

Department of Computer Science and Engineering
University of Connecticut, U-2155
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

ALEXANDER C. RUSSELL

Professor

Professional Experience

As of 8/10	• <i>Professor</i> Department of Computer Science and Engineering	UNIVERSITY OF CONNECTICUT Storrs, CT
8/03–8/10	• <i>Associate Professor</i> Department of Computer Science and Engineering	UNIVERSITY OF CONNECTICUT Storrs, CT
8/99–8/03	• <i>Assistant Professor</i> Department of Computer Science and Engineering	UNIVERSITY OF CONNECTICUT Storrs, CT
9/97–8/99	• <i>Postdoctoral Fellow</i> Computer Science Division	UNIVERSITY OF CALIFORNIA, BERKELEY Berkeley, CA
	Joint position at: Department of Computer Science	UNIVERSITY OF TEXAS AT AUSTIN Austin, TX
9/96–8/97	• <i>Postdoctoral Fellow</i> Department of Computer Science and Numerical Analysis	ROYAL INSTITUTE OF TECHNOLOGY Stockholm, Sweden
As of 9/08	• <i>Senior Scientist, Member</i>	VOTING SYSTEMS SECURITY LLC Tolland, CT

Degrees

5/96	• Ph. D., Applied Mathematics	MASSACHUSETTS INSTITUTE OF TECHNOLOGY Cambridge, MA
1/93	• M. S., Computer Science	MASSACHUSETTS INSTITUTE OF TECHNOLOGY Cambridge, MA
5/91	• B. A. cum laude, Computer Science; B. A. cum laude, Mathematics	CORNELL UNIVERSITY Ithaca, NY

Honors and Professional Activities

Honors

- Member, Connecticut Academy of Science and Engineering; inducted in 2016.
- 2016 AsiaCrypt prize paper, “Ciphertexts: Clipping the Power of Kleptographic Attacks.” (Paper was also invited to the *Journal of Cryptology*.)
- National Science Foundation CAREER Award, 2001–2006.
- 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.
- University of Connecticut School of Engineering Junior Faculty Award 2003.
- University of Connecticut, Departmental Outstanding Faculty Award 2003.

Honors and Professional Activities (continued)

- National Science Foundation Graduate Fellow.
- Member Φ BK.

Professional Activities

- Associate Editor-in-Chief, *Theory of Computing*, 2005–2017.
- Principal investigator & co-director, *University of Connecticut Center for Voting Technology Research (VoTeR)*.
- Program Committee Member, *9th International Conference on Post-Quantum Cryptography (PQCrypto)*, 2018.
- Guest editor, *SIAM Journal on Computing*, special issue for FOCS 2014.
- Program Committee Track Chair, *17th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS)*, 2015.
- Program Committee Member, *IEEE Symposium on Foundations of Computer Science (FOCS)*, 2014.
- Program Committee Member, *18th. International Workshop on Randomization and Computation (RANDOM)*, 2014.
- Program Committee Member, *The 10th annual conference on Theory and Applications of Models of Computation*, 2013.
- Program Committee Member, *IEEE Symposium on Foundations of Computer Science (FOCS)*, 2012.
- Guest editor, *SIAM Journal on Computing*, special issue for STOC 2010.
- Program Committee Member, *ACM Symposium on the Theory of Computing (STOC)*, 2010.
- Program Committee Member, *The Twelfth Workshop on Quantum Information Processing*, 2009.
- Program Committee member, *The 2008 IEEE International Symposium on Network Computing and Applications*, 2008.
- Program Committee member, *The 2007 IEEE International Symposium on Network Computing and Applications*, 2007.
- Workshop Chair, *The 2006 IEEE International Symposium on Network Computing and Applications Workshop on Trusted Network Computing*, 2006.
- Program Committee Member, *ACM Symposium on Discrete Algorithms (SODA)*, 2006.
- Program Committee Member, *ACM Symposium on the Theory of Computing (STOC)*, 2004.
- Program Committee Member, *Latin American Informatics (LATIN)*, 2002.
- Conference Organizer, *AMS-IMS-SIAM Summer Research Conference: Graph Coloring and Symmetry*, July 21–25, 2002, South Hadley, Massachusetts.
- Local Arrangements vice-chair, *Twentieth ACM Symposium on Principles of Distributed Computing (PODC)*, 2001.
- Program Committee Member, *Scandinavian Workshop on Algorithm Theory (SWAT)*, 1998.
- Seminar Series Organizer, “Quantum Information Seminar Series,” organized with R. Côté and E. Donkor. Funded by UCRF, the School of Engineering, and the Department of Physics.

Publications

Journal Articles (published or in press)

1. Varsha Dani, Thomas P. Hayes, Cristopher Moore, and Alexander Russell. Codes, lower bounds, and phase transitions in the symmetric rendezvous problem. *Random Struct. Algorithms*, 49(4):742–765, 2016. DOI: [10.1002/rsa.20691](https://doi.org/10.1002/rsa.20691)
2. Cristopher Moore, Shachar Lovett, and Alexander Russell. Group representations that resist random sampling. *Random Structures and Algorithms*, 47(3):605–614, October 2015. DOI: [10.1002/rsa.20555](https://doi.org/10.1002/rsa.20555)
3. Cristopher Moore and Alexander Russell. Optimal ϵ -biased sets with just a little randomness. *SIAM Journal on Discrete Mathematics*, 29(3):1303–1311, 2015. DOI: [10.1137/130934490](https://doi.org/10.1137/130934490)

Publications (continued)

