January 1, 2024

# Curriculum Vitae

**Stanisław Paweł Radziszowski**

Professor, Department of Computer Science
Rochester Institute of Technology
Rochester, NY 14623, USA
(585) 4755193 - office, 3590245 - home
http://www.cs.rit.edu/~spr, spr@cs.rit.edu
born June 7, 1953, in Gdańsk, Poland
US permanent resident

## Education

M.S. degree in theoretical computer science at the University of Warsaw, Poland, April 1976. M.S. thesis - *"Programmability and P=?NP Conjecture"* [1][2], advised by Antoni Kreczmar.

Ph.D. degree obtained in March 1980 in the Institute of Informatics at the University of Warsaw. Ph.D. thesis - *"Logic and Complexity of Synchronous Parallel Computations"* [3][4], advised by Antoni Kreczmar and Andrzej Salwicki.

## Professional Experience, Teaching

From 1976 to 1980 worked as an Assistant Professor at the Institute of Informatics, Faculty of Mathematics, Informatics and Mechanics of the University of Warsaw.

In the period 1980-1984 worked as a Visiting Professor at universities of Mexico City, initially at the Research Institute of Applied Mathematics and System Sciences (IIMAS) of the National University (UNAM), since 1983 also in the Department of Mathematics in the Autonomous Metropolitan University (UAM).

From October 1984 worked as an Assistant Professor in the School of Computer Science and Technology at the Rochester Institute of Technology, NY. In September 1988 promoted to the rank of Associate Professor. Tenure granted in February 1990. In September 1995 promoted to the rank of Full Professor. Since 1997 Fellow of the Institute of Combinatorics and Its Applications.

Extensive experience in teaching a variety of courses, mostly in theoretical computer science, on applications of computer science in mathematics, cryptography, and on algorithms in various domains.

## Research and Teaching Areas

- computational combinatorics, computational Ramsey theory
- applied cryptography, computations in number theory
- theory and practice of graphs, complexity theory

The specific problems of particular interest are algorithms for hard problems like: Ramsey numbers, $t$-designs, knapsack, arithmetic of large integers, tests for primality, factoring into primes and other combinatorial problems in graph theory. The general problems of particular interest are in the complexity of algorithms and related areas, such as $P=NP$ conjecture. I was fortunate to obtain some interesting results in computational discrete mathematics. CPU intensive computations were an essential tool and an object of study for most of the results pointed to below.

- 1986, the discovery of the first simple $6-(14,7,4)$ design, the smallest possible 6-design, jointly with Don Kreher [8][17].
- 1990, the computation of the first classical Ramsey number for hypergraphs $R(4,4;3)=13$, jointly with Brendan McKay [25].
- 1993, 1995, the computation of the classical Ramsey number for graphs $R(4,5)=25$ [32], and the upper bound $R(5,5)\leq 49$ [35], jointly with Brendan McKay.
- 1995, computational proof of the nonexistence of $4-(12,6,6)$ designs, answering the last open existence question in design theory for at most 12 points, jointly with Brendan McKay [33].
- 1998, the computation of the smallest unknown Folkman number $F(3,3;5) = 15$ [38], jointly with Konrad Piwakowski and Sebastian Urbański.
- 2001, upper bound for the four color Ramsey number $R_4(3) \leq 62$ [43], jointly with Susan Fettes and Richard Kramer.
- 2004, general and computational constructive lower bounds for classical two-color [45] and multicolor [47] Ramsey numbers, jointly with Xu Xiaodong, Xie Zheng and Geoffrey Exoo.
- 2006, nonexistence of $2-(22,8,4)$ BIBD designs, answering the smallest open parameters existence question [51], jointly with Richard Bilous, Clement W. H. Lam, Larry H. Thiel, (Ben) P. C. Li, G. H. John van Rees, Wolfgang Holzmann and Hadi Kharaghani.
- 2009, 2011, progress on graph reconsruction conjecture for vertex and edge deleted cards, existential and universal reconstruction numbers, jointly with David Rivshin [59][67].
- 2011, 2013, more constructive lower bounds for classical Ramsey numbers [68] and their relation to Shannon capacity of noisy channels [75], jointly with Xu Xiaodong.
- 2013, 2016, progress on bounds for Ramsey numbers $R(3,\,k)$ [74][91] and $R(3,\,K_k-e)$ [78], jointly with Jan Goedgebeur and Xiaodong Xu.
- 2022, on Folkman $(K_4-e)$-free graphs and their chromatic number [112], jointly with Zohair Hassan, Yu Jiang, David Narváez and Xiaodong Xu.

**Dynamic Survey of Ramsey Numbers**

I am the author and a maintainer of the survey paper "*Small Ramsey Numbers*" [31], whose 16 revisions appeared in the *Electronic Journal of Combinatorics*, 1994-2021. It is a dynamic survey of my main area of interest, updated periodically as a living article at **http://www.combinatorics.org**.

**External Research Grants**

1. *"Improvements and Applications of the Lenstra, Lenstra, Lovász Basis Reduction Algorithm"* (with D.L. Kreher), from the National Science Foundation, DCR-8606378, 1986.
2. *"Computing Combinatorial Configurations: t-designs and Ramsey Numbers"* (with D.L. Kreher), from the National Science Foundation, CCR-8711229, 1987-1988.
3. *"Computer Search for Elusive Combinatorial Configurations: A Research Toolchest"* (with D.L. Kreher), from the National Science Foundation, CCR-8920692, 1990-1991.
4. *"Innovative Searches for Ramsey Graphs and Other Extremal Combinatorial Configurations"*, from the National Security Agency, MDA904-94-H-2009, 1994-1996.
5. *"Multi-Cast Key Management"* (with A. Kaminsky and M. Łukowiak), from Harris RF Communications Division, 2011-2013.
6. *"Authenticated Encryption"* (with A. Kaminsky, M. Łukowiak and P. Bajorski), from Harris RF Communications Division, 2014-2015, 2016-2017.
7. *"Cross Domain Solutions Using Homomorphic/Functional Cryptography"* (with A. Kaminsky, M. Łukowiak and P. Bajorski), from Harris RF Communications Division, 2018-2019.
8. *"Obfuscation for Securing IP on FPGAs"* (with M. Łukowiak and P. Bajorski), from L3Harris Technologies, 2020-2021.

