

Feb. 5, 2007

Curriculum vitae
MARIUS ZIMAND

Work Address

Department of Computer & Information Sciences
Towson University
8000 York Road
Towson, MD 21252
Tel: (410) 704 4967
Email: mzimand@towson.edu
URL: <http://triton.towson.edu/~mzimand>
Fax: (410) 704 3868

Home Address

326 Dunkirk Road
Baltimore, MD 21212
Tel: (410) 377 2879

RESEARCH AREA

Computational complexity, cryptography, network security, randomized algorithms, experimental algorithms.

TEACHING CAPABILITIES

Algorithms and data structures, theory of computation and computational complexity, network security, cryptography, introduction to programming, discrete mathematics, programming languages, operating systems.

PERSONAL US citizen; Married; One child.

EDUCATION

- **Ph.D. in Computer Science**, July 1996, Univ. of Rochester. Title of thesis: Existential theorems in computational complexity: size and robustness. Advisor: Lane Hemaspaandra.
- **M.S. in Computer Science**, Univ. of Rochester, 1994.
- **Ph.D. in Mathematics**, Univ. of Bucharest, June 1991. Title of thesis: Positive relativizations and Baire classification in computational complexity; Advisor: Cristian Calude.
- **M.S. in Mathematics**, Univ. of Bucharest, 1982.

OTHER EDUCATIONAL ACHIEVEMENTS

Postgraduate Summer School on Combinatorial Optimization, Cortona, Italy, July-August 1990, organized by Council of National Research Italy.
Postgraduate Course on Database Management Systems, Bucharest, March-April 1984, organized by the Central Institute for Computer Science Bucharest, Romania.
Postgraduate Course on Assembly Programming, Bucharest, October 1986, organized by the Central Institute for Computer Science, Bucharest, Romania.

HONORS Excellence in Scholarship Award, given by the Fischer College of Science and Mathematics, Towson University, Oct. 27, 2006.

EATCS ICALP Best Paper Award 2005 for the paper "Simple extractors via constructions of cryptographic pseudo-random generators."

GRANTS 2006, Grant from NSF (NSF award number CCF-0634830), New directions in the study of randomness extractors (PI), \$125306. 2004, Grant from NSF (NSF award number 0353868) REU Site: CS Undergraduate Research at Towson University (co-PI), \$223764, 06/01/2004- 05/31/2007.
2001, Grant from NSF (NSF award number 0113783), Undergraduate Computer Security Track, \$160,068 (co-PI), 09/01/2001-09/01/2003.
1997, Grant from Georgia Southwestern State Univ., within the Distinguished Professor Program for the development of a distance learning course in Discrete Mathematics.
1990, Grant from the Romanian Ministry of Education and Science for the research project "Topology and theory of computation."
1984, Grant from the Academy of Medical Sciences, Romania, for the project "Computer-assisted diagnosis for liver diseases."

ACADEMIC EXPERIENCE

Towson University Associate Professor, Fall 2003 - present.

Assistant Professor, Fall 1999 - Fall 2003, courses

Security and Internet Algorithms (Spring 2004, Spring 2005, Spring 2006, graduate level)

Applied Cryptography (Spring 2004, Spring 2003, Fall 2003, Fall 2004, Fall 2005, Fall 2006, graduate level)

Network Security and Cryptography (Fall 2001, Spring 2002, Fall 2002, graduate level)

Cryptography (Fall 2002, Fall 2003, Fall 2004, Fall 2005, Fall 2006, undergraduate level)

Data Structures and Algorithms (Spring 2001, Spring 2002, Fall 2003, Spring 2005, Spring 2006, undergraduate level)

Theory of Computation (Spring 2005, Spring 2006)

Operating Systems (Spring 2001, Fall 2001, graduate level)

Design and Analysis of Algorithms (Fall'2000; Fall 2005, fall 2006, undergraduate level)

Computer Science II (Fall 2001, Spring 2003; undergraduate level)

Distributed Operating Systems (Spring'00, Fall'2000; graduate level)

Computer Graphics (Fall'99, Summer'2000, Summer'2001, Summer 2002, Summer 2003; graduate level)

Introduction to Computer Science I (Fall'99, Spring'00; undergraduate level)

