

Department of Computer Science and Engineering  
University of Connecticut, U-3155  
Storrs, CT 06269  
tel. (860) 486-4290, fax. (860) 486-4817  
acr@cse.uconn.edu  
<http://www.engr.uconn.edu/~acr/>

Home address:  
148 Chaffeeville Rd.  
Storrs, CT 06268  
tel. (860) 423-6436

# ALEXANDER C. RUSSELL

## Professional Experience

- 9/1999 – present      • Assistant Professor  
UNIVERSITY OF CONNECTICUT      Storrs, CT  
Department of Computer Science and Engineering
- 9/1997 – 8/1999      • Postdoctoral Fellow, Advisor: Professor David Zuckerman. Joint position:  
UNIVERSITY OF CALIFORNIA, BERKELEY      Berkeley, CA  
Computer Science Division, and  
UNIVERSITY OF TEXAS AT AUSTIN      Austin, TX  
Department of Computer Science
- 9/1996 – 8/1997      • Postdoctoral Fellow, Advisor: Professor Johan Håstad.  
ROYAL INSTITUTE OF TECHNOLOGY      Stockholm, Sweden  
Department of Computer Science and Numerical Analysis

## Degrees

- 5/1996      • Doctor of Philosophy, Applied Mathematics, Advisor: Professor Michael Sipser  
MASSACHUSETTS INSTITUTE OF TECHNOLOGY      Cambridge, MA
- 1/1993      • Master of Science, Computer Science, Advisor: Professor Silvio Micali  
MASSACHUSETTS INSTITUTE OF TECHNOLOGY      Cambridge, MA
- 5/1991      • Bachelor of Arts cum laude, Computer Science;  
Bachelor of Arts cum laude, Mathematics  
CORNELL UNIVERSITY      Ithaca, NY

## Honors and Professional Activities

- National Science Foundation CAREER Award, 2001-2006.
- National Science Foundation Graduate Fellow.
- Member  $\Phi\beta\kappa$ .
- Best Paper Award: L. Engebretsen, J. Holmerin, A. Russell, “Inapproximability Results for Equations over Finite Groups,” 29th International Colloquium on Automata, Languages, and Programming (ICALP), July 2002.
- Conference Organizer, “AMS-IMS-SIAM Summer Research Conference: Graph Coloring and Symmetry,” July 21-25, 2002, South Hadley, Massachusetts.

## Honors and Professional Activities (continued)

- Program Committee Member, Latin American Informatics (LATIN), 2002.
- Local Arrangements vice-chair, Twentieth ACM Symposium on Principles of Distributed Computing (PODC), 2001.
- Program Committee Member, Scandinavian Workshop on Algorithm Theory (SWAT), 1998.