9. *"Cross Domain Solutions Using Homomorphic/Functional Cryptography", "Soldier Systems Security Architecture"* (two projects with M. Łukowiak and P. Bajorski), from L3Harris Technologies, 2021-2023.

**External Educational Grants**

1. *"REU Site: Extremal Graph Theory and Dynamical Systems at RIT"* (with D. Narayan/PI, W. Basener and T. Wiandt), from the National Science Foundation, DMS-0552418, 2007-2010.
2. *"Multi-disciplinary Applied Cryptography"* (with M. Łukowiak/PI and J. Vallino), CCLI grant from the National Science Foundation, DUE-0837656, 2009-2012.
3. *"REU Site: Extremal Graph Theory and Dynamical Systems at RIT"* (with D. Narayan/PI, A. Agarwal, B. Brooks, J. Jacob and T. Wiandt), from the National Science Foundation, DMS-1062128, 2011-2013.
4. *"REU Site: Extremal Graph Theory and Dynamical Systems at RIT"* (with D. Narayan/PI, E. Cherry, T. Harkin, J. Jacob, P. Wenger and T. Wiandt), from the National Science Foundation, DMS-1358583, 2014-2017, and DMS-1659075, 2017-2020.
5. *"REU Site: Extremal Graph Theory and Dynamical Systems at RIT"* (with D. Narayan/PI, J. Jacob, N. Malik and L. Munoz), from the National Science Foundation, DMS for 2020-2023.

**Internal RIT Grants**

1. *"Automating Reasonings about Graph Colorings"*, Faculty Development Grant FEAD, 2000.
2. *"Graph Coloring Algorithms and their Implementations"*, FEAD Grant, 2001.
3. *"Constructive Design Theory: Quest for the 2-(22,8,4) Designs"*, FEAD Grant, 2002/3.
4. *"Enhancing Cryptography Expertise"*, FEAD Grant, 2003/4.
5. *"Computational Ramsey Theory"*, FEAD Grant, 2004/5.
6. *"Computational Study of Ramsey Arrowing"*, GCCIS Seed Funding, 2012, 2013 and 2016.
7. *"Secure Distributed Homomorphic Encryption"* (with Peizhao Hu), GCCIS Seed Funding, 2015.
8. *"Privacy-Preserving for the Connected World"* (lead of 6-person group), SIRA Project, 2016-2018.
9. *"Ramsey Colorings and Constraint Satisfaction Problems"*, GCCIS Seed Funding, 2018.

**Patents**

Four patents resulting from joint projects with the L3/Harris RF Communications Division:

1. *Electronic key management using PKI to support group key establishment in the tactical environment* (October 2014, no. 8,873,759).
2. *Customizable encryption algorithm based on a sponge construction with authenticated and non-authenticated modes of operation* (September 2016, no. 9,438,416).
3. *Customizable encryption/decryption algorithm* (May 2020, no. 10,666,437).
4. *Cross-domain information transfer system and associated methods* (January 2021, no. 11,115,395).

**Advising**

I was the main advisor for 81 MS students (mainly CS, 37 theses and 44 projects), and I was a member of 12 Ph.D. committees. The publications listed below at positions 16, 24, 27, 30, 41-43, 46, 49, 50, 52, 58-60, 63, 64, 66, 67, 69, 72, 76, 77, 80, 81, 85, 86, 89, 90, 92, 93, 95, 101-103, 105, 106 and 108 were the result of joint work with RIT CS/CE/Math students. I was a mentor for NSF-REU Mathematics programs during most summers of 2007-2020 (10 out of 15), which resulted in publications at positions 65, 70, 73, 94 and 100.

**List of Publications (in chronological order of writing)**

1. "Programmability and $P = NP$ Conjecture", in *Proceedings of Foundamentals of Computation Theory*, Poznań-Kórnik 1977, LNCS 56, Berlin, Springer-Verlag, (1977) 494-498.
2. "Programmability and $P = NP$ Conjecture", *Fundamenta Informaticae IV*, 2 (1978/79) 71-82.

3. "Logic and Complexity of Synchronous Parallel Computations", in *Proceedings of Mathematical Logic in Computer Science*, Colloquia Mathematica Societatis János Bolyai 26, Salgótarján, Hungary (1978), North-Holland, (1981) 675-697.

4.+ "Logic and Complexity of Synchronous Parallel Computations",
a) Ph.D. thesis (in Polish), University of Warsaw, 1980,
b) English version appeared in the CCPAS-report no. 353, Warsaw, 1980.

5. "Bounded Alternation", *IIMAS CT 242, Universidad Nacional Autónoma de México*, 1980.

6. "Desarollo de la teoria de los algoritmos en paralelo y su aplicación para evaluación en la máquina AHR" (in Spanish), [Theory of Parallel Algorithms and its Applications for the AHR Machine], *IIMAS CT 347, Universidad Nacional Autónoma de México*, México D.F., 1983.

7. "Aritmética en Precisión Múltiple para la Máquina FOONLY-F2" (in Spanish), [Multiple Precision Integer Arithmetic for the Computer FOONLY-F2], *IIMAS CT Mon. 76, Universidad Nacional Autónoma de México*, México D.F., 1983.

8. "The Existence of Simple 6-(14,7,4) Designs" (with D.L. Kreher), *Journal of Combinatorial Theory, Series A*, 43 (1986) 237-243.

9. "Finding Simple $t$–Designs by Using Basis Reduction" (with D.L. Kreher), in *Proceedings of the 17-th Southeastern International Conference on Combinatorics, Graph Theory, and Computing*, Utilitas Mathematica, Winnipeg, Canada, *Congressus Numerantium*, 55 (1986) 235-244.