4. Chadi El-Kari, Alexander Russell, and Narasimha Shashidhar. Work-competitive scheduling on task dependency graphs. *Parallel Processing Letters*, 25(2):1550001, June 2015. DOI: [10 . 1142 / S0129626415500012](https://doi.org/10.1142/S0129626415500012)
5. Alexander Russell, Sudarshan Vasudevan, Bing Wang, Wei Zeng, Xian Chen, and Wei Wei. Neighbor discovery in wireless networks with multipacket reception. *IEEE Transactions on Parallel and Distributed Systems*, 26(7):1984–1998, July 2015. DOI: [10 . 1109/TPDS . 2014 . 2321157](https://doi.org/10.1109/TPDS.2014.2321157)
6. Hari Krovi and Alexander Russell. Quantum Fourier transforms and the complexity of link invariants for quantum doubles of finite groups. *Communications in Mathematical Physics*, 334(2):743–777, 2015. DOI: [10 . 1007/s00220-014-2285-5](https://doi.org/10.1007/s00220-014-2285-5)
7. Cristopher Moore and Alexander Russell. Approximate representations, approximate homomorphisms, and low-dimensional embeddings of groups. *SIAM Journal on Discrete Mathematics*, 29(1):182–197, 2015. DOI: [10 . 1137/140958578](https://doi.org/10.1137/140958578)
8. Seda Davtyan, Kishori M. Konwar, Alexander Russell, and Alexander A. Shvartsman. Dealing with un-dependable workers in decentralized network supercomputing. *Theoretical Computer Science*, 561, Part B:96–112, 2015. DOI: [10 . 1016/j . tcs . 2014 . 10 . 015](https://doi.org/10.1016/j.tcs.2014.10.015). Special Issue on Distributed Computing and Networking
9. Hang Dinh, Cristopher Moore, and Alexander Russell. Limitations of single coset states and quantum algorithms for code equivalence. *Quantum Information and Computation*, 15(3&4):260–294, 2015. QIC: [v15n34](https://arxiv.org/abs/1503.034)
10. Kyung-Min Chung, Frederick W. Kolling IV, Mathew D. Gajdosik, Steven Burger, Alexander Russell, and Craig E. Nelson. Single cell analysis reveals the stochastic phase of reprogramming to pluripotency is an ordered probabilistic process. *PLoS ONE*, 9(4):e95304, 2014. DOI: [10 . 1371 / journal . pone . 0095304](https://doi.org/10.1371/journal.pone.0095304)
11. Sixia Chen and Alexander Russell. Online metric tracking and smoothing. *Algorithmica*, 68(1):133–151, 2014. DOI: [10 . 1007/s00453-012-9669-8](https://doi.org/10.1007/s00453-012-9669-8)
12. Russell Impagliazzo, Cristopher Moore, and Alexander Russell. An entropic proof of Chang’s inequality. *SIAM Journal on Discrete Mathematics*, 28(1):173–176, 2014. DOI: [10 . 1137/120877982](https://doi.org/10.1137/120877982)
13. Aggelos Kiayias, Yona Raekow, Alexander Russell, and Shashidhar Narasimha. A one-time stegosystem and its application to efficient covert communication. *Journal of Cryptology*, 27(1):23–44, 2014. DOI: [10 . 1007/s00145-012-9135-4](https://doi.org/10.1007/s00145-012-9135-4)
14. Hang Dinh, Hieu Dinh, Laurent Michel, and Alexander Russell. The time complexity of A^* with approximate heuristics on multiple-solution search spaces. *Journal of AI Research*, 45:685–729, 2012. DOI: [10 . 1613/jair . 3779](https://doi.org/10.1613/jair.3779)
15. Cristopher Moore and Alexander Russell. Approximating the permanent via nonabelian determinants. *SIAM Journal on Computing*, 41(2):332–355, 2012. DOI: [10 . 1137/100806709](https://doi.org/10.1137/100806709)
16. Scott Aaronson, François LeGall, Alexander Russell, and Seiichiro Tani. The one-way communication complexity of subgroup membership. *Chicago Journal of Theoretical Computer Science*, 2011(6):1–17, 2011. DOI: [10 . 4086/cjtcs . 2011 . 006](https://doi.org/10.4086/cjtcs.2011.006)
17. Cristopher Moore and Alexander Russell. A graph integral formulation of the circuit partition polynomial. *Combinatorics, Probability & Computing*, 20(6):911–920, 2011. DOI: [10 . 1017/S0963548311000393](https://doi.org/10.1017/S0963548311000393)
18. Gorjan Alagic and Alexander Russell. Spectral concentration of positive functions on compact groups. *Journal of Fourier Analysis and Applications*, 17(3):355–373, 2011. DOI: [10 . 1007 / s00041 - 011 - 9174-5](https://doi.org/10.1007/s00041-011-9174-5)
19. Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. *Journal of the ACM*, 57(6):34:1–34:33, November 2010. DOI: [10 . 1145/1857914 . 1857918](https://doi.org/10.1145/1857914.1857918)
20. Hang Dinh and Alexander Russell. Quantum and randomized lower bounds for local search on vertex-transitive graphs. *Quantum Information and Computation*, 10(7&8):636–652, 2010. QIC: [v10n78](https://arxiv.org/abs/1007.078)
21. Aaron Denney, Cristopher Moore, and Alexander Russell. Finding conjugate stabilizer subgroups in PSL and related groups. *Quantum Information and Computation*, 10(3&4):282–291, 2010. QIC: [v10n34](https://arxiv.org/abs/1003.034)

Publications (continued)