Georgia Southwestern State University

Assistant Professor, 1996 - 1999, courses:

Design and Analysis of Algorithms (Fall'96, Fall'97, Fall'98; undergraduate and graduate level)

Introduction to Structured Programming (C) (Fall'97, Winter'98; undergraduate level)

Introduction to Structured Programming (C++) (Fall'98; undergraduate level)

Advanced Structured Programming (C) (Spring'98; undergraduate level)

Object Oriented Programming (Java) (Summer'97; undergraduate and graduate level)

Data Structures (Winter'97; undergraduate level)

Theory of Computation (Fall'96, Winter'97, Fall'98; undergraduate and graduate level)

Microcomputer Application (Summer'97; undergraduate level)

Formal Methods in Programming Languages (Fall'96; graduate level)

Advanced Data Structures (Fall'96; graduate level)

Concepts of Programming Languages (Spring'97, Spring'98; undergraduate and graduate level)

Network Security and Applied Cryptography (Winter'98; graduate level)

Artificial Intelligence (Spring'97; undergraduate and graduate level)

University of Bucharest:

Assistant Professor, Spring 1989 - 1992 , courses:

Theory of computation and computational complexity (Spring 1992, graduate level), Data structures (Spring 1992, graduate level), Introduction to programming (Spring 1989, Fall-Spring 1990, 1991, Spring 1992 undergraduate level), Theory of computation (Fall-Spring 1990, undergraduate level), Formal languages and automata (Fall 1991, undergraduate level), Algorithms and data structures (Spring 1991, undergraduate level), Workshop in programming (Fall-Spring 1989, 1990, 1991, Spring 1992, undergraduate level).

DEPARTMENT AND UNIVERSITY SERVICE

- Towson University
 - Member of the Doctoral Program Committee, 2004 -.
 - Member of the Doctoral Dissertation Committee, 2004 -.

- Member of the Scholarship Committee of the College of Science and Mathematics, 2000-.
- Member of the College of Science and Mathematics Council, 2001-2004.
- Member of the Graduate Committee of the Department of Computer and Information Sciences, 1999-.
- Member of the Scholarship and Retention Committee for the “CSEMS: Towson Tiger” Scholarship.
- Georgia Southwestern State University
 - Director of the Graduate Program, 1998 - 1999.
 - Advisor for the Bachelor Degree in Computer Information Science, 1996 - 1997.
 - Member of the Faculty Recruiting Committee, 1996, 1997.
 - Member of the Instructional Technology Advisory Committee, 1996-1999.
 - Member of the University Relations Committee, 1997.
 - Member of the Faculty Affairs Committee, 1998-1999.
 - Member of the GSW Task Force on Alcohol and Other Drugs, 1998-1999.
 - Member of the Curriculum Committee at University of Rochester, 1995-1996.

INDUSTRIAL EXPERIENCE

Research Institute for the Electrotechnical Industry, Bucharest:

Mathematician, 1982-1986 ; researcher, 1986-1988.

Responsible for the following projects: Computer-aided diagnosis of liver diseases, Spectral analysis of the vibrations of naval engines, Graphical presentation of geophysical data.

Computing Center of the University of Bucharest:

Programmer, 1988-1989.

Projects: Interpreter for Prolog. Research study: Topological size of complexity classes.

MISCELLANEOUS

Member of the Editorial Board of Journal of Universal Computer Science, an international journal published by Springer Verlag.

Editor of a special issue of the Journal of Universal Computer Science dedicated to the SAWN 2005 workshop.

Member of the Program Committee of the International Multi-Conference on Computing in the Global Information Technology -Challenges for the Next Generation of IT & C- ICCGI'07.

Member of the Program Committee of the conference 7th ACIS International Conference on Software Engineering, AI, Networking, and Parallel/Distributed Computing (SNPD'2006), June 19-10, Las Vegas, Nevada.