10. "Simple 5-(28,6,$\lambda$) Designs from $PSL_2(27)$" (with D.L. Kreher), *Annals of Discrete Mathematics 34*, special volume on Combinatorial Design Theory dedicated to Alexander Rosa (edited by C.J. Colbourn and R.A. Mathon), North-Holland Mathematics Studies, 149 (1987) 315-318.

11. "New $t$–Designs Found by Basis Reduction" (with D.L. Kreher), in *Proceedings of the 18-th Southeastern International Conference on Combinatorics, Graph Theory, and Computing*, Utilitas Mathematica, Winnipeg, Canada, *Congressus Numerantium*, 59 (1987) 155-164.

12. "Solving Subset Sum Problem with the $L^3$ algorithm" (with D.L. Kreher), *Journal of Combinatorial Mathematics and Combinatorial Computing*, 3 (1988) 49-63.

13. "Search Algorithm for Ramsey Graphs by Union of Group Orbits" (with D.L. Kreher), *Journal of Graph Theory*, 12(1) (1988) 59-72.

14. "On $R(3, k)$ Ramsey Graphs: Theoretical and Computational Results" (with D.L. Kreher), *Journal of Combinatorial Mathematics and Combinatorial Computing*, 4 (1988) 37-52.

15. "Upper Bounds for Some Ramsey Numbers $R(3, k)$" (with D.L. Kreher), *Journal of Combinatorial Mathematics and Combinatorial Computing*, 4 (1988) 207-212.

16. "Lower Bounds for Multi-Colored Ramsey Numbers from Group Orbits" (with D.L. Kreher and Wei Li), *Journal of Combinatorial Mathematics and Combinatorial Computing*, 4 (1988) 87-96.

17. "Constructing 6-(14,7,4) Designs" (with D.L. Kreher), in *Contemporary Mathematics*, AMS, 111 (1990) 137-151.

18. "Minimum Triangle-Free Graphs" (with D.L. Kreher), *Ars Combinatoria*, 31 (1991) 65-92.

19. "On the Covering of $t$-sets with $(t+1)$-sets: $C(9, 5, 4)$ and $C(10, 6, 5)$" (with D. de Caen, D.L. Kreher and W.H. Mills), *Discrete Mathematics*, 92 (1991) 65-77.

20. "On the Ramsey Number $R(K_5-e, K_5-e)$", *Ars Combinatoria*, 36 (1993) 225-232.

21. "The Parameters 4-(12,6,6) and Related $t$–Designs" (with D.L. Kreher, D. de Caen, S.A. Hobart and E.S. Kramer), *Australasian Journal of Combinatorics*, 7 (1993) 3-20.

22. "The Ramsey Numbers $R(K_3, K_8-e)$ and $R(K_3, K_9-e)$", *Journal of Combinatorial Mathematics and Combinatorial Computing*, 8 (1990) 137-145.

23. "Enumeration of All Simple $t-(t+7, t+1, 2)$ Designs", *Journal of Combinatorial Mathematics and Combinatorial Computing*, 12 (1992) 175-178.

---

+ more than one version was published

24. "The Number of Edges in Minimum ($K_3$, $K_p - e$, $n$) Graphs" (with Jing Zou), in *Proceedings of the 21-st Southeastern International Conference on Combinatorics, Graph Theory, and Computing,* Utilitas Mathematica, Winnipeg, Canada, *Congressus Numerantium,* 78 (1990) 153-165.

25. "The First Classical Ramsey Number for Hypergraphs Is Computed" (with B.D. McKay), in *Proceedings of the Second Annual ACM-SIAM Symposium on Discrete Algorithms,* SODA'91, San Francisco CA, (1991) 304-308.

26. "A New Upper Bound for the Ramsey Number $R(5,5)$" (with B.D. McKay), *Australasian Journal of Combinatorics,* 5 (1992) 13-20.

27. "The Ramsey Numbers $R(K_4-e, K_6-e)$ and $R(K_4-e, K_7-e)$" (with J. McNamara), in *Proceedings of the 22-nd Southeastern International Conference on Combinatorics, Graph Theory, and Computing,* Utilitas Mathematica, Winnipeg, Canada, *Congressus Numerantium,* 81 (1991) 89-96.

28. "On $(n,5,3)$-Turán Systems" (with E.D. Boyer, D.L. Kreher and A.F. Sidorenko), *Ars Combinatoria,* 37 (1994) 13-31.

29. "Linear Programming in Some Ramsey Problems" (with B.D. McKay), *Journal of Combinatorial Theory, Series B,* 61 (1994) 125-132.

30.+ "Paths, Cycles and Wheels in Graphs without Antitriangles" (with Jin Xia), *Australasian Journal of Combinatorics,* 9 (1994) 221-232. Preliminary version appeared as RIT Technical Report, Department of Computer Science, RIT-TR-92-008, 1992.

31.+ "Small Ramsey Numbers", *Electronic Journal of Combinatorics, Dynamic Survey* DS1, revision #16, 116 pages (2021), http://www.combinatorics.org/, revisions #1 through #15, 1994-2017. Preliminary version appeared as RIT Technical Report, Department of Computer Science, RIT-TR-93-009, 1993.

32. "$R(4,5)=25$" (with B.D. McKay), *Journal of Graph Theory,* 19(3) (1995) 309-322.

33. "The Nonexistence of 4–(12, 6, 6) Designs" (with B.D. McKay), in *Computational and Constructive Design Theory,* (edited by W.D. Wallis), Mathematics and its Applications 368, Kluwer Academic Publishers, 1996, 177-188.

34. "Towards Deciding the Existence of 2–(22, 8, 4) Designs" (with B.D. McKay), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 22 (1996) 211-222.

35. "Subgraph Counting Identities and Ramsey Numbers" (with B.D. McKay), *Journal of Combinatorial Theory, Series B,* 69(2) (1997) 193-209.

36. "$30 \le R(3,3,4) \le 31$" (with K. Piwakowski), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 27 (1998) 135-141.