22. Cristopher Moore, Alexander Russell, and Piotr Śniady. On the impossibility of a quantum sieve algorithm for graph isomorphism. *SIAM Journal on Computing*, 39(6):2377–2396, April 2010. ISSN: 0097-5397. DOI: [10.1137/080724101](https://doi.org/10.1137/080724101)
23. Gorjan Alagic, Cristopher Moore, and Alexander Russell. Quantum algorithms for Simon’s problem over general groups. *ACM Transactions on Algorithms*, 6(1):19:1–19:15, 1, December 2009. ISSN: 1549-6325. DOI: [10.1145/16444015.1644034](https://doi.org/10.1145/16444015.1644034)
24. Tigran Antonyan, Seda Davtyan, Sotirios Kentros, Aggelos Kiayias, Laurent Michel, Nicolas Nicolaou, Alexander Russell, and Alexander A. Shvartsman. State-wide elections, optical scan voting systems, and the pursuit of integrity. *IEEE Transactions on Information Forensics and Security*, 4(4):597–610, December 2009. ISSN: 1556-6013. DOI: [10.1109/TIFS.2009.2033232](https://doi.org/10.1109/TIFS.2009.2033232)
25. Gorjan Alagic and Alexander Russell. Uncertainty principles for compact groups. *Illinois Journal of Mathematics*, 52(4):1315–1324, 2008. URL: <http://projecteuclid.org/euclid.ijm/1258554365>
26. K. E. Jordan, Lance E. Miller, E. L. F. Moore, T. J. Peters, and Alexander Russell. Modeling time and topology for animation and visualization with examples on parametric geometry. *Theoretical Computer Science*, 405(1-2):41–49, October 2008. ISSN: 0304-3975. DOI: [10.1016/j.tcs.2008.06.023](https://doi.org/10.1016/j.tcs.2008.06.023). ACM: [1410885.1410909](https://doi.org/10.1145/1410885.1410909)
27. Cristopher Moore, Alexander Russell, and Leonard J. Schulman. The symmetric group defies strong Fourier sampling. *SIAM Journal on Computing*, 37(6):1842–1864, March 2008. DOI: [10.1137/050644896](https://doi.org/10.1137/050644896). ACM: [1362744.1362749](https://doi.org/10.1145/1362744.1362749)
28. Cristopher Moore and Alexander Russell. For distinguishing conjugate hidden subgroups, the pretty good measurement is as good as it gets. *Quantum Information and Computation*, 7(8):752–765, 2007. QIC: [v7n8](https://doi.org/10.1145/1226616.1226619)
29. Cristopher Moore, Daniel Rockmore, Alexander Russell, and Leonard J. Schulman. The power of strong Fourier sampling: Quantum algorithms for affine groups and hidden shifts. *SIAM Journal on Computing*, 37(3):938–958, June 2007. DOI: [10.1137/S0097539705447177](https://doi.org/10.1137/S0097539705447177). ACM: [1328865.1328877](https://doi.org/10.1145/1328865.1328877)
30. Chryssis Georgiou, Alexander Russell, and Alexander A. Shvartsman. Failure-sensitive analysis of parallel algorithms with controlled memory access concurrency. *Parallel Processing Letters*, 17(2):153–168, 2007. DOI: [10.1142/S0129626407002946](https://doi.org/10.1142/S0129626407002946)
31. Kinetsu Abe, Justin Bisceglia, David Ferguson, Thomas Peters, Alexander Russell, and Takis Sakkalis. Computational topology for isotopic surface reconstruction. *Theoretical Computer Science*, 365(3):184–198, November 2006. DOI: [10.1016/j.tcs.2006.07.062](https://doi.org/10.1016/j.tcs.2006.07.062). ACM: [1226616.1226619](https://doi.org/10.1145/1226616.1226619)
32. Grzegorz Malewicz, Alexander Russell, and Alexander Shvartsman. Distributed scheduling for disconnected cooperation. *Distributed Computing*, 18(6):409–420, 6, 2006. DOI: [10.1007/s00446-005-0149-0](https://doi.org/10.1007/s00446-005-0149-0)
33. Robin Côté, Alexander Russell, Edward E. Eyler, and Phillip L. Gould. Quantum random walk with Rydberg atoms in an optical lattice. *New Journal of Physics*, 8(8):156, 2006. DOI: [10.1088/1367-2630/8/8/156](https://doi.org/10.1088/1367-2630/8/8/156). URL: <http://stacks.iop.org/1367-2630/8/i=8/a=156>
34. Alexander Russell and Hong Wang. How to fool an unbounded adversary with a short key. *IEEE Transactions on Information Theory*, 52(3):1130–1140, March 2006. DOI: [10.1109/TIT.2005.864438](https://doi.org/10.1109/TIT.2005.864438)
35. Gorjan Alagic and Alexander Russell. Decoherence in quantum walks on the hypercube. *Phys. Rev. A*, 72(6):062304, December 2005. DOI: [10.1103/PhysRevA.72.062304](https://doi.org/10.1103/PhysRevA.72.062304)
36. Antonio Fernández, Chryssis Georgiou, Alexander Russell, and Alex A. Shvartsman. The Do-All problem with Byzantine processor failures. *Theoretical Computer Science*, 333(3):433–454, March 2005. DOI: [10.1016/j.tcs.2004.06.034](https://doi.org/10.1016/j.tcs.2004.06.034). ACM: [1195997.1196005](https://doi.org/10.1145/1195997.1196005)
37. Chryssis Georgiou, Alexander Russell, and Alexander A. Shvartsman. Work-competitive scheduling for cooperative computing with dynamic groups. *SIAM Journal on Computing*, 34(4):848–862, April 2005. DOI: [10.1137/S0097539704440442](https://doi.org/10.1137/S0097539704440442). ACM: [1064628.1064938](https://doi.org/10.1145/1064628.1064938)
38. Lars Engebretsen, Jonas Holmerin, and Alexander Russell. Inapproximability results for equations over finite groups. *Theoretical Computer Science*, 312(1):17–45, January 2004. DOI: [10.1016/S0304-3975\(03\)00401-8](https://doi.org/10.1016/S0304-3975(03)00401-8). ACM: [985557.985560](https://doi.org/10.1145/985557.985560). Special issue for ICALP 2002

Publications (continued)