## Publications

### Journal Articles (published or in press)

1. Nina Amenta, Thomas Peters, and Alexander Russell. Computational topology: Ambient isotopic approximation of 2-manifolds. *Theoretical Computer Science*. In press.
2. Mikael Goldmann, Mats Näslund, and Alexander Russell. Complexity bounds on general-hard core predicates. *Journal of Cryptology*, 14(3):177–195, 2001.
3. Mikael Goldmann and Alexander Russell. The computational complexity of solving equations over finite groups. *Information and Computation*, 178:253–262, 2002.
4. Mikael Goldmann, Alexander Russell, and Denis Thérien. An ergodic theorem for read-once nonuniform deterministic finite automata. *Information Processing Letters*, 73:23–28, 2000.
5. Marcos Kiwi, Carsten Lund, Alexander Russell, Daniel Spielman, and Ravi Sundaram. Alternation in interaction. *Computational Complexity*, 9(3-4):202–246, 2000.
6. Michael Klugerman, Alexander Russell, and Ravi Sundaram. Embedding complete graphs into hypercubes. *Discrete Mathematics*, 186(1–3):289–293, 1998.
7. S. Ravi Kumar, Rina Panigrahy, Alexander Russell, and Ravi Sundaram. A note on optical routing on trees. *Information Processing Letters*, 62(6):296–300, June 1997.
8. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Approximating latin square extensions. *Algorithmica*, 24(2):128–138, 1999.
9. Mats Näslund and Alexander Russell. Extraction of optimally unbiased bits from a biased source. *IEEE Transactions on Information Theory*, 46(3):1093–1103, May 2000.
10. Alexander Russell. Necessary and sufficient conditions for collision-free hashing. *Journal of Cryptology*, 8:87–99, 1995.
11. Alexander Russell. An easy reduction of an isoperimetric inequality on the sphere to extremal set theory. *American Mathematical Monthly*, 107(1):57–59, January 2000.
12. Alexander Russell, Michael Saks, and David Zuckerman. Lower bounds for leader election and collective coin-flipping in the perfect information model. *SIAM Journal on Computing*, 31(6), 2003.
13. Alexander Russell and Ravi Sundaram. The relativized relationship between probabilistically checkable debate systems, IP, and PSPACE. *Information Processing Letters*, 53:61–68, 1995.
14. Alexander Russell and Ravi Sundaram. A note on the asymptotics and computational complexity of the graph distinguishing problem. *Electronic Journal of Combinatorics*, 5(1):R23, 1998.
15. Alexander Russell and Ravi Sundaram. Symmetric alternation captures BPP. *Computational Complexity*, 7(2):152–162, 1998.
16. Alexander Russell and David Zuckerman. Perfect information leader election in  $\log^* n + O(1)$  rounds. *Journal of Computer and System Sciences*. 63:612–626, 2001.
17. Alberto Segre, Charles Elkan, and Alexander Russell. A critical look at experimental evaluations of EBL. *Machine Learning*, 6:183–195, 1991.

## Publications (continued)

### Journal Articles (accepted)

1. Lars Engebretsen, Jonas Holmerin, and Alexander Russell. Inapproximability Results for Equations over Finite Groups. *Theoretical Computer Science*. Accepted pending revision.
2. Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. The Hidden Subgroup Problem and Quantum Computation Using Group Representations. *SIAM Journal on Computing*. Accepted pending revision.

### Articles in Periodicals

1. Alexander Russell and Alex A. Shvartsman. Distributed Computation Meets Design Theory: Local Scheduling for Disconnected Cooperation. *Bulletin of the EATCS*. 77:120–131, 2002.

### Book Chapters

1. Mats Näslund and Alexander Russell. Achieving optimal fairness from biased coinflips. In Kwok-Yan Lam, Igor Shparlinski, Huaxiong Wang, and Chaopeng Xing, editors, *Cryptography and Computational Number Theory*, volume 20 of *Progress in Computer Science and Applied Logic*, pages 303–319. Birkhäuser, 2001.
2. Alberto Segre, Charles Elkan, Daniel Scharstein, Geoff Gordon, and Alexander Russell. Adaptive inference. In S. Chipman and A. Meyrowitz, editors, *Foundations of Knowledge Acquisition*, volume 2, pages 43–81. Kluwer, 1993.

### Conference Articles (in published proceedings)

1. Mihir Bellare, Shafi Goldwasser, Carsten Lund, and Alexander Russell. Efficient probabilistically checkable proofs and applications to approximation. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on the Theory of Computing (STOC)*, pages 294–304, San Diego, California, 16–18 May 1993.
2. Lars Engebretsen, Jonas Holmerin, and Alexander Russell. Inapproximability results for equations over finite groups. In *Proceedings of the Twenty-Ninth International Colloquium on Automata, Languages, and Computation (ICALP)*, volume 2380 of *Lecture Notes in Computer Science*, pages 73–85, Springer, July 2002.
3. Ch. Georgiou, A. Russell, and A. A. Shvartsman. The complexity of distributed cooperation in the presence of failures. In *Proceedings of the 4th International Conference on Distributed Computing (OPODIS)*, pages 245–264, Paris, France, December 2000.
4. Ch. Georgiou, A. Russell, and A. A. Shvartsman. The complexity of synchronous iterative Do-All with crashes. In *Proceedings of the 15th Annual Symposium on Distributed Computing (DISC)*, volume 2180 of *Lecture Notes in Computer Science*, pages 151–165. Springer, October 2001.
5. Mikael Goldmann and Alexander Russell. The computational complexity of solving systems of equations over finite groups. In *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity*, pages 80–86, Atlanta, GA, May 1999. IEEE.
6. Mikael Goldmann and Alexander Russell. Spectral bounds on general hard core predicates. In *Proceedings of the Seventeenth Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, number 1770 in *Lecture Notes in Computer Science*, pages 614–624. Springer, 2000.
7. Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC)*, pages 627–635, Portland, OR, May 2000. ACM.