Member of the Program Committee of the conference International Multi-Conference

on Computing in the Global Information Technology, Challenges for the Next Generation of IT&C - ICCGI06, August 1-3, 2006, Bucharest, Romania
 Member of the Program Committee of the conference Discrete Mathematics and Theoretical Computer Science (DMTCS'01), Constanta, Romania, July 2-6, 2001.
 Reviewer for *Zentrallblatt für Mathematik*, *Mathematical Reviews*, *Computing Reviews*.
 Reviewer for ICALP'2002, STACS'2000, the International Conference on Computing and Information (1994, 1996), IEEE Conference on Computational Complexity (1996, 1997), Internat. Parallel Processing Symposium (1998), 9th Symposium on Parallel and Distributed Processing (1998), Computer Science Logic (1998), *SIAM Journal on Computing*, *Information Processing Letters*, *Journal of Computer and System Sciences*, *Journal of Universal Computer Science*, *Information and Computation*, and others.
 Session chair at the 7th International Conference on Computing and Information (1995).
 Session chair at the 8th International Conference on Computing and Information (1996).
 Member of the Association for Computer Machinery, EATCS, Sigact, IEEE, ISCA, and Balkan Logical Society.

BOOKS and BOOK CHAPTERS

1. **Computational Complexity - A Quantitative Perspective**, Elsevier, 2004.
2. **Structural Complexity**, in *How To Cope With Complexity*, M. Malita and C. Calude (eds.), Ed. Academiei, 1993, 211-273 (in Romanian).

REFEREED JOURNAL PUBLICATIONS

1. **The complexity of finding top-Toda-equivalence-class members**, L. Hemaspaandra, M. Ogihara, M. Zaki, and Marius Zimand, *Theory of Computing Systems*, vol. 39, no. 5 (Sept. 2006), pp. 669-684.
2. **Almost-everywhere superiority for quantum polynomial time**, E. Hemaspaandra, L. Hemaspaandra, and M. Zimand, *Information and Computation*, vol. 175(2), 171-181, 2002.
3. **Extractors for the real world**, K. Xue and M. Zimand, *Journal of Universal Computer Science*, vol.6(1), pp. 212-225, 2000.
4. **Weighted NP optimization problems: logical definability and approximation properties**, M. Zimand, *SIAM J. on Computing*, vol. 28(1), 36-56, 1999.
5. **Relative to a random oracle, P/poly is not measurable in EXP**, M. Zimand, *Information Processing Letter*, vol. 69, pp. 83-86, 1999.
6. **On the size of classes with weak membership properties**, M. Zimand, *Theoretical Computer Science*, vol. 209, pp. 225-235, 1998.
7. **Power Balance and Congressional Apportionment**, L. Hemaspaandra, K. Rajasethupathy, P. Sethupathy, and M. Zimand, *Journal of Experimental Algorithms*, vol. 3(#1), Aug. 1998. (16 pp.)

8. **Large sets in AC^0 have many strings with low Kolmogorov complexity**, M. Zimand, *Information Processing Letters* 62(3), 165-170, 1997.
9. **Polynomial-time semi-rankable sets**, L. Hemaspaandra, M. Zaki, and M. Zimand, *Journal of Computing and Information*, 2(1), Special Issue: Proceedings of the 8th International Conference on Computing and Information, pages 50-67, 1996. CD-ROM ISSN 1201-8511/V2/#1.
10. **A high-low Kolmogorov complexity law equivalent to the 0-1 law**, M. Zimand, *Information Processing Letters*, 57(2)(1996), pp.59-64.
11. **Strong self-reducibility precludes strong immunity**, L. Hemaspaandra and M. Zimand, *Mathematical Systems Theory* 29(5) (1996), pp. 539- 548.
12. **Effective category and measure in abstract complexity theory**, C. Calude and M. Zimand, *Theoretical Computer Science* 154 (2) (1996), pp. 307-327.
13. **On the topological size of p-m-complete sets**, M. Zimand, *Theoretical Computer Science* 147(2)(1995), pp. 137-147.
14. **Is independence an exception?**, C. Calude, H. Jürgensen and M. Zimand, *Applied Mathematics and Computation* 66, 1(1994), pp. 63-76.
15. **Minimum spanning hypertrees**, I. Tomescu and M. Zimand, *Discrete Applied Mathematics* 54(1994), pp. 67-76 (reviewed in MR 95f:05085, Gui Zhen Liu).
16. **If not empty, NP-P is topologically large**, M. Zimand, *Theoretical Computer Science* 119(1993), pp. 293-310 (reviewed in MR 94k:68074, self-review).
17. **Recursive Baire classification and speedable functions**, C. Calude, G. Istrate, and M. Zimand, *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 38(1992), pp. 169-178 (reviewed in MR 94j:03083, Robert M. Baer).
18. **Set restricted relativization**, M. Zimand, *Anal. Univ. Al. I. Cuza Iasi*, 25(1989), pp. 329-335 (reviewed in MR 92e:03058, M.I. Dekhtyar).
19. **On the existence of complete problems for positive relativized complexity classes**, M. Zimand, *Anal. Univ. Bucharest Mat.-Inf.*, 2(1988), pp. 88-92 (reviewed in MR 90b:03056, Wen Qi Huang).
20. **On relativizations with restricted number of accesses to the oracle set**, M. Zimand, *Mathematical Systems Theory* 20(1987), pp. 1-11 (reviewed in MR 89a:68080, K.W. Wagner; ZBL 638.68030, D.Yu. Grigoriev).
21. **On the topological size of sets of random strings**, M. Zimand, *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 32(1986), pp. 81-88 (reviewed in MR 87f:03108, C.P. Schnorr).
22. **Baire classification and partial recursive functions**, M. Zimand, *Recursive Function Theory Newsletter*, 32(1984), 346.
23. **A relation between correctness and randomness in the computation of probabilistic algorithms**, C. Calude and M. Zimand, *International Journal of Computer Mathematics*, 16(1984), pp. 47-53 (reviewed in MR 86e: 68052, C.P. Schnorr).
24. **Complexity of probabilistic algorithms**, M. Zimand, *Foundations of Control Engineering* 8(1983), pp. 33-49 (reviewed in MR 85e:03096, self-review).