37. "2–(22, 8, 4) Designs Have No Blocks of Type 3" (with B.D. McKay), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 30 (1999) 251-253.

38. "Computation of the Folkman Number $F_e(3,3;5)$" (with K. Piwakowski and S. Urbański), *Journal of Graph Theory,* 32 (1999) 41-49.

39. "Ramsey Numbers for Triangles versus Almost-Complete Graphs" (with B.D. McKay and K. Piwakowski), *Ars Combinatoria,* LXXIII (2004) 205-214.

40.+ "The Ramsey Multiplicity of $K_4$" (with K. Piwakowski), *Ars Combinatoria.* LX (2001) 131-136. Preliminary version "Computation of the Ramsey Multiplicity of $K_4$" appeared in the *Proceedings of the Workshop on Computational Graph Theory and Combinatorics,* Victoria, British Columbia (1999) 28-30.

41. "On Halving Line Arrangements" (with A. Beygelzimer), *Discrete Mathematics,* special issue "Kleitman and Combinatorics: A Celebration", 257 (2002) 267-283.

42. "A Computational Approach for the Ramsey Numbers $R(C_4, K_n)$" (with Kung-Kuen Tse), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 42 (2002) 195-207.

43. "An Upper Bound of 62 on the Classical Ramsey Number $R(3,3,3,3)$" (with S. Fettes and R. Kramer), *Ars Combinatoria,* LXXII (2004) 41-63.

44. "Towards the Exact Value of the Ramsey Number $R(3,3,4)$" (with K. Piwakowski), *Proc. of the 33-rd Southeastern International Conference on Combinatorics, Graph Theory, and Computing*, Utilitas Mathematica, Winnipeg, Canada, *Congressus Numerantium*, 148 (2001) 161-167.

45. "A Constructive Approach for the Lower Bounds on the Ramsey Numbers $R(s, t)$" (with Xu Xiaodong and Xie Zheng), *Journal of Graph Theory*, 47 (2004) 231-239.

46. "Computation of the Ramsey Number $R(B_3, K_5)$" (with A. Babak and Kung-Kuen Tse), *Bulletin of the Institute of Combinatorics and Its Applications*, 41 (2004) 71-76.

47. "Constructive Lower Bounds on Classical Multicolor Ramsey Numbers" (with Xu Xiaodong, Xie Zheng and G. Exoo), *Electronic Journal of Combinatorics*, 11 (2004) #R35, 24 pages, http://www.combinatorics.org/.

48.+ "Complexity Results in Graph Reconstruction" (with Edith Hemaspaandra, Lane Hemaspaandra and Rahul Tripathi), *Discrete Applied Mathematics*, 152(2) (2007) 103-118. Preliminary version in the Proceedings of the 29-th International Symposium on Mathematical Foundations of Computer Science, MFCS Prague 2004, LNCS 3153, 287-297. Also, Technical Report 852, Department of Computer Science, University of Rochester, October 2004, 27 pages.

49. "Computation of the Ramsey Number $R(W_5, K_5)$" (with Joshua Stinehour and Kung-Kuen Tse), *Bulletin of the Institute of Combinatorics and Its Applications*, 47 (2006) 53-57.

50. "Computing the Folkman Number $F_v(2,2,3;4)$" (with Jonathan Coles), *Journal of Combinatorial Mathematics and Combinatorial Computing*, 58 (2006) 13-22.

51. "There is no $(22,8,4)$ Block Design" (with R. Bilous, C. W. H. Lam, L. H. Thiel, P. C. Li, G. H. J. van Rees, W. Holzmann and H. Kharaghani), *J of Combinatorial Designs*, 15 (2007) 262-267.

52. "Graph Reconstruction Numbers" (with Brian McMullen), *Journal of Combinatorial Mathematics and Combinatorial Computing*, 62 (2007) 85-96. Errata in 63 (2007) 93-95.

53. "On the Most Wanted Folkman Graph" (with Xu Xiaodong), *Geombinatorics*, XVI (4) (2007) 367-381. Substantial citations in *The Mathematical Coloring Book* by A. Soifer, Springer 2009.

54. "$28 \le R(C_4, C_4, C_3, C_3) \le 36$" (with Xu Xiaodong), *Utilitas Mathematica*, 79 (2009) 253-257.

55. "A Case for a Parallelizable Hash" (with Alan Kaminsky), in *Proceedings of MILCOM'2008*, San Diego CA, November 2008.

56. "Bounds on Some Ramsey Numbers Involving Quadrilateral" (with Xiaodong Xu and Zehui Shao), *Ars Combinatoria*, 90 (2009) 337-344.

57. "An Improvement to Mathon's Cyclotomic Ramsey Colorings" (with Xiaodong Xu), *Electronic Journal of Combinatorics*, 16(1) (2009) #N1, 5 pages, http://www.combinatorics.org/.

58. "NTRU-Based Sensor Network Security: a low-power hardware implementation perspective" (with Fei Hu, Kyle Wilhelm, Michael Schab, Marcin Łukowiak, and Yang Xiao), *Security and Communication Networks*, 2 (2009) 71-81.

59. "Vertex and Edge Graph Reconstruction Numbers of Small Graphs" (with David Rivshin), *Australasian Journal of Combinatorics*, 45 (2009) 175-188.

60.+ "Scalable FPGA Design and Performance Analysis of PHASH Hashing Function" (with Przemysław Zalewski and Marcin Łukowiak), in *Proceedings of the 16-th International Conference Mixed Design of Integrated Circuits and Systems*, June 2009, Łódź, Poland. Extended version "Case Study on FPGA Performance of Parallel Hash Functions", *Przeglad Elektrotechniczny/Electrical Review*, ISSN 0033-2097, R86/NR11a (2010) 151-155.

61. "Ramsey Numbers Involving Cycles", a survey in *Ramsey Theory: Yesterday, Today and Tomorrow*, edited by Alexander Soifer, Progress in Mathematics 285, Springer-Birkhauser 2011, 41-62.