39. Chryssis Georgiou, Alexander Russell, and Alex A. Shvartsman. Analysis of instant and total memory access concurrency in robust parallel algorithms. *Studia Informatica Universalis*, 3(2):125–150, 2004
40. Marcos Kiwi and Alexander Russell. The Chilean highway problem. *Theoretical Computer Science*, 326(1-3):329–342, October 2004. doi: [10.1016/j.tcs.2004.07.030](https://doi.org/10.1016/j.tcs.2004.07.030). ACM: 1045979.1045995
41. Cristopher Moore, Daniel Rockmore, and Alexander Russell. Generic quantum Fourier transforms. *ACM Transactions on Algorithms*, 2(4):707–723, October 2006. doi: [10.1145/1198513.1198525](https://doi.org/10.1145/1198513.1198525). Special issue for SODA 2004
42. Zeph Landau and Alexander Russell. Random Cayley graphs are expanders: A simple proof of the Alon-Roichman theorem. *Electronic Journal of Combinatorics*, 11(1):R62, 2004. URL: www.combinatorics.org/Volume_11/PDF/v11i1r62.pdf
43. Chryssis Georgiou, Alexander Russell, and Alex A. Shvartsman. The complexity of synchronous iterative Do-All with crashes. *Distributed Computing*, 17(1):47–63, February 2004. doi: [10.1007/s00446-003-0099-3](https://doi.org/10.1007/s00446-003-0099-3). ACM: 1018448.1018452
44. Alexander Russell and Igor E. Shparlinski. Classical and quantum function reconstruction via character evaluation. *Journal of Complexity*, 20(2-3):404–422, April 2004. doi: [10.1016/j.jco.2003.08.019](https://doi.org/10.1016/j.jco.2003.08.019). ACM: 998277.998295
45. Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. The hidden subgroup problem and quantum computation using group representations. *SIAM Journal on Computing*, 32(4):916–934, 2003. doi: [10.1137/S009753970139450X](https://doi.org/10.1137/S009753970139450X)
46. 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):1645–1662, 2002. doi: [10.1137/S0097539700376007](https://doi.org/10.1137/S0097539700376007). Special issue for STOC 1999
47. Nina Amenta, Thomas J. Peters, and Alexander Russell. Computational topology: Ambient isotopic approximation of 2-manifolds. *Theoretical Computer Science*, 305(1-3):3–15, August 2003. doi: [10.1016/S0304-3975\(02\)00691-6](https://doi.org/10.1016/S0304-3975(02)00691-6). ACM: 945266.945268
48. Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. *Information and Computation*, 178(1):253–262, October 2002. doi: [10.1016/S0890-5401\(02\)93173-1](https://doi.org/10.1016/S0890-5401(02)93173-1). ACM: 603645.603656. URL: <http://portal.acm.org/citation.cfm?id=603645.603656>
49. Alexander Russell and David Zuckerman. Perfect information leader election in $\log^* n + O(1)$ rounds. *Journal of Computer and System Sciences*, 63(4):612–626, December 2001. doi: [10.1006/jcss.2001.1776](https://doi.org/10.1006/jcss.2001.1776). ACM: 569473.569479. Special issue for FOCS 1998
50. Mikael Goldmann, Mats Näslund, and Alexander Russell. Complexity bounds on general hard-core predicates. *Journal of Cryptology*, 14(3):177–195, 2001. doi: [10.1007/s00145-001-0007-6](https://doi.org/10.1007/s00145-001-0007-6)
51. Mikael Goldmann, Alexander Russell, and Denis Thérien. An ergodic theorem for read-once non-uniform deterministic finite automata. *Information Processing Letters*, 73(1-2):23–28, January 2000. doi: [10.1016/S0020-0190\(99\)00162-3](https://doi.org/10.1016/S0020-0190(99)00162-3)
52. Mats Näslund and Alexander Russell. Extraction of optimally unbiased bits from a biased source. *IEEE Transactions on Information Theory*, 46(3):1093–1103, 2000. doi: [10.1109/18.841191](https://doi.org/10.1109/18.841191)
53. Alexander Russell. An easy reduction of an isoperimetric inequality on the sphere to extremal set theory. *The American Mathematical Monthly*, 107(1):57–59, January 2000. doi: [10.2307/2589379](https://doi.org/10.2307/2589379). JSTOR: 2589379
54. Marcos Kiwi, Carsten Lund, Alexander Russell, Daniel Spielman, and Ravi Sundaram. Alternation in interaction. *Computational Complexity*, 9(3-4):202–246, 2000. doi: [10.1007/PL00001607](https://doi.org/10.1007/PL00001607)
55. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Approximating Latin square extensions. *Algorithmica*, 24(2):128–138, 1999. doi: [10.1007/PL00009274](https://doi.org/10.1007/PL00009274)
56. Alexander Russell and Ravi Sundaram. A note on the asymptotics and computational complexity of graph distinguishability. *Electronic Journal of Combinatorics*, 5(1):R23, 1998. URL: http://www.combinatorics.org/Volume_5/Abstracts/v5i1r23.html

Publications (continued)