## Publications (continued)

8. Marcos Kiwi, Carsten Lund, Alexander Russell, Daniel Spielman, and Ravi Sundaram. Alternation in interaction. In *Proceedings of the Ninth IEEE Annual Conference on Structure in Complexity Theory*, pages 294–303, Amsterdam, The Netherlands, June 1994. IEEE.
9. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Approximating latin square extensions. In *Proceedings of the Second Annual Computing and Combinatorics Conference (COCOON)*, volume 1090 of *Lecture Notes in Computer Science*, Hong Kong, December 1995. Springer.
10. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Faster algorithms for optical switch configuration. In *IEEE International Conference on Communications (ICC)*, pages 1320–1324, Montreal, Quebec, June 1997.
11. Greg Grzegorz Malewicz, Alexander Russell, and Alex Allister Shvartsman. Distributed cooperation in absence of communication. In *Proceedings of the Fourteenth Annual Symposium on Distributed Computing (DISC)*, volume 1914 of *Lecture Notes in Computer Science*, pages 119–133, Toledo, Spain, October 2000. Springer.
12. Greg Grzegorz Malewicz, Alexander Russell, and Alex Allister Shvartsman. Local scheduling for distributed cooperation. In *Proceedings of the IEEE International Symposium on Network Computing and Applications (NCA)*, pages 244–255, Boston, MA, September 2001. IEEE.
13. Greg Grzegorz Malewicz, Alexander Russell, and Alex Allister Shvartsman. Optimal scheduling for disconnected cooperation. In *Proceedings of the Eighth Annual Colloquium on Structural Information and Communication Complexity (SIROCCO)*, pages 259–274, Barcelona, Spain, June 2001. Carlton Scientific.
14. Cristopher Moore and Alexander Russell. Quantum Walks on the Hypercube. In *Proceedings of the Sixth International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, volume 2483 of *Lecture Notes in Computer Science*, pages 164–178, Cambridge, MA, September 2002. Springer.
15. Mats Näslund and Alexander Russell. Extraction of optimally unbiased bits from a biased source. In *Proceedings of the 1998 IEEE Information Theory Workshop*, pages 90–91, Killarney, Ireland, June 1998.
16. Mats Näslund and Alexander Russell. Hard-core functions: Survey and new results. In *The Fifth Nordic Workshop on Secure IT Systems (NORDSEC)*, pages 305–322, 2000.
17. Alexander Russell. Necessary and sufficient conditions for collision-free hashing. In *Proceedings of Twelfth Annual IACR CRYPTO Conference*, volume 740 of *Lecture Notes in Computer Science*, pages 433–441, Berlin, 1992. Springer.
18. Alexander Russell, Michael Saks, and David Zuckerman. Lower bounds for leader election and collective coin-flipping in the perfect information model. In *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computation (STOC)*, pages 339–347, Atlanta, GA, May 1999. IEEE.
19. Alexander Russell and Hong Wang. How to fool an unbounded adversary with a short key. In *Proceedings of the 21st Annual Eurocrypt Conference (EUROCrypt 2002)*, volume 2332 of *Lecture Notes in Computer Science*, pages 133–145, Amsterdam, The Netherlands, 2002. Springer.
20. Alexander Russell and David Zuckerman. Perfect information leader election in  $\log^* n + O(1)$  rounds. In *Proceedings of the Thirty-ninth Annual Symposium on Foundations of Computer Science (FOCS)*, pages 576–583, Palo Alto, CA, November 1998. IEEE.