62. "An Overview of Cryptanalysis Research of the Advanced Encryption Standard" (with Alan Kaminsky and Michael Kurdziel), in *Proceedings of MILCOM'2010*, San Jose CA, November 2010.

63. "Trustworthy Data Collection from Implantable Medical Devices via High-Speed Security Implementation Based on IEEE 1363" (with Fei Hu, Qi Hao, Marcin Łukowiak, Qingquan Sun, Kyle

Wilhelm and Yao Wu), *IEEE Trans. on Inf. Tech. in Biomedicine,* 14(6) (2010) 1397-1404.

64. "NTRU-based confidential data transmission in telemedicine sensor networks" (with Fei Hu, Xiaojun Cao, Kyle Wilhelm and Marcin Łukowiak), in *Security in Ad Hoc and Sensor Networks,* Singapore World Scientific, 2010, 159-192.
65. "New Bounds on Some Ramsey Numbers" (with Kevin Black and Daniel Leven), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 78 (2011) 213-222.
66. "Computing the Folkman Number $F_v(2,2,2,2,2;4)$" (with Joel Lathrop), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 78 (2011) 119-128.
67. "Multi-Vertex Deletion Graph Reconstruction Numbers" (with David Rivshin), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 78 (2011) 303-321.
68. "More Constructive Lower Bounds on Classical Ramsey Numbers" (with Xiaodong Xu and Zehui Shao), *SIAM Journal on Discrete Mathematics,* 25 (2011) 394-400.
69. "Effects of GPU and CPU Loads on Performance of CUDA Applications" (with Maksim Bobrov, Roy Melton and Marcin Łukowiak), in *Proceedings of International Conference on Parallel and Distributed Processing Techniques and Applications,* PDPTA'11, Las Vegas, NV, July 2011, Vol. II, 575-581.
70. "Computing the Ramsey Number $R(K_5-P_3, K_5)$" (with Jesse Calvert and Michael Schuster), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 82 (2012) 131-140.
71. "Designing a Secure Cloud-Based EHR System Using Ciphertext-Policy Attribute-Based Encryption" (with Suhair Alshehri and Rajendra K. Raj), in *Proceedings of the Data Management in the Cloud Workshop, DMC 2012,* Washington D.C., April 2012.
72. "Developing an Applied, Security-Oriented Computing Curriculum" (with Marcin Łukowiak, Andy Meneely, James Vallino and Christopher Wood), in *Proceedings of the Annual Conference of American Society for Engineering Education, ASEE 2012,* San Antonio TX, June 2012.
73. "On Some Multicolor Ramsey Numbers Involving $K_3+e$ and $K_4+e$" (with Daniel S. Shetler and Michael A. Wurtz), *SIAM Journal on Discrete Mathematics,* 26 (2012) 1256-1264.
74. "New Computational Upper Bounds for Ramsey Numbers $R(3, k)$" (with Jan Goedgebeur), *Electronic Journal of Combinatorics,* 20(1) (2013) #P30, 28 pages, http://www.combinatorics.org/.
75. "Bounds on Shannon Capacity and Ramsey Numbers from Product of Graphs" (with Xiaodong Xu), *IEEE Transactions on Information Theory,* 59(8) (2013) 4767-4770.
76. "Use of MAX-CUT for Ramsey Arrowing of Triangles" (with Alexander Lange and Xiaodong Xu), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 88 (2014) 61-71.
77. "Cybersecurity Education: Bridging the Gap between Hardware and Software Domains" (with Marcin Łukowiak, James Vallino and Christopher Wood), *ACM Transactions on Computing Education,* 14(1) (2014), article #2.
78. "The Ramsey Number $R(3, K_{10}-e)$ and Computational Bounds for $R(3, G)$" (with Jan Goedgebeur), *Electronic Journal of Combinatorics,* 20(4) (2013) #P19, 25 pages, http://www.combinatorics.org/.
79. "On Some Zarankiewicz Numbers and Bipartite Ramsey Numbers for Quadrilateral" (with Janusz Dybizbański and Tomasz Dzido), *Ars Combinatoria,* 119 (2015) 275-287.
80. "Stochastic Analysis and Modeling of a Tree-Based Group Key Distribution Method in Tactical Wireless Networks" (with Peter Bajorski, Alan Kaminsky, Michael Kurdziel, Marcin Łukowiak and Christopher Wood), *Journal of Telecommunications Systems & Management,* 3(2) (2014), 8p.
81. "Computation of the Ramsey Numbers $R(C_4, K_9)$ and $R(C_4, K_{10})$" (with Ivan Livinsky and Alexander Lange), *Journal of Combinatorial Mathematics and Combinatorial Computing,* 97 (2016) 139-154.
82. "Ramsey Numbers of $C_4$ versus Wheels and Stars" (with Wu Yali, Sun Yongqi and Zhang Rui), *Graphs and Combinatorics,* 31(1) (2015) 2437-2446.

83. "Wheel and Star-critical Ramsey Numbers for Quadrilateral" (with Wu Yali and Sun Yongqi), *Discrete Applied Mathematics,* 186 (2015) 260-271.

84.+ "On Some Open Questions for Ramsey and Folkman Numbers" (with Xiaodong Xu), *Graph Theory, Favorite Conjectures and Open Problems,* vol. 1, edited by Ralucca Gera, Stephen Hedetniemi and Craig Larson, Problem Books in Mathematics, Springer 2016, 43-62. Early version, *Institut Mittag-Leffler Technical Report,* 2013/2014 No. 19, spring 2014.

85. "Constructing Large S-Boxes with Area-Minimized Implementations" (with Christopher Wood and Marcin Łukowiak), in *Proceedings of MILCOM'2015,* Tampa, FL, October 2015.

86. "Customizable Sponge-Based Authenticated Encryption Using 16-bit S-boxes" (with Matthew Kelly, Alan Kaminsky, Michael Kurdziel and Marcin Łukowiak, in *Proceedings of MILCOM'2015,* Tampa, FL, October 2015.