57. Alexander Russell and Ravi Sundaram. Symmetric alternation captures BPP. *Computational Complexity*, 7(2):152–162, November 1998. DOI: [10.1007/s000370050007](https://doi.org/10.1007/s000370050007). ACM: 306576.306608
58. Michael Klugerman, Alexander Russell, and Ravi Sundaram. On embedding complete graphs into hypercubes. *Discrete Mathematics*, 186(1-3):289–293, May 1998. DOI: [10.1016/S0012-365X\(97\)00239-2](https://doi.org/10.1016/S0012-365X(97)00239-2). ACM: 287396.287535
59. S. Ravi Kumar, Rina Panigrahy, Alexander Russell, and Ravi Sundaram. A note on optical routing on trees. *Information Processing Letters*, 62(6):295–300, June 1997. DOI: [10.1016/S0020-0190\(97\)00077-X](https://doi.org/10.1016/S0020-0190(97)00077-X). ACM: 261591.261594
60. Alexander Russell. Necessary and sufficient conditions for collision-free hashing. *Journal of Cryptology*, 8(2):87–99, 1995. DOI: [10.1007/BF00190757](https://doi.org/10.1007/BF00190757)
61. Alexander Russell and Ravi Sundaram. The relativized relationship between probabilistically checkable debate systems, IP and PSPACE. *Information Processing Letters*, 53(2):61–68, January 1995. DOI: [10.1016/0020-0190\(94\)00185-2](https://doi.org/10.1016/0020-0190(94)00185-2)
62. Alberto Segre, Charles Elkan, and Alexander Russell. A critical look at experimental evaluations of EBL. *Machine Learning*, 6(2):183–195, March 1991. DOI: [10.1023/A:1022658420943](https://doi.org/10.1023/A:1022658420943). ACM: 104724.104733

Articles in Periodicals

1. Gorjan Alagic and Alexander Russell. Quantum computing and the hunt for hidden symmetry. *Bulletin of the EATCS*. 93:53–75, 2007.
2. 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. K. E. Jordan, L. E. Miller, T. J. Peters, and Alexander Russell. Geometric Topology and Visualizing 1-Manifolds, in *Topological Methods in Data Analysis and Visualization*, V. Pascucci, X. Tricoche, H. Hagen, and J. Tierny, Eds., pages 1–13, 2011. Springer. Kishori Konwar, Ion Mandoiu, Alexander Russell, and Alex A. Shvartsman. Algorithms for multiplex PCR primer set selection with amplification length constraints. In I. Mandoiu and A. Zelikovsky, editors, *Bioinformatics Algorithms: Techniques and Applications*, pages 241–258. Wiley Interscience, 2008.
2. Lance Edward Miller, Edward L. F. Moore, Thomas J. Peters, and Alexander Russell. Topological Neighborhoods for Spline Curves: Practice & Theory. In *Reliable Implementation of Real Number Algorithms: Theory and Practice*, volume 5045 of Lecture Notes in Computer Science, pages 149–161. Springer, 2008.
3. Alexander Russell and Alex A. Shvartsman. Distributed Computation Meets Design Theory: Local Scheduling for Disconnected Cooperation. In G. Paun, G. Rozenberg, and A. Salomaa, editors, *Current Trends in Computer Science: The Challenge of a New Century, Volume 1: Algorithms and Complexity*, pages 315–336. World Scientific, 2004.
4. 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.
5. 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.

Publications (continued)

Conference Articles (in published proceedings)

1. Bernardo David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. To appear, *Eurocrypt 2018*.
2. Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Generic semantic security against a kleptographic adversary. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 907–922. ACM, 2017. doi: [10.1145/3133956.3133993](https://doi.org/10.1145/3133956.3133993).
3. Bochao Shen, Ravi Sundaram, Alexander Russell, Srinivas Aiyar, Karan Gupta, Abhinay Nagpal, Aditya Ramesh, and Himanshu Shukla. High availability for VM placement and a stochastic model for multiple knapsack. In *26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–9. IEEE, 2017. doi: [10.1109/ICCCN.2017.8038384](https://doi.org/10.1109/ICCCN.2017.8038384)
4. Chaoqun Yue, Shweta Ware, Reynaldo Morillo, Jin Lu, Chao Shang, Jinbo Bi, Jayesh Kamath, Alexander Russell, Athanasios Bamis and Bing Wang. Fusing Location Data for Depression Prediction. 2017 IEEE Ubiquitous Intelligence and Computing (UIC), 2017.
5. Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Katz and Hovav Shacham, editors, *37th Annual International Cryptology Conference (CRYPTO)*, volume 10401 of *Lecture Notes in Computer Science*, pages 357–388. Springer, 2017. doi: [10.1007/978-3-319-63688-7_12](https://doi.org/10.1007/978-3-319-63688-7_12).
6. Gorjan Alagic and Alexander Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, volume 10212 of *Lecture Notes in Computer Science*, pages 65–93, 2017. doi: [10.1007/978-3-319-56617-7_3](https://doi.org/10.1007/978-3-319-56617-7_3). Additionally presented at Theory of Quantum Computation, Communication and Cryptography (TQC) 2017.
7. Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Cliptography: Clipping the power of kleptographic attacks. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *22nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)*, volume 10032 of *Lecture Notes in Computer Science*, pages 34–64, Berlin, Heidelberg. Springer, 2016. doi: [10.1007/978-3-662-53890-6_2](https://doi.org/10.1007/978-3-662-53890-6_2). (AsiaCrypt prize paper.)
8. Asma Ahmad Farhan, Chaoqun Yue, Reynaldo Morillo, Shweta Ware, Jin Lu, Jinbo Bi, Jayesh Kamath, Alexander Russell, Athanasios Bamis, and Bing Wang. Behavior vs. introspection: Refining prediction of clinical depression via smartphone sensing data. In *2016 IEEE Wireless Health (WH)*, pages 30–37. IEEE Computer Society, 2016. doi: [10.1109/WH.2016.7764553](https://doi.org/10.1109/WH.2016.7764553)
9. Aggelos Kiayias, Ozgur Oksuz, Alexander Russell, Qiang Tang, and Bing Wang. Efficient encrypted keyword search for multi-user data sharing. In Ioannis G. Askoxylakis, Sotiris Ioannidis, Sokratis K. Katsikas, and Catherine A. Meadows, editors, *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS)*, volume 9878 of *Lecture Notes in Computer Science*, pages 173–195. Springer, 2016. doi: [10.1007/978-3-319-45744-4_9](https://doi.org/10.1007/978-3-319-45744-4_9)
10. Asma Ahmad Farhan, Jin Lu, Jinbo Bi, Alexander Russell, Bing Wang, and Athanasios Bamis. Multi-view bi-clustering to identify smartphone sensing features indicative of depression. In *IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, pages 264–273. IEEE Computer Society, June 2016. doi: [10.1109/CHASE.2016.27](https://doi.org/10.1109/CHASE.2016.27)
11. Sixia Chen, Matthew Dippel, Alexander Russell, Abhishek Samanta, and Ravi Sundaram. Markovian hitters and the complexity of blind rendezvous. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 610–619. ACM Press, 2016. doi: [10.1137/1.9781611974331.ch45](https://doi.org/10.1137/1.9781611974331.ch45)