OTHER: COLUMNS, INVITED SURVEY PAPERS

1. **Worlds to die for**, L. Hemaspaandra, A. Ramachandran, M. Zimand, *Sigact News*, 26(4), pp. 5-15, December 1995.
2. **Précisions sur la methode topologique en complexité algorithmique**, M. Zimand, *Singularité*, 3(1992), pp. 25-27.

MAIN REFEREED CONFERENCE CONTRIBUTIONS

1. **On derandomizing probabilistic sublinear-time algorithms**, Marius Zimand, 22nd IEEE Conference in Computational Complexity, July 13-16, 2007, San Diego, California.
2. **Exposure-resilient extractors**, Marius Zimand, 21st IEEE Conference in Computational Complexity, Prague, July 16-20, 2006, Prague, Czech Republic.
3. **Undergraduate Computer Security Education: A Report on our Experiences & Learning** Shiva Azadegan, Michael O'Leary, Alexander Wijesinha, Marius Zimand, Workshop on Education in Computer Security (WECS'2006), Monterey, Jan. 4-6, 2006.
4. **Simple extractors via cryptographic pseudo-random generators**, Marius Zimand, ICALP'05, July 11 - 15, 2005. Published in Proceedings ICALP 2005, Lisbon, Lecture Notes in Computer Science vol. 3580, pp. 115-127, Springer Verlag (publisher). - Winner of the EATCS ICALP Best Paper Award 2005.
5. **A list-decodable error-correcting code with local encoding and decoding**, Marius Zimand, Proceedings SNPD 2005, pp. 232-237, Towson, May 23-25 2005, IEEE Computer Society (publisher).
6. **The complexity of finding top-Toda-equivalence-class members**, L. Hemaspaandra, M. Ogihara, M. Zaki, and Marius Zimand, Latin'2004, Buenos Aires, Argentine, April 5-8 2004. Published in the Proceedings of Latin'2004, Lecture Notes in Computer Science Springer Verlag, pp. 90-99.
7. **Kolmogorov random strings and hard functions**, M. Zimand, Centennial Seminar on Kolmogorov complexity and Applications, Dagstuhl, Germany, April 27- May 2, 2003.
8. **A dedicated undergraduate track in computer security education**, S. Azadegan, M. Lavine, M. O'Leary, A. Wijesinha, M. Zimand, 3rd World Conference on Information Security, Monterey, California, June 26-28 2003.
9. **An undergraduate track in computer security**, S. Azadegan, M. Lavine, M.O'Leary, A. Wijesinha, M. Zimand, 8th Annual Conference in Innovation and Technology in Computer Science Education (ITiCSE'2003), Thesaloniki, Greece, June 30 - July 2, 2003.
10. **Probabilistically checkable proofs the easy way**, M. Zimand, in TCS'2002 part of the 7th IFIP World Computer Congress, Montreal, Aug. 26-29, 2002.