### Conference Articles (in published proceedings; to appear)

## Publications (continued)

1. Eric Allender, Sanjeev Arora, Michael Kearns, Cristopher Moore, and Alexander Russell. A Note on the Representational Incompatibility of Function Approximation and Factored Dynamics. In *Proceedings of the Sixteenth Annual Conference on Neural Information Processing Systems: Natural and Synthetic (NIPS)*, Vancouver, Canada, December, 2002.
2. S. Ravi Kumar and Alexander Russell. A note on the set systems used for broadcast encryption. To appear in *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, Baltimore, MD, January 2003. ACM.

### Short Conference Articles (in published proceedings)

1. Grzegorz Greg Malewicz, Alexander Russell, and Alex A. Shvartsman. Distributed Cooperation in the Absence of Communication. In *Proceedings of the Nineteenth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, page 339, Portland, OR, July, 2000. ACM.
2. Grzegorz Greg Malewicz, Alexander Russell, and Alex A. Shvartsman. Optimal Scheduling for Disconnected Cooperation. In *Proceedings of the Twentieth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 305–306, Newport, RI, August 2001. ACM.
3. Chryssis Georgiou, Alexander Russell, and Alex A. Shvartsman. Optimally Work-Competitive Scheduling for Cooperative Computing with Merging Groups. In *Proceedings of the Twenty-First Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 132, Monterey, CA, July, 2002. ACM.

## External Research Grants and Fellowships

- |                  |   |
|------------------|---|
| 9/2001 – 8/2006  | • “CAREER: Efficient Cryptography with Provable Security Guarantees,” National Science Foundation, \$305,000. PI: Alexander Russell.  |
| 9/2002 – 8/2005  | • “QuBIC: Quantum Monte-Carlo Algorithms and Quantum Circuit Complexity,” National Science Foundation, \$150,000, PI: Alexander Russell.  |
| 9/2002 – 8/2005  | • “ITR: Complexity-Theoretic Applications of Fourier Analysis,” National Science Foundation, \$125,000, PI: Alexander Russell.  |
| 9/2001 – 8/2006  | • “ITR: Communication and Data Sharing in Dynamic Distributed Systems,” National Science Foundation subcontract through the Massachusetts Institute of Technology, \$463,421. PI: Alex Shvartsman, coPI: Alexander Russell.   |
| 8/2002 – 7/2004  | • “SGER: Computational Topology for Surface Reconstruction,” National Science Foundation, \$100,000, PI: Tom Peters, coPIs: Kinetsu Abe, Alexander Russell.   |
| 9/2002 – 12/2002 | • MSRI Travel/Research Fellow, 2002 Special Semester on Quantum Computation, Mathematical Sciences Research Institute, \$4500.  |
| 7/2002           | • “Summer Research Conference: Graph Coloring and Symmetry,” American Mathematical Society and the Society for Industrial and Applied Mathematics, (conference dates: 7/21/02–7/25/02,) \$30,000. coPIs: Karen Collins, Daniel Krizanc (Wesleyan), Alexander Russell. |

## Teaching Experience

## Teaching Experience (continued)

- UNIVERSITY OF CONNECTICUT Storrs, CT  
*Undergraduate Courses: CSE228: Parallel Systems, fall 2000 (team taught with Prof. A. Shvartsman); CSE233: Programming Languages, spring 2000, fall 2001; CSE237: Automata Theory and Complexity, spring 2001, spring 2002; CSE268: Undergraduate Design Laboratory, fall 1999.*  
*Graduate Courses: CSE300, Modern Cryptography, spring 2000; CSE361: Computational Complexity of Parallel and Sequential Algorithms, fall 2000 (team taught with Prof. A. Shvartsman); CSE365: Automata and Complexity, fall 2001.*
- UNIVERSITY OF CHILE Santiago, Chile  
Summer workshop on zero-knowledge proof systems, cryptography, and secure distributed computation, summer 1997.
- ROYAL INSTITUTE OF TECHNOLOGY Stockholm, Sweden  
*The Probabilistic Method, spring 1997.*

## Personal Information

- Member ACM/SIGACT, AMS, MAA.