Publications (continued)

12. Sixia Chen, Alexander Russell, Ruofan Jin, Yanyuan Qin, Bing Wang, and Sudarshan Vasudevan. Asynchronous neighbor discovery on duty-cycled mobile devices: Integer and non-integer schedules. In Sherman X. Shen, Youxian Sun, Jiming Chen, Junshan Zhang, and Gil Zussman, editors, *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 47–56. ACM Press, 2015. doi: [10.1145/2746285.2746297](https://doi.org/10.1145/2746285.2746297).
13. Sotirios Kentros, Chadi Kari, Aggelos Kiayias, and Alexander Russell. Asynchronous adaptive task allocation. In *35th IEEE International Conference on Distributed Computing Systems (ICDCS)*, pages 83–92. IEEE Computer Society, 2015. doi: [10.1109/ICDCS.2015.17](https://doi.org/10.1109/ICDCS.2015.17)
14. Sixia Chen, Alexander Russell, Abhishek Samanta, and Ravi Sundaram. Deterministic blind rendezvous in cognitive radio networks. In *IEEE 34th International Conference on Distributed Computing Systems (ICDCS)*, pages 358–367. IEEE Computer Society, 2014. doi: [10.1109/ICDCS.2014.44](https://doi.org/10.1109/ICDCS.2014.44)
15. Sixia Chen, Christopher Moore, and Alexander Russell. Small-bias sets for nonabelian groups: Derandomizations of the Alon-Roichman theorem. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013*, volume 8096 of *Lecture Notes in Computer Science*, pages 436–451. Springer, 2013. doi: [10.1007/978-3-642-40328-6_31](https://doi.org/10.1007/978-3-642-40328-6_31)
16. Seda Davtyan, Kishori M. Konwar, Alexander Russell, and Alexander A. Shvartsman. Dealing with undependable workers in decentralized network supercomputing. In *Proceedings of the 14th International Conference on Distributed Computing and Networking (ICDCN)*, volume 7730 of *Lecture Notes in Computer Science*, pages 27–41. Springer, 2013. doi: [10.1007/978-3-642-35668-1](https://doi.org/10.1007/978-3-642-35668-1)
17. Russell J. Jancewicz, Aggelos Kiayias, Laurent D. Michel, Alexander Russell, and Alexander A. Shvartsman. Malicious takeover of voting systems: Arbitrary code execution on optical scan voting terminals. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing (SAC)*, pages 1816–1823. ACM, 2013. doi: [10.1145/2480362.2480702](https://doi.org/10.1145/2480362.2480702). ACM: 2480362.2480702
18. Aggelos Kiayias, Alexander Russell, and Shashidhar Narasimha. Key-efficient steganography. In *Proceedings of the 14th International Conference on Information Hiding (IH)*, volume 7692 of *Lecture Notes in Computer Science*, pages 142–159. Springer, 2013. doi: [10.1007/978-3-642-36373-3_10](https://doi.org/10.1007/978-3-642-36373-3_10)
19. Seda Davtyan, Aggelos Kiayias, Laurent Michel, Alexander Russell, and Alexander A. Shvartsman. Integrity of electronic voting systems: Fallacious use of cryptography. In Sascha Ossowski and Paola Lecca, editors, *Proceedings of the 27th Symposium on Applied Computing (SAC)*, pages 1486–1493. ACM, 2012. doi: [10.1145/2245276.2232013](https://doi.org/10.1145/2245276.2232013)
20. Chryssis Georgiou, Nicolas C. Nicolaou, Alexander Russell, and Alexander A. Shvartsman. Towards feasible implementations of low-latency multi-writer atomic registers. In *Proceedings of The Tenth IEEE International Symposium on Networking Computing and Applications (NCA)*, pages 75–82. IEEE Computer Society, 2011. doi: [10.1109/NCA.2011.18](https://doi.org/10.1109/NCA.2011.18).
21. Hang Dinh, Christopher Moore, and Alexander Russell. McEliece and Niederreiter cryptosystems that resist quantum fourier sampling attacks. In Phillip Rogaway, editor, *31st Annual Cryptology Conference (CRYPTO)*, volume 6841 of *Lecture Notes in Computer Science*, pages 761–779. Springer, 2011. doi: [10.1007/978-3-642-22792-9_43](https://doi.org/10.1007/978-3-642-22792-9_43).
22. Chadi Kari, Yoo-Ah Kim, and Alexander Russell. Data migration in heterogeneous storage systems. In *International Conference on Distributed Computing Systems (ICDCS)*, pages 143–150. IEEE Computer Society, 2011. doi: [10.1109/ICDCS.2011.46](https://doi.org/10.1109/ICDCS.2011.46).
23. Wei Zeng, Sudarshan Vasudevan, Xian Chen, Bing Wang, Alexander Russell, and Wei Wei. Neighbor discovery in wireless networks with multipacket reception. In *Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, page 3. ACM, 2011. doi: [10.1145/2107502.2107506](https://doi.org/10.1145/2107502.2107506).