11. **Sampling under adverse conditions with applications to distributed computing**, Workshop on Parallel Algorithms (WOPA'99), part of FCRC Atlanta, May, 1999.
12. **Efficient privatization of random bits**, Workshop on Randomized Algorithms, Satellite Workshop of MFCS'98, Brno, Czech Republic, Aug. 27-28, 1998. (Proceedings available at the web site of Electronic Colloquium in Computational Complexity, <http://www.eccc.uni-trier.de/eccc-local/ECCC-LectureNotes/eccc-lecture-notes.html>)
13. **Sharing random bits with no process coordination**, 1998 12th Internat. Parallel Processing Sympos. and 9th Symp. on Parallel and Distributed Processing (IPPS/SPDP), Orlando, March 30 - April 3, 1998, pp. 455-459.
14. **How to share random bits**, M. Zimand, Proc. of the ISCA 10th International Conference "Parallel and Distributed Computing Systems," New Orleans, Oct. 1-3, 1997, pp. 23-26.
15. **Polynomial-time semi-rankable sets**, L. Hemaspaandra, M. Zaki and M. Zimand, Proceedings of the 8th International Conference on Computing and Information, Waterloo, Canada, pp. 50-67, 1996.
16. **Weighted NP optimization problems: logical definability and approximation properties**, M. Zimand, Proceedings of the 10th IEEE Structure in Complexity Conference, Minneapolis, USA, June 1995, IEEE Press, pp. 12-28, 1995.
17. **Effective category and measure in abstract complexity theory**, C. Calude and M. Zimand, Proceedings of the 10th Fundamentals of of Computation Theory Conference, Dresden, Germany, August 1995, Springer-Verlag Lecture Notes in Computer Science #965, pp. 156-171, 1995.
18. **Large sets in AC^0 : a Kolmogorov complexity property and some applications**, M. Zimand, 7th International Conference on Computing and Information, Peterborough, Canada, July 1995.
19. **On the size of classes with weak membership properties**, M. Zimand, 7th International Conference on Computing and Information, Peterborough, Canada, July 1995.
20. **On three theorems in abstract complexity theory: a topological glimpse**, C. Calude and M. Zimand, Second International Colloquium on Words, Languages and Combinatorics, Kyoto, Japan, 1992.
21. **If not empty, NP-P is topologically large**, M. Zimand, Conference: "NP-Completeness: The first 20 years," Erice, Italy, 1991.
22. **Complexity bounded Martin-Löf tests**, M. Zimand, Proceedings of the Conference "Mathematical Logic and its Applications," Druzhba (Bulgaria), 1986, Plenum Press, pp. 351-359 (reviewed in MR 89i:03108, J. L. Balcazar).
23. **Expert systems in medicine: consideration regarding the design of a knowledge base for computer aided medical diagnosis**, E. Diatcu and M. Zimand, 9th Conf. Medinfo, Cluj, Romania, 1985.

24. **A data base for computer aided medical diagnosis**, E. Diatcu, A. Susea, M. Zimand, I. Greceanu, 12th Symp. of Romanian Academy for Medical Sciences, 1984.
25. **On the logical independence of random strings**, M. Zimand, Symp. Info'83, Jassy, Romania, 1983.