87. "On Some Three-Color Ramsey Numbers for Paths" (with Janusz Dybizbański and Tomasz Dzido), *Discrete Applied Mathematics,* 204 (2016) 133-141.

88. "On Bipartization of Cubic Graphs by Removal of an Independent Set" (with Hanna Furmańczyk and Marek Kubale), *Discrete Applied Mathematics,* 209 (2016) 115-121.

89. "Evaluation of Homomorphic Primitives for Computations on Encrypted Data for CPS Systems" (with Peizhao Hu, Tamalika Mukherjee and Alagu Valliappan), in *Proceedings of the IEEE Smart City Security and Privacy,* CPS Week'16 workshop, Vienna, Austria, April 2016.

90. "Homomorphic Proximity Computation in Geosocial Networks" (with Peizhao Hu, Tamalika Mukherjee and Alagu Valliappan), in *Proceedings of the Fourth IEEE International Workshop on Security and Privacy in Big Data,* BigSecurity INFOCOM'16, San Francisco CA, April 2016.

91. "A Small Step Forwards on the Erdős-Sós Problem Concerning the Ramsey Numbers $R(3, k)$" (with Rujie Zhu and Xiaodong Xu), *Discrete Applied Mathematics,* 214 (2016) 216-221.

92. "Effectiveness of Variable Bit-Length Power Analysis Attacks on SHA-3 Based MAC" (with Xuan Tran and Marcin Łukowiak), in *Proceedings of MILCOM'2016,* Baltimore, November 2016.

93. "Implementing Authenticated Encryption Algorithm MK-3 on FPGA" (with Gordon Werner, Steven Farris, Alan Kaminsky, Michael Kurdziel and Marcin Łukowiak), in *Proceedings of MILCOM'2016,* Baltimore MD, November 2016.

94. "Zarankiewicz Numbers and Bipartite Ramsey Numbers" (with Alex Collins, Alexander Riasanovsky and John Wallace), *Journal of Algorithms and Computation,* 47 (2016) 63-78.

95. "Neural Networks and the Search for a Quadratic Residue Detector" (with Michael Potter and Leon Reznik), in *Proceedings of the International Joint Conference on Neural Networks,* Anchorage AK, May 2017.

96. "A Note on Upper Bounds for Some Generalized Folkman Numbers" (with Xiaodong Xu and Meilian Liang), *Discussiones Mathematicae Graph Theory,* 39 (2019) 939-950.

97. Array-Based Statistical Analysis of the MK-3 Authenticated Encryption Scheme" (with Peter Bajorski, Alan Kaminsky, Michael Kurdziel and Marcin Łukowiak), in *Proceedings of MILCOM'2018,* Los Angeles CA, November 2018.

98. "Customization Modes for the Harris MK-3 Authenticated Encryption Algorithm" (with Peter Bajorski, Alan Kaminsky, Michael Kurdziel and Marcin Łukowiak), in *Proceedings of MILCOM'2018,* Los Angeles CA, November 2018.

99. "On the Nonexistence of Some Generalized Folkman Numbers" (with Xiaodong Xu and Meilian Liang), *Graphs and Combinatorics,* 34 (2018) 1101-1110.

100. "On Some Edge Folkman Numbers Large and Small" (with Jenny Kaufmann and Henry Wickus), *Involve, a Journal of Mathematics,* 12 (2019) 813-822.

101. "Flexible HLS-Based Implementation of the Karatsuba Multiplier Targeting Homomorphic Encryption Schemes" (with Michael J. Foster and Marcin Łukowiak), *Proceedings of the 26-th International Conference on Mixed Design of Integrated Circuits and Systems,* MIXDES'2019, 217-222, Rzeszów, Poland, June 2019.

102. "Exploring the Application of Homomorphic Encryption to a Cross Domain Solution" (with Cody Tinker, Kevin Millar, Alan Kaminsky, Michael Kurdziel and Marcin Łukowiak), *Proceedings of MILCOM'2019*, Norfolk, VA, November 2019.
103. "Design of a Flexible Schönhage-Strassen FFT Polynomial Multiplier with High-Level Synthesis to Accelerate HE in the Cloud" (with Kevin Millar and Marcin Łukowiak), *Proceedings of the International Conference on Reconfigurable Computing and FPGAs*, ReConFig'2019, Cancún, México, December 2019.
104. "On a Diagonal Conjecture for Classical Ramsey Numbers" (with Xiaodong Xu and Meilian Liang), *Discrete Applied Mathematics*, 267 (2019) 195-200.
105. "Star-critical Ramsey Numbers for Cycles Versus $K_4$" (with Chula Jayawardene and David Narváez), *Discussiones Mathematicae Graph Theory*, 41 (2021) 381-390.
106. "Failed Power Domination on Graphs" (with Abraham Glasser, Bonnie Jacob and Emily Lederman), *Australasian Journal of Combinatorics*, 76(2) (2020) 232-247.
107. "Chromatic Vertex Folkman Numbers" (with Xiaodong Xu and Meilian Liang), *Electronic Journal of Combinatorics*, 27(3) (2020) #P3.53, 12 pages, http://www.combinatorics.org/.
108. "Hardware Obfuscation of the 16-bit S-box in the MK-3 Cipher" (with Jason Blocklove, Steve Farris, Michael Kurdziel and Marcin Łukowiak), *Proceedings of the 28-th Conference on Mixed Design of Integrated Circuits and Systems*, MIXDES'2021, 104-109, Łódź, Poland, June 2021.
109. "Solving the Cross Domain Problem with Functional Encryption" (with Alan Kaminsky, Michael Kurdziel, Steve Farris and Marcin Łukowiak), *Proceedings of MILCOM'2021*, San Diego CA, November 2021.
110. "Memory Protection with Dynamic Authentication Trees" (with Matthew Millar and Marcin Łukowiak), *Proceedings of the 29-th International Conference on Mixed Design of Integrated Circuits and Systems*, MIXDES'2022, 202-207, Wrocław, Poland, June 2022.
111. "Statistical Analysis of the MK-3 Customizable Authenticated Encryption" (with Peter Bajorski, Alan Kaminsky, Michael Kurdziel and Marcin Łukowiak), *Proceedings of MILCOM'2022*, Bethesda MD, November/December 2022. Extended journal version in preparation.
112. "On Some Generalized Vertex Folkman Numbers" (with Zohair Hassan, Yu Jiang, David Narváez and Xiaodong Xu), *Graphs and Combinatorics*, 39 (2023).
113. "Power Analysis Attacks on the Customizable MK-3 Authenticated Encryption Algorithm" (with Peter Fabinski, Steve Farris, Michael Kurdziel and Marcin Łukowiak), *Proceedings of the 30-th International Conference on Mixed Design of Integrated Circuits and Systems*, MIXDES'2023, Kraków, Poland, June 2023. Extended journal version in preparation.
114. "The Complexity of $(P_k, P_l)$–Arrowing", (with Zohair Raza Hassan and Edith Hemaspaandra), *Proceedings of 24th International Symposium on Fundamentals of Computation Theory*, Trier, Germany, September 18-21, 2023 (best student paper award). Lecture Notes in Computer Science, Springer, 2023. Extended journal version in preparation.

**Forthcoming Publications**

115. "Designing and Delivering a Post-Quantum Cryptography Course" (with T.J. Borrelli and Monika Polak), to appear in *Proceedings of the 55th ACM Symposium on Computer Science Education*, SIGCSE'2024.
116. "Upper Bounds on Ramsey Numbers Involving $C_4$" (with Luis Boza), *in preparation.*

**Science Magazines and other Dissemination**

117. "W poszukiwaniu funkcji skrótu", in Polish, (Designing hash function) with Michał Adamaszek, *DELTA*, 408 (2008) 1-3.
118. "Some Ramsey Problems Involving Triangles - Computational Approach", in *Ramsey Theory: Yesterday, Today and Tomorrow*, edited by Alexander Soifer, Progress in Mathematics 285, Springer-Birkhauser 2011, 185-188.

**Visiting Positions/Fellowships**

| | | |
|---|---|---|
| October - November | 1988 | National Autonomous University of Mexico in Mexico City |
| July - December | 1991 | Technical University of Gdańsk, Poland |
| July - August | 1992 | Australian National University in Canberra, Australia |
| January - February | 1994 | Australian National University in Canberra, Australia |
| July - August | 1997 | Australian National University in Canberra, Australia |
| November | 2010 | Technical University of Gdańsk, Poland |
| February, April-May | 2014 | Technical University of Gdańsk, Poland |
| May | 2014 | Institut Mittag-Leffer, Djursholm, Sweden |

**Invited Presentations**

1987 - University of Kentucky, Lexington, KY
1988 - National University of Mexico, Mexico City, Mexico
1990 - University of Alberta, Edmonton, AB, Canada
1990 - Pennsylvania State University, University Park, PA
1991 - Queens University, Kingston, ON, Canada
1991 - Technical University of Gdańsk, Poland
1991 - University of Warsaw, Poland
1991 - Technical University of Wrocław, Poland
1991 - Technical University of Braunschweig, Germany
1991 - Polish Academy of Sciences, Warsaw, Poland
1992 - Australian National University, Canberra, Australia
1992 - University of Sydney, Sydney, Australia
1993 - University of Colorado at Denver, CO
1993 - St. John Fisher College, Rochester, NY
1994 - University of Queensland, Brisbane, Australia
1994 - Concordia University, Montreal, PQ, Canada
1995 - Technical University of Gdańsk, Poland
1996 - Technical University of Gdańsk, Poland
1996 - University of Sevilla, Spain
1997 - University of Alberta, Edmonton, AB, Canada
1997 - Technical University of Gdańsk, Poland
1998 - University of Rochester (2), NY
1999 - University of Alberta, Edmonton, AB, Canada
1999 - Michigan Technological University, Houghton, MI
1999 - Technical University of Gdańsk, Poland
2001 - XXVII Szkoła Matematyki Pogladowej, Grzegorzewice, Poland
2001 - Technical University of Gdańsk, Poland
2002 - Technical University of Gdańsk, Poland
2003 - Rochester Institute of Technology, Mathematics Colloquium, Rochester, NY
2004 - Technical University of Gdańsk, Poland
2005 - University of Rochester, NY
2005 - Nineteenth Midwest Conference on Combinatorics, Cryptography and Computing, Rochester, NY
2006 - Technical University of Gdańsk, Poland
2007 - University of Rochester, NY
2007 - Harris Corp., Rochester, NY
2007 - Technical University of Gdańsk, Poland
2007 - Technical University of Poznań, Poland
2007 - University of Warsaw, Poland
2008 - University of Alberta, Edmonton, AB, Canada
2008 - University of Colorado at Denver, CO

2009 - DIMACS Ramsey Theory Workshop, Rutgers University, New Brunswick, NJ
2010 - University of Rochester, NY
2010 - West Virginia University, Morgantown, WV
2010 - Technical University of Gdańsk, Poland
2012 - AMS Eastern Meeting, Rochester, NY
2012 - Technical University of Gdańsk, Poland
2013 - Ghent University, Belgium
2014 - AMS Joint Mathematics Meetings, Baltimore, MD
2014 - Technical University of Gdańsk, Poland
2014 - Cardinal Stefan Wyszyński University, Warszawa, Poland
2014 - Technical University of Wrocław (2), Poland
2014 - Institut Mittag-Leffler, Djursholm, Sweden
2014 - Fifth Polish Combinatorial Conference, Bedlewo, Poland
2015 - Canadian Discrete and Algorithmic Mathematics Conference, Saskatoon, SK, Canada
2015 - Third Gdańsk Workshop on Graph Theory, Poland
2017 - Canadian Discrete and Algorithmic Mathematics Conference, Toronto, ON, Canada
2017 - Ghent Graph Theory Workshop, Ghent, Belgium
2017 - Computers in Scientific Discovery 8, Mons, Belgium
2018 - AMS Joint Mathematics Meetings, San Diego, CA
2018 - SIAM Conference on Discrete Mathematics, Denver, CO
2019 - Ghent Graph Theory Workshop, Ghent, Belgium
2020 - Extremal Graph Theory Conference, Xining, Qinghai, China (planned, cancelled)
2022 - Combinatorics Today Series, Bandung, Indonesia, online
2023 - Belgian Graph Theory Conference on Structure and Algorithms, Ghent, Belgium