Publications (continued)

24. Sergey Bravyi, Cristopher Moore, and Alexander Russell. Bounds on the quantum satisfiability threshold. In Andrew Chi-Chih Yao, editor, *Proceedings of Innovations in Computer Science (ICS)*, pages 482–489. Tsinghua University Press, 2010. URL: <http://conference.itcs.tsinghua.edu.cn/ICS2010/content/papers/37.html>.
25. Hang Dinh and Alexander Russell. Quantum and randomized lower bounds for local search on vertex-transitive graphs. In Ashish Goel, Klaus Jansen, José D. P. Rolim, and Ronitt Rubinfeld, editors, *Proceedings of the 11th international workshop, APPROX 2008, and 12th international workshop, RANDOM 2008 on Approximation, Randomization and Combinatorial Optimization: Algorithms and Techniques*, volume 5171 of *Lecture Notes in Computer Science*, pages 385–401. Springer, 2008. DOI: [10.1007/978-3-540-85363-3_31](https://doi.org/10.1007/978-3-540-85363-3_31).
26. Seda Davtyan, Sotiris Kentros, Aggelos Kiayias, Laurent Michel, Nicolas C. Nicolaou, Alexander Russell, Andrew See, Narasimha Shashidhar, and Alexander A. Shvartsman. Pre-Election Testing and Post-Election Audit of Optical Scan Voting Terminal Memory Cards. In *Proceedings 2008 USENIX/ACCURATE Electronic Voting Workshop (EVT'08)*.
27. Chadi Kari, Alexander Russell, and Narasimha Shashidhar. Randomized Work-Competitive Scheduling for Cooperative Computing on k -partite Task Graphs. In *Proceedings of The Seventh IEEE International Symposium on Networking Computing and Applications (NCA)*, pages 267–270, 2008. IEEE.
28. Gorjan Alagic, Cristopher Moore, and Alexander Russell. Quantum algorithms for Simon’s problem over general groups. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1217–1224, New Orleans, LA, January 7-9, 2007. ACM.
29. Hang Dinh, Alexander Russell, and Yuan Su. On the value of good advice: The complexity of A^* search with accurate heuristics. In *Proceedings of the Twenty-Second Conference on Artificial Intelligence (AAAI)*, pages 1140–1145, Vancouver, British Columbia, July 2007.
30. Chadi Kari, Yoo-Ah Kim, Seungjoon Lee, Alexander Russell and Min-ho Shin. Soft Edge Coloring. In *Proceedings of the 10th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems (APPROX)*, volume 4627 of *Lecture Notes in Computer Science*, pages 189–203, Princeton, New Jersey, August 2007, Springer.
31. Aggelos Kiayias, Laurent Michel, Alexander Russell, Narasimha Shashidhar, Andy See, Alex Shvartsman and Seda Davtyan. An authentication and ballot attack against an optical scan voting terminal. In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)*, Boston, MA, August 6, 2007.
32. Aggelos Kiayias, Laurent Michel, Alexander Russell, Narasimha Shashidhar, Andy See, Alex Shvartsman and Seda Davtyan, Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting. In *Proceedings of Annual Computer Security Application Conference (ACSAC)*, Miami Beach, Florida, December 10-14, 2007.
33. Cristopher Moore, Alexander Russell, and Piotr Śniady. On the impossibility of a quantum sieve algorithm for graph isomorphism. In *Proceedings of the thirty-ninth annual ACM symposium on theory of computing (STOC)*, pages 536–545, San Diego, CA, 2007.
34. M.T. Hajiaghayi, K. Jain, L.C. Lau, I.I. Măndoiu, A.C. Russell, and V.V. Vazirani. The minimum multicolored subgraph problem in haplotyping and PCR primer set selection. In *Proceedings of the 6th International Conference on Computational Science (ICCS 2006)*, volume 3992 of *Lecture Notes in Computer Science*, pages 758–766. Springer, 2006.
35. Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. In *Proceedings of the 38th ACM Symposium on Theory of Computing (STOC)*, pages 604–617, May 21–23, 2006, Seattle, WA.
36. Sean Hallgren, Alexander Russell, and Igor Shparlinski. Quantum Noisy Rational Functional Reconstruction. In *Proceedings of the Eleventh Annual Computing and Combinatorics Conference (COCOON)*, volume 3595 of *Lecture Notes in Computer Science*, pages 420–429. Springer, 2005.

Publications (continued)

37. Kinetsu Abe, Justin Bisceglia, Thomas Peters, Alexander Russell, and Takis Sakkalis. Computational topology for reconstruction of surfaces with boundary: integrating experiments and theory. In *Proceedings of the IEEE International Conference on Shape Modeling and Applications 2005 (SMI' 05)*, pp. 290–299, Cambridge, MA, 2005.
38. Aggelos Kiayias, Yona Raekow, and Alexander Russell. Efficient steganography with provable security guarantees. In M. Barni, J. Herrera Joancomartí, S. Katzenbeisser, and F. Pérez-González, editors, *Proceedings of the Seventh International Workshop on Information Hiding (IH)*, volume 3727 of *Lecture Notes in Computer Science*, pages 118–130. Springer, 2005. DOI: [10.1007/11558859_10](https://doi.org/10.1007/11558859_10)
39. Kishori Konwar, Ion Măndoiu, Alexander Russell, and Alex Shvartsman. Improved Algorithms for Multiplex PCR Primer Set Selection with Amplification Length Constraints. In *Proceedings of the 3rd Asia-Pacific Bioinformatics Conference (APBC)*, pp. 41–50. Imperial College Press, 2005.
40. Cristopher Moore, Alexander Russell, and Leonard Schulman. The symmetric group defies Fourier sampling. In *Proceedings of the 46th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 479–488, Pittsburgh, PA, 2005.
41. Cristopher Moore, Daniel Rockmore, and Alexander Russell. Generic quantum Fourier transforms. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 778–787, New Orleans, LA, January 11-13 2004. ACM.
42. Cristopher Moore, Daniel Rockmore, Alexander Russell, and Leonard Schulman. The power of basis selection in Fourier sampling: The hidden subgroup problem in affine groups. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1113–1122, New Orleans, LA, January 11-13 2004. ACM.
43. Chrysis Georgiou, Alexander Russell, and Alex Shvartsman. Work-Competitive Scheduling for Cooperative Computing with Dynamic Groups. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on the Theory of Computing (STOC)*, pages 294–304, San Diego, California, 9–11 June 2003. ACM.
44. Chrysis Georgiou, Alexander Russell, and Alex Shvartsman. Distributed Cooperation and Adversity: Complexity Trade-Offs. In *Proceedings of Principles of Computing and Knowledge: Paris C. Kanellakis Memorial Workshop (PK50)*, pages 60–71, San Diego, California, 9–11 June 2003. ACM.
45. S. Ravi Kumar and Alexander Russell. A note on the set systems used for broadcast encryption. In the *Proceedings of the Fourteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 470–471, Baltimore, MD, January 2003. ACM.
46. 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.
47. 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.
48. 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.
49. Alexander Russell and Hong Wang. How to fool an unbounded adversary with a short key. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques*, volume 2332 of *Lecture Notes in Computer Science*, pages 133–148. Springer, 2002. ISBN: 3-540-43553-0. DOI: [10.1007/3-540-46035-7_9](https://doi.org/10.1007/3-540-46035-7_9). ACM: [647087.757013](https://doi.org/10.1145/647087.757013)
50. Chrysis Georgiou, Alexander Russell, and Alex 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.