TECHNICAL REPORTS

1. **Simple extractors via constructions of cryptographic pseudo-random generators**, M. Zimand, European Computational Complexity Colloquium Technical Report TR05-071, July 2005. Also released as Los Alamos National Laboratories Quantum-Ph TR cs.CC/0501075, February 2005 (Revised May 2005).
2. **The complexity of finding the top-Toda-equivalence-class members** L. Hemaspaandra, M. Ogihara, M. Zaki, M. Zimand Technical Report 808, Department of Computer Science, Univ. of Rochester, August 2003.
3. **Almost-everywhere superiority for polynomial quantum time languages**, E. Hemaspaandra, L. Hemaspaandra, and M. Zimand, Technical Report 754, Department of Computer Science, Univ. of Rochester, July 2001.
4. **Probabilistically checkable proofs the easy way**, M. Zimand, European Computational Complexity Colloquium Technical Report TR01-027, April 2001.
5. **Almost-everywhere superiority for polynomial quantum time**, E. Hemaspaandra, L. Hemaspaandra, and M. Zimand, Technical Report 720, Department of Computer Science, Univ. of Rochester, October 1999. Also released as Los Alamos National Laboratories Quantum-Ph TR 9910033, October 1999.
6. **How to privatize random bits**, M. Zimand, Technical Report 616, Department of Computer Science, Univ. of Rochester, April 1996.
7. **Worlds to die for**, L. Hemaspaandra, A. Ramachandran, and M. Zimand, Technical Report 597, Department of Computer Science, Univ. of Rochester, November 1995.
8. **On randomized cryptographic primitives**, Marius Zimand, Technical Report 586, Department of Computer Science, Univ. of Rochester, May 1995.
9. **Polynomial-time semi-rankable sets**, L. Hemaspaandra, M. Zaki, and M. Zimand, Technical Report 584, Department of Computer Science, Univ. of Rochester, May 1995.
10. **On the size of sets with weak membership properties**, M. Zimand, Technical Report 557, Department of Computer Science, Univ. of Rochester, December 1994.
11. **Large sets in AC^0 : a Kolmogorov complexity property and some applications**, M. Zimand, Technical Report 556, Department of Computer Science, Univ. of Rochester, December 1994.
12. **Martin-Löf tests can help too**, M. Zimand, Technical Report 541, Department of Computer Science, Univ. of Rochester, November 1994.

13. **Effective category and measure in abstract complexity theory**, C. Calude and M. Zimand, Technical Report 529, Department of Computer Science, Univ. of Rochester, August 1994.
14. **Weighted NP optimization problems: logical definability and approximation properties**, M. Zimand, Technical Report 516, Department of Computer Science, Univ. of Rochester, June 1994.
15. **Strong forms of balanced immunity**, L.A. Hemaspaandra and M. Zimand, Technical Report 480, Department of Computer Science, Univ. of Rochester, December 1993, revised May 1994.
16. **Baire category classification in abstract complexity theory**, C. Calude and M. Zimand, Technical Report 84, Department of Computer Science, Univ. of Auckland, New Zealand, November 1993.
17. **The complexity of the optimal spanning hypertree problem**, M. Zimand, Technical Report 471, Department of Computer Science, Univ. of Rochester, September 1993.
18. **On the topological size of p-m-complete sets**, M. Zimand, Technical Report 459, Department of Computer Science, Univ. of Rochester, May 1993.
19. **The set of independent statements is topologically large**, C. Calude, H. Jürgensen, and M. Zimand, Technical Report No. 338, Dec. 1992, Department of Computer Science, Univ. of Western Ontario, London, Ontario, Canada.

RECENT SELECTED INVITED TALKS

1. **Exposure-resilient extractors with an application to the derandomization of probabilistic sublinear-time algorithms**, University of Maryland College Park, December 8, 2006.
2. **Derandomization of BPTIME[sublinear]**, University of Maryland College Park, May 3, 2006.
3. **Extractors via constructions of cryptographical pseudo-random generators**, presented at the Rutgers/DIMACS Theoretical Computer Science Seminar on May 2, 2006.
4. **Extractors from pseudo-random generators via Kolmogorov complexity**, presented at the seminar "Kolmogorov Complexity and Applications," Dagstuhl, Germany, Jan. 29 - Feb. 3, 2006.
5. **Simple extractors via constructions of cryptographic pseudo-random generators**, presented at University of Maryland College Park, Nov. 3, 2004.
6. **Kolmogorov random strings and hard functions**, presented at the Centennial Seminar on Kolmogorov Complexity and Applications, Dagstuhl, Germany, April 27 - May 2, 2003.
7. **Probabilistically checkable proofs the easy way**, presented at University of Rochester, March 2001.
8. **Probabilistically checkable proofs the easy way**, presented at University of Maryland College Park, February 2001.

9. **Sampling under adverse conditions**, presented at University of Rochester, Jan. 2000.
10. **Privatizing random bits and applications**, presented at University of Nevada at Las Vegas, Vassar College, Eastern Carolina University, 1999.