**Contributed Conference Presentations**

1977-1980 - Local and regional conferences in Poland,
1978 - Conference on Logic in Parallel Computations, Salgótarján, Hungary
1979 - Conference on Complexity of Parallel Computations, Berlin, Germany
1980-1983 - Local/regional conferences in Mexico
1987 - 18-th Southeastern Conference on Combinatorics, Boca Raton, FL
1988 - Fourth SIAM Conference on Discrete Mathematics, San Francisco, CA
1989 - 20-th Southeastern Conference on Combinatorics, Boca Raton, FL
1989 - First Great Lakes Computer Science Conference, Kalamazoo, MI
1990 - Fifth SIAM Conference on Discrete Mathematics, Atlanta, GA
1991 - Second Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco, CA
1991 - Colloquium on Combinatorics, Braunschweig, Germany
1993 - 24-th Southeastern Conference on Combinatorics, Boca Raton, FL
1994 - Ninth Midwest Conference on Combinatorics and Computing, Lincoln, NE
1995 - 6-th Auburn Combinatorics Conference, Auburn, AL
1995 - 8-th Cumberland Conference, Nashville, TN
1996 - 7-th Auburn Combinatorics Conference, Auburn, AL
1996 - Eleventh Midwestern Conference on Combinatorics and Computing, Las Vegas, NV
1997 - 28-th Southeastern Conference on Combinatorics, Boca Raton, FL
1997 - Colloquium on Combinatorics, Braunschweig, Germany
1998 - 11-th Cumberland Conference, Johnson City, TN
1999 - 3in1 Graph Theory Workshop, Kraków, Poland
2000 - Tenth SIAM Conference on Discrete Mathematics, Minneapolis, MN
2000 - Fourteenth Midwest Conference on Combinatorics, Cryptography and Computing, Wichita, KS
2001 - 32-nd Southeastern Conference on Combinatorics, Baton Rouge, LA
2001 - Fifteenth Midwest Conference on Combinatorics, Cryptography and Computing, Las Vegas, NV

2002 - 33-rd Southeastern Conference on Combinatorics, Boca Raton, FL
2003 - 34-th Southeastern Conference on Combinatorics, Boca Raton, FL
2004 - Fourteenth SIAM Conference on Discrete Mathematics, Nashville, TN
2004 - 29-th Int. Symposium on Mathematical Foundations of Computer Science, MFCS'04, Prague
2004 - Eighteenth Midwest Conference on Combinatorics, Cryptography and Computing, Rochester, NY
2006 - 37-th Southeastern Conference on Combinatorics, Boca Raton, FL
2007 - 38-th Southeastern Conference on Combinatorics, Boca Raton, FL
2008 - 39-th Southeastern Conference on Combinatorics, Boca Raton, FL
2009 - 40-th Southeastern Conference on Combinatorics, Boca Raton, FL
2010 - SIAM Conference on Discrete Mathematics, Austin, TX
2011 - 24-th Cumberland Conference, Louisville, KY
2012 - 43-rd Southeastern Conference on Combinatorics, Boca Raton, FL
2012 - SIAM Conference on Discrete Mathematics, Halifax, NS, Canada
2012 - Colloquium on Combinatorics, Berlin, Germany
2013 - Canadian Discrete and Algorithmic Mathematics Conference, St. John's, NL, Canada
2019 - Canadian Discrete and Algorithmic Mathematics Conference, Vancouver, BC, Canada
2020 - SIAM Conference on Discrete Mathematics, Portland, OR (planned, cancelled)
2021 - Canadian Discrete and Algorithmic Mathematics Conference, online
2023 - The 8-th Gdańsk Workshop on Graph Theory, Sopot, Poland

**Other Attended Conferences**

1977-1980 - Local and regional conferences in Poland,
1978 - The World Congress of Mathematics, Helsinki, Finland
1979 - The FCS Conference in Olomouc, Czechoslovakia
1980-1983 - Local/regional conferences in Mexico
1985 - STOC'85, Providence, RI
1985 - Symposium on Complexity Theory, New York, NY
1986 - Third SIAM Conference on Discrete Mathematics, Clemson, SC
1989 - Theoretical Computer Science Conference, GWU, Washington, DC
1993 - Twentieth Mighty Conference on Graph Theory, Oxford, OH
1998 - Complexity '98, Buffalo, NY
1999 - Algorithms in Quantum Information Processing, Chicago, IL
1999 - Paul Erdős Memorial Lecture, Memphis, TN
2000 - Advanced Cluster Computing Consortium Workshop, Ithaca, NY
2001 - Symposium in honor of Juris Hartmanis, Ithaca, NY
2005 - Symposium on High-Performance Computing, Cornell Theory Center, Ithaca, NY
2009 - 23-rd Midwest Conference on Combinatorics, Cryptography and Computing, Rochester, NY
2011 - Atlanta Lecture Series in Combinatorics and Graph Theory, GSU, Atlanta, GA
2016 - 50 Years of the Hales-Jewett Theorem, Bellingham, WA
2016 - EXCILL III: Extremal Combinatorics at Illinois, Chicago, IL
2019 - 33-rd Midwest Conference on Combinatorics, Cryptography and Computing, Rochester, NY
2021 - National AI and Quantum Computing Symposium, MD, online
2021 - Graph Theory for Combinatorial Reconfiguration, Japan, online
2022 - 53-rd Southeastern Conference on Combinatorics, Boca Raton, FL, online

**Languages:** English (fluent), Spanish (fluent), Polish (native), some Russian