Publications (continued)

51. 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.
52. Greg Grzegorz Malewicz, Alexander Russell, and Alex Allister Shvartsman. Optimal scheduling for disconnected cooperation without communication. In *Proceedings of the Eighth Annual Colloquium on Structural Information and Communication Complexity (SIROCCO)*, pages 259–274, Barcelona, Spain, June 2001. Carlton Scientific.
53. Chryssis Georgiou, Alexander Russell, and Alexander A. Shvartsman. The complexity of distributed cooperation in the presence of failures. In Franck Butelle, editor, *Proceedings of the 4th International Conference on Principles of Distributed Systems (OPODIS)*, Studia Informatica Universalis, pages 245–264. Suger, 2000
54. Mikael Goldmann and Alexander Russell. Spectral bounds on general hard core predicates. In *Proceedings of the 17th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, number 1770 in Lecture Notes in Computer Science, pages 614–625. Springer, 2000. ACM: [646514.695810](#)
55. 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, New York, NY, USA. ACM, 2000. DOI: [10.1145/335305.335392](#). ACM: [335392](#)
56. Grzegorz Greg Malewicz, Alexander Russell, and Alexander A. Shvartsman. Distributed cooperation during the absence of communication. In *Proceedings of the 14th International Conference on Distributed Computing (DISC)*, volume 1914 of *Lecture Notes in Computer Science*, pages 119–133. Springer, 2000. ACM: [675959](#)
57. Mats Näslund and Alexander Russell. Hard-core functions: Survey and new results. In *Proceedings of the Fifth Nordic Workshop on Secure IT Systems (NORDSEC)*, pages 305–322, 2000
58. Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. In *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity*, pages 80–86. IEEE Computer Society, 1999. ACM: [792764.793400](#)
59. 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 Computing (STOC)*, pages 339–347. ACM, 1999. DOI: [10.1145/301250.301337](#). ACM: [301250.301337](#)
60. Alexander Russell and David Zuckerman. Perfect information leader election in $\log^* n + O(1)$ rounds. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 576–583. IEEE Computer Society, 1998. ACM: [795664.796399](#)
61. 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. IEEE Computer Society, 1998
62. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Faster algorithms for optical switch configuration. In *Proceedings of 1997 IEEE International Conference on Communications (ICC)*, volume 3, pages 1320–1324. IEEE Computer Society, 1997. DOI: [10.1109/ICC.1997.595003](#)
63. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Approximating Latin square extensions. In Jin-Yi Cai and Chak Kuen Wong, editors, *Proceedings of the Second Annual International Conference on Computing and Combinatorics (COCOON)*, volume 1090 of *Lecture Notes in Computer Science*, pages 280–289. Springer, 1996. DOI: [10.1007/3-540-61332-3_162](#). ACM: [701577](#)
64. Marcos Kiwi, Carsten Lund, Alexander Russell, Daniel Spielman, and Ravi Sundaram. Alternation in interaction. In *Proceedings of the Ninth IEEE Annual Structure in Complexity Theory Conference*, pages 294–303. IEEE Computer Society, June 1994. DOI: [10.1109/SCT.1994.315795](#)
65. Mihir Bellare, Shafi Goldwasser, Carsten Lund, and Alexander Russell. Efficient probabilistically checkable proofs and applications to approximations. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC)*, pages 294–304. ACM, 1993. DOI: [10.1145/167088.167174](#). ACM: [167174](#)

Publications (continued)

66. Alexander Russell. Necessary and sufficient conditions for collision-free hashing. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference*, volume 740 of *Lecture Notes in Computer Science*, pages 433–441. Springer, 1992. ISBN: 3-540-57340-2. DOI: [10.1007/3-540-48071-4_30](https://doi.org/10.1007/3-540-48071-4_30). ACM: [646757.705517](https://doi.org/10.1145/646757.705517)

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)*, page 132, Monterey, CA, July, 2002. ACM.

Technical reports

1. See http://arxiv.org/a/russell_a_1 for a listing of my arXiv.org postings.

Research Grants and Fellowships

Federal Research Grants and Fellowships

- | | |
|-----------|--|
| 8/17–7/20 | • “Advanced Algorithmic Tools for Discovery in Cognitive Radio Networks,” <i>National Science Foundation</i> , \$250,000, PI: Alexander Russell. |
| 