Access to Shared Radio Channel in Ad Hoc Networks"**, coauthors: J. Cichoń, M. Zawada, Proceedings of MSN (Mobile Ad-hoc and Sensor Networks)'2008, IEEE Computer Society Press, ISBN: 978-0-7695-3457-2, 9-15

[103] **"Scratch, Click & Vote: E2E Voting over the Internet"**, coauthor F. Zagórski, preprint: Cryptology ePrint Archive: Report 2008/314 `http://eprint.iacr.org/2008/314`, in: Towards Trustworthy Elections, in State-of-the-Art Survey Series, Springer Verlag, Lecture Notes in Computer Science 6000, 2010, 343-356

[104] **"Attacking and Repairing the Improved ModOnions Protocol"**, coauthors: N. Borisov, M. Klonowski, A. Lauks ICISC'2009, Lecture Notes in Computer Science 5984, 258-273, presented also at ACNS'2009, Industrial Track, journal extended version: **"Attacking and Repairing the Improved ModOnions Protocol-Tagging Approach"**, KSII Transactions on Internet and Information Systems, 4(3): 380-399 (2010)

[105] **"Towards Fair Leader Election in Wireless Networks"**, coauthors: Z. Gołębiewski, M. Klonowski, M. Koza, AD HOC NOW 2009, Lecture Notes in Computer Science 5793, 166-179

[106] **"Lagrangian E-Voting: Strong Privacy and Verfiability on Demand"**, coauthor Ł. Krzywiecki, TRUST'2010, Lecture Notes in Computer Science 6101, 109-123

[107] **"Detecting Heavy-Hitters in a P2P Network"**, coauthors: Zbigniew Gołębiewski, Jarosław Kutyłowski, Mirosław Kutyłowski, Filip Zagórski, Network and Service Security. IEEE 2009, ISBN 978-2-9532-4431-1, 1-6.

[108] **"Security Challenges for Wireless Sensor Networks. Dynamic Routing as a Security Paradigm"**, coauthors: M. Koza, M. Klonowski, ERCIM News 76, January 2009, `http://ercim-news.ercim.org/images/stories/EN76/EN76-web.pdf`,

[108a] **"How to Transmit Messages via WSN in a Hostile Environment"**, coauthors: M. Koza, M. Klonowski, SECRYPT'2011, SciTePress, 2011, ISBN 978-989-8425-71-3, 387-390.

[109] **"Energy Efficient Alert in Single-Hop Networks of Extremely Weak Devices"**, coauthors: M. Klonowski, J.Zatopiański, ALGOSENSORS'2009, Lecture Notes in Computer Science 5304, 139-150, journal version: Theoretical Computer Science, vol. 453, 2012, Pages 65â74

[110] **"On Optimal One-dimensional Routing Strategies in Sensor Networks"**, coauthors: J.Cichoń, M.Gębala, Broadcom'2009

[111] **"Hierarchical Ring Signatures"**, coauthors: Ł. Krzywiecki, A. Lauks-Dutka, presented at WeWorc' 2009 (Western European Workshop on Research in Cryptology), Graz

[112] **"How to Construct State Registries – Matching Undeniability with Public Security"**, coauthors: P. Kubiak, Jun Shao, Intelligent Information and Database Systems, ACIIDS 2010, Lecture Notes in Artificial Intelligence 5990, 64-73

[113] **"Mediated Signatures - Towards Undeniability of Digital Data in Technical and Legal Framework"**, coauthors: P. Kubiak, A. Lauks-Dutka, M. Tabor, 3rd Workshop on Legal Informatics and Legal Information Technology (LIT 2010), Lecture Notes in Business Information Processing 57, 298-309

[114] **"Repelling Sybil-type attacks in wireless ad hoc systems"**, coauthors: M. Koza, M. Klonowski, ACISP 2010, Lecture Notes in Computer Science 6168, 391-402

[115] **"Two-Head Dragon. Clone-Fail Signature Creation Devices"**, coauthors: P. Błaśkiewicz, P. Kubiak, INTRUST'2010, Lecture Notes in Computer Science 6802, 173-188

[117] **"From Key Predistribution to Key Redistribution "**, coauthors: J. Cichoń, Z. Gołębiewski, ALGOSENSORS'2010, Lecture Notes in Computer Science 6451, 92-104,

[117a] **"From Key Predistribution to Key Redistribution "**, coauthors: J. Cichoń, Z. Gołębiewski, extended version of [117], Theoretical Computer Science, vol. 453, 2012, pp. 75–87

[118] **"Digital Signatures for e-Government – a Long-Term Security Architecture"**, coauthors: P. Błaśkiewicz, P. Kubiak, Journal version: China Communications, vol. 7, no. 6, 2010, 64-70.

[119] **"Private Information Retrieval with a Trusted Hardware Unit - Revisited"**, coauthors: Ł. Krzywiecki, H. Misztela, T. Strumiński, INSCRYPT 2010, Lecture Notes in Computer Science 6584, 373-386

[120] **"Universal Step-out Ring Signatures"**, coauthor Ł. Krzywiecki, manuscript

[121] **"Signing with Multiple ID's and a Single Key"**, coauthor Jun Shao, IEEE Consumer Communications and Networking Conference (CCNC)'2011, ISBN 978-1-4244-8788-2 675-676

[122] **"1-out-of-2 Signature"**, coauthor Jun Shao, ACM ASIACCS, ACM Press, 391-395

[123] **"RFID Electronic Visa with Personalized Verification"**, coauthors: P. Błaśkiewicz, J. Cichoń, K. Majcher, In: Radio Frequency Identification Systems Security, IOS Press 2011, Cryptology and Information Security Series, vol. 6, pp. 81-95

[125] **"Collusion Resistant Anonymous Broadcast Encryption Scheme based on PUF"**, coauthor Ł. Krzywiecki, TRUST 2011, Lecture Notes in Computer Science 6740, 48-62

[127] **"Technical and Legal Meaning of "Sole Control" – Towards Verifiability in Signing Systems"**, coauthors: P. Błaśkiewicz, P. Kubiak, Ł. Krzywiecki, W. Paluszyński , M. Tabor, 4rd Workshop on Legal Informatics and Legal Information Technology (LIT 2011), LNBIP (Lecture Notes in Business Information Processing) 97, 277-288

[128] **"Restricted Identification Scheme and Diffie-Hellman Linking Problem"**, coauthors: Łukasz Krzywiecki, Przemysław Kubiak, Michał Koza, INTRUST 2011, Lecture Notes in Computer Science 7222, 221-238

[129] **"Optimizing Segment Based Document Protection"**, coauthor M. Gębala, SOFSEM 2012, Lecture Notes in Computer Science 7147, 566-575,
corrected version: **"Optimizing Segment Based Document Protection (Corrected Version)**, IACR eprint, 520 (2012), `http://eprint.iacr.org/2012/52`

[130] **"Attack against Ibrahim's Distributed Key Generation for RSA"**, coauthors: B. Brzeźniak, L. Hanzlik, P. Kubiak, International Journal of Network Security, Vol. 15, No. 1, 2013, 237-240

[131] **"Restricted Identification without Group Keys"**, coauthors: L. Hanzlik, K. Kluczniak, P. Kubiak, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE 2012, 1194-1199

[132] **"Lightweight Certificates- Towards a Practical Model for PKI"**, coauthors: Ł. Krzywiecki, P. Kubiak, M. Tabor, D. Wachnik, Business Information Systems - 15th International Conference, BIS 2012, Lecture Notes in Business Information Processing 117, 296-307

[133] **"Extreme Propagation in an Ad-hoc Radio Network - Revisited"**, coauthors: P. Błaśkiewicz, W. Wodo, K. Wolny, Computational Collective Intelligence Technologies and Applications, ICCCI 2012, Lecture Notes in Computer Science 7654, 142-151

[134] **"Proof of Possession for Cloud Storage via Lagrangian Interpolation Techniques"**, coauthor Ł. Krzywiecki, 6th International Conference on Network and System Security, NSS'2012, Lecture Notes in Computer Science 7645, 305-319

[135] **"How to Make Operating Systems for Smart Cards Open"**, coauthors: P.Błaśkiewicz, P. Kubiak, Bulcrypt'2012 Proceedings, ISBN 978-954-2946-22-9, 129-140

[136] **"Stamp & Extend - Instant but Undeniable Timestamping based on Lazy Trees"**, coauthors: Ł. Krzywiecki, P. Kubiak, INTRUST'2012, Lecture Notes in Computer Science 7711, 5-24

[137] **"Simplified PACE|AA Protocol"**, coauthors: L. Hanzlik, K. Kluczniak, Ł. Krzywiecki, ISPEC'2013, Lecture Notes in Computer Science 7863, 218-232

[138] **"Mutual Chip Authentication"**, coauthors: L. Hanzlik, K. Kluczniak, Ł. Krzywiecki, 3rd IEEE International Symposium on Anonymity and Communication Systems, in Proc. IEEE 12th International Conference on Trust, Security and Privacy in Computing and Communications, 1683-1689

[139] **"Disability Parking Permit"**, coauthor P. Lipiak, IEEE TRUSTID'2013, in Proc. IEEE 12th International Conference on Trust, Security and Privacy in Computing and Communications, 1535-1540

[140] **"Mutual Restricted Identification"**, coauthors: L. Hanzlik, K. Kluczniak, Ł. Krzywiecki, EUROPKI'2013, Lecture Notes in Computer Science 8341, 119-133

[141] **"Chameleon RFID and Tracking Prevention"**, coauthors: M. Klonowski, P. Syga, RFID Sec Asia'2013, Radio Frequency Identification System Security, pp. 17-30, IOS Press, ISBN 978-1-61499-327-8

[142] **"Bit Reversal Broadcast Scheduling for Ad Hoc Systems"**, coauthors: M. Kik, M. Gębala, IDCS'2013, Lecture Notes in Computer Science 8223, 223-237

[143] **"Protection of Data Groups from Personal Identity Documents"**, coauthors: P. Kubiak, W. Wodo, Journal of Infocommunications, V.3, 2013, 2-7

[144] **"Provable unlinkability against traffic analysis with low message overhead"**, coauthors: R. Berman, A. Fiat, M. Gomułkiewicz, M. Klonowski, T. Levinboim, A. Ta-Shma, Journal of Cryptology, 28(3) (2015), 623-640

[145] **"Probabilistic Admissible Encoding on Elliptic Curves -Towards PACE with Generalized Integrated Mapping"**, coauthors: P. Kubiak, Ł. Krzywiecki, SOFSEM 2014, Lecture Notes in Computer Science 8327, 395-406

[146] **"Supervised Usage of Signature Creation Devices"**, coauthor P. Kubiak, INSCRYPT 2013, Lecture Notes in Computer Science 8567, 132–149

[147] **"Lightweight Signature with Secretly Embedded Warning"**, coauthor P. Kubiak, Control & Cybernetics, 4/2013, pp. 825-827

[148] **"Efficient and Robust Data Aggregation Using Untrusted Infrastructure"**, coauthors: M. Koza, M. Klonowski, SIN 2013 (6th International Conference on Security of Information and Networks), ACM, 2013, ISBN 978-1-4503-2498-4, pp. 123-130

[149] **"Attack on a U-Prove Revocation Scheme from FC'13 - Passing Verification by Revoked Users"**, coauthors: L. Hanzlik, K. Kluczniak, Financial Cryptography 2014, Lecture Notes in Computer Science 8437, 283-290

[150] **"Forbidden City Model – towards a Practice Relevant Framework for Designing Cryptographic Protocols"**, coauthors: L. Hanzlik, K. Kluczniak, P. Kubiak, Ł. Krzywiecki, ISPEC 2014 (invited paper), Lecture Notes in Computer Science 8434, pp. 42-59

[151] **"Mixing in random digraphs with application to the forward-secure key evolution in WSNs"**, coauthors: M. Klonowski, M. Ren, K. Rybarczyk, ACM Transactions on Sensor Networks, vol. 11(2) (extended version of [90])

[152] **"Stand-by Attacks on E-ID Password Authentication"**, coauthors: L. Hanzlik, P. Kubiak, INSCRYPT 2014, Lecture Notes in Computer Science 8957, pp. 475-495

[153] **"Lightweight Protocol for Trusted Spontaneous Communication"**, coauthors: Przemysław Błaśkiewicz, Marek Klonowski, Piotr Syga, INTRUST 2014, Lecture Notes in Computer Science 9473, pp. 1â15

[154] **"On Distributed Cardinality Estimation: Random Arcs Recycled"**, coauthors: M. Kardas, J. Lemiesz, ANALCO 2015, Proceedings of the Twelfth Workshop on Analytic Algorithmics and Combinatorics, SIAM, 129–137, ISBN 978-1-61197-376-1

[155] **"Tracing Attacks on U-Prove with Revocation Mechanism"**, coauthors: L. Hanzlik, P. Kubiak, ASIACCS 2015, ACM Press, pp. 603-608, ISBN: 978-1-4503-3245-3

[156] **"Hard Invalidation of Electronic Signatures"**, coauthors: L. Hanzlik, M. Yung, ISPEC 2015, Lecture Notes in Computer Science 9065, pp. 421-436

[157] **"Restricted Identification Secure in the Extended Canetti-Krawczyk Model"**, coauthor L. Hanzlik, Journal of Universal Computer Science 21(3), 2015, pp. 419-439

[158] **"Anonymous Evaluation System"**, coauthors: L. Hanzlik, K. Kluczniak, P. Kubiak NSS'2015, Lecture Notes in Computer Science 9408, pp. 283–299

[159] **"Insecurity of Anonymous Login with German Personal Identity Cards"**, coauthors: L. Hanzlik, K. Kluczniak, Security and Privacy in Social Networks and Big Data (SocialSec) 2015, DOI: 10.1109/SocialSec2015.12, IEEE Conference Publications, pp. 39-43

[160] **"A New Secure Data Deduplication Approach Supporting User Traceability"**, coauthors: Jianfeng Wang, Xiaofeng Chen, Jin Li, Kamil Kluczniak, 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA) 2015, IEEE Computer Society, pp. 120-124

[160A] **"TrDup: Enhancing Secure Data Deduplication with User Traceability in Cloud Computing"**, coauthors: Jianfeng Wang, Xiaofeng Chen, Jin Li, Kamil Kluczniak, extended journal version of [160], International Journal of Web and Grid Services, 13(3): 270-289 (2017)

[161] **"Ad-Hoc-Domain Signatures for Personal eID Documents"**, coauthors: Kamil Kluczniak, Lucjan Hanzlik, presented at ARTICCRYPT 2016

[162] **"Pseudonymous Signature on eIDAS Token – Implementation Based Privacy Threats"**, coauthors: Kamil Kluczniak, Lucjan Hanzlik, ACISP'2016, Lecture Notes in Computer Science 9723, 467–477

[163] **"Pseudonymous Identification for Embedded Devices"**, coauthors: Kamil Kluczniak, Lucjan Hanzlik, 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), Conference Publications, ISBN 978-1-5090-0706-6/16, 90-93

[164] **"Chip Authentication for E-Passports: PACE with Chip Authentication Mapping v2"**, coauthors: Lucjan Hanzlik, ISC 2016, Lecture Notes in Computer Science 9866, 1â15

[165] **"Local Self-Organization with Strong Privacy Protection"**, coauthors: Lucjan Hanzlik, Kamil Kluczniak, Shlomi Dolev, IEEE TRUSTCOM'2016, ISBN 978-1-5090-3205-1, 775-782

[166] **"Multi-Device Anonymous Authentication"**, coauthors: Jianfeng Wang, Xiaofeng Chen, Kamil Kluczniak, NSS'2016, Lecture Notes in Computer Science 9955, 21-36

[166A] **"Multi-Device Anonymous Authentication"**, coauthors: Jianfeng Wang, Xiaofeng Chen, Kamil Kluczniak, journal version of [166], . Int. J. Inf. Sec. 18(2): 181-197 (2019)

[167] **"Controlled Randomness - A Defense against Backdoors in Cryptographic Devices"**, coauthors: Lucjan Hanzlik, Kamil Kluczniak MYCRYPT-Paradigm-shifting Crypto '2016, Lecture Notes in Computer Science 10311, 252-274

[168] **"A Formal Concept of Domain Pseudonymous Signatures"**, coauthors: Kamil Kluczniak, Lucjan Hanzlik, ISPEC'2016, Lecture Notes in Computer Science 10060, 238-254

[169] **"Ghost Train for Anonymous Communication"**, coauthors: Przemysław Bła śkiewicz, Mirosław Kutyłowski, Jakub Lemiesz, Małgorzata Sulkowska, SPACCS'2016, Lecture Notes in Computer Science 10066, 224-239

[170] **"Protecting Electronic Signatures in Case of Key Leakage"**, coauthors: Jacek Cichoń, Lucjan Hanzlik, Kamil Kluczniak, Chen Xiaofeng, Wang Jianfeng MYCRYPT-Paradigm-shifting Crypto '2016, Lecture Notes in Computer Science 10311, 215-232

[171] **"Security of Okamoto Identification Scheme in Practice - a Defense against Ephemeral Key Leakage and Setup"**, coauthors: Ł. Krzywiecki, Proc. 5th ACM Int. Workshop on Security in Cloud Computing, SCC@AsiaCCS 2017, 43–50

[172] **"Brief Announcement: Anonymous Credentials Secure to Ephemeral Leakage"**, coauthors: Ł. Krzywiecki, M. Wszoła, Cyber Security Cryptography and Machine Learning, CSCML Lecture Notes in Computer Science 10332, 96-98

[173] **"Braid Chain Radio Communication"**, coauthors: J.Cichoń, K. Wolny, ALGOSENSORS'2017, Lecture Notes in Computer Science 10718, 223-235

[174] **"Pseudonymous Signature Schemes"**, coauthors: Przemysław Blaśkiewicz, Lucjan Hanzlik, Kamil Kluczniak, Łukasz Krzywiecki, Marcin Słowik, Marta Wszoła, in: Advances in Cyber Security: Principles, Techniques, and Applications, eds.: Kuan-Ching Li, Xiaofeng Chen, Willy Susilo, Springer, 2019, 185-255

[175] **"CTRL-PACE: Controlled Randomness for e-Passport Password Authentication"**, coauthors: Kamil Kluczniak,Lucjan Hanzlik, Fundamenta Informaticae, 69 (2019) 295â330

[176] **"Privacy-Aware Identity Management"**, coauthor Przemysław Błaśkiewicz, Encyclopedia of Big Data Technologies 2019, eds.: Sherif Sakr, Albert Y. Zomaya, Springer, Cham, DOI https://doi.org/10.1007/978-3-319-63962-8

[177] **"Emerging Security Challenges for Ubiquitous Devices"**, coauthors: Piotr Syga, Moti Yung, accepted for publication in Security of Ubiquitous Computing Systems Selected Topics, COST Action IC1403, CRYPTACUS, Springer-Verlag

[178] **"E-Passport and E-ID Technologies"**, coauthor Lucjan Hanzlik, accepted for publication in Security of Ubiquitous Computing Systems Selected Topics, COST Action IC1403, CRYPTACUS, Springer-Verlag

[179] **"Rethinking Identification Protocols from the Point of View of the GDPR"**, coauthors: Łukasz Krzywiecki, Xiaofeng Chen, 3rd International Symposium on Cyber Security Cryptology and Machine Learning (CSCML 2019), Lecture Notes in Computer Science 11527, 296–315

[180] **"Anonymous Deniable Identification in Ephemeral Setup & Leakage Scenarios"**, coauthors: Łukasz Krzywiecki, Jakub Pezda, Marcin Słowik, 3rd International Symposium on Cyber Security Cryptology and Machine Learning (CSCML 2019), Lecture Notes in Computer Science 11527, 320-323

[181] **"Privacy and Security Analysis of PACE GM Protocol"**, coauthor Przemysław Kubiak, SECSOC 2019, IEEE Computer Society, TrustCom/BigData 2019 Proceedings, pp. 763-768.

[182] **"Revised Gateway Selection for LoRa Radio Networks"**, coauthors: Przemysław Błaśkiewicz, Jacek Cichoń, Marcin Zawada, AdHocNow'2019, Lecture Notes in Computer Science 11803, pp. 228–240

[183] **"GDPR-Compliant Reputation System Based on Self-Certifying Domain Signatures"**, coauthors: Jakub Lemiesz, Marta Słowik, Marcin Słowik, Kamil Kluczniak, Maciej Gebala, ISPEC'2019, Lecture Notes in Computer Science 11879, 341-361

[184] **"Derandomized PACE with Mutual Authentication"**, coauthor Adam Bobowski, NSS'2019, Lecture Notes in Computer Science 11928, 697-705

[185] **"GDPR - Challenges for Reconciling Legal Rules with Technical Reality"**, coauthor Anna Lauks-Dutka, Moti Yung ESORICS'2020, Lecture Notes in Computer Science 12308, 736-755

[186] **"Preventing a Fork in a Blockchain – David fighting Goliath"**, coauthor Przemysław Kubiak, TRUSTCOM 2020, IEEE Computer Society, TrustCom/BigData 2020 Proceedings, 1044-1051

[187] **"Hierarchical Ring Signatures Immune to Randomness Injection Attacks "**, coauthors: Łukasz Krzywiecki, Rafał Rothenberger, Bartosz Drzazga CSCML'21, Lecture Notes in Computer Science 12716, 171–186

[188] **"Extensions for Apple-Google Exposure Notification Mechanism"**, coauthors: Adam Bobowski, Jacek Cichoń, Bulletin of Polish Academy of Sciences, Technical Sciences, vol. 69, issue 4, 2021

[189] **"Poster: eID in Europe - Password Authentication Revisited"**, coauthors: Patryk Kozieł, Przemysław Kubiak, Yanmei Cao, IFIP-Networking'21, DOI: 10.23919/IFIP-Networking52078.2021.9472856

[190] **"Fair Mutual Authentication"**, coauthors: Jacek Cichoń, Krzysztof Majcher, Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, SCITEPRESS, 754–759

[191] **"PACE with Mutual Authentication â towards an upgraded eID in Europe"**, coauthors: Patryk Kozieł, Przemysław Kubiak, ESORICS'21, Lecture Notes in Computer Science 12973, 501-519

[192] **"The Last Line of Defence in Case of Signing Key Compromise"**, coauthors: Przemysław Błaśkiewicz, Marcin Słowik, ESORICS'21 (poster track)

EDITOR OF SPECIAL ISSUES

[1] **Cyber security, crime, and forensics of wireless networks and applications.** Xiuzhen Cheng, Mirosław Kutyłowski, Kuai Xu, Haojin Zhu: Security and Communication Networks 9(16): 3763-3764 (2016)

[2] **Security and privacy in social networks**, Yang Xiang, Elisa Bertino, Mirosław Kutyłowski, Concurrency and Computation: Practice and Experience 29(7) (2017)

[3] **Social network security and privacy.** Mirosław Kutyłowski, Yu Wang, Shouhuai Xu, Laurence T. Yang, Concurrency and Computation: Practice and Experience 30(5) (2018)

LAW and SOCIAL SCIENCES

[1] **Koncepcje uregulowań prawnych dotyczących bezpieczeństwa technicznego banków elektronicznych a polski stan prawny**, Prawo Mediów Elektronicznych, Dodatek do Monitora Prawniczego nr 12/2005

[2] **Prawne aspekty wykorzystania technologii cyfrowych w komunikacji urząd - obywatel** coauthor D. Adamski, Kwartalnik Prawa Publicznego nr 1-2/2005

[3] **Terminologia ustawy o informatyzacji - niespójności ciąg dalszy**, coauthor D. Adamski, Prawo Mediów Elektronicznych, Dodatek do Monitora Prawniczego nr 2/2006

[4] **Krytyczny komentarz do ustawy o informatyzacji**, coauthor D. Adamski, E-administracja, 1(2), 2006, 45-58

[5] **Wnoszenie do sądu pism procesowych w postaci elektronicznej**, coauthor S. Kotecka, Prawo Mediów Elektronicznych, Dodatek do Monitora Prawniczego

[6] **Podpis elektroniczny osoby prawnej w Republice Czeskiej. Koncepcja prawna, technologiczna i zastosowania gospodarcze**, Wydawnictwo Zakamycze, 2006, ISBN 83-7444-244-1, 195-204

[7] **Sąd nad e-sądem gospodarczym**, coauthor S. Kotecka, Prawo Teleinformatyczne, 1, 2006, 52-57

[9] **Why Digital Signatures Fail - Legal Concepts for Long Term Validity**, coauthors: Dariusz Adamski, Anna Lauks, in *Long Term and Dynamical Aspects of Information Security*, 113-124, ed.: Andreas Schmidt, Michael Kreutzer, Rafael Accorsi, Nova Science Publishers, New York 2008, ISBN 1-60021-912-8

[10] **Archiwizacja dokumentów elektronicznych**, coauthor Sylwia Kotecka, Prawo Nowych Technologii, 2008

[11] **E-voting, głosowanie elektroniczne**, INFOS 10/57, Biuro Analiz Sejmowych, 2009

[12] **Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society**, Baer, Walter S., Borisov, Nikita, Danezis, George, Guerses, Seda F., Klonowski, Marek, Kutyłowski, Mirosław, Maier-Rabler, Ursula, Moran, Tal, Pfitzmann, Andreas, Preneel, Bart, Sadeghi, Ahmad-Reza, Vedel, Thierry, Westen, Tracy, Zagórski, Filip and Dutton, William H., Social Science Research Network, 1521222, 2009, `http://ssrn.com/abstract=1521222`

[13] **Perspektywy rozwoju publicznych systemów elektronicznej identyfikacji** , coauthor Anna Lauks, *Informatyzacja postępowania sądowego i administracji publicznej*, C.H. Beck, 2010, ISBN: 9788325513962

[14] **Polish Concepts for Securing E-Government Document Flow**, coauthor Przemysław Kubiak, ISSE 2010 (Information Security Solutions Europe)

[15] **Elektroniczne postępowanie upominawcze : komentarz**, ed. Jacek Gołaczyński. Warszawa ; Kraków : Wolters Kluwer Polska, 2010, some sections

[16] **Democracy in a Network Society. Dagstuhl Manifesto**, Informatik Spektrum, 3, 2011, 326–329

[17] **Challenges for electronic identity documents**, coauthor Anna Lauks-Dutka, Lecture Notes in Business Information Processing 97, Springer 2011, 256-257

[18] **Nowe perspektywy prawa do prywatności**, X-lecie : księga pamiątkowa z okazji dziesięciolecia CBKE, eds. Ewa Galewska, Sylwia Kotecka. Wrocław : Oficyna Prawnicza, 2012. 137-146.

[19] **Ochrona bezpieczeństwa danych - granice wykorzystania podpisu elektronicznego**, Czas Informacji, 1/2, 2010,

[20] **Kryptograficzne funkcje skrótu - rzut oka na sytuację**, coauthor Krystian Matusiewicz, Czas Informacji, 2/3, 2010,

[21] **Prawo zamówień publicznych w Chinach**, coauthor Yifan Liu, Czas Informacji, 3/4, 2010,

[22] **Pieczęć elektroniczna**, Czas Informacji, 4/5, 2010,

[23] **E-dowód osobisty - projekt zmian w ustawie o dowodzie osobistym**, Czas Informacji, 2/7, 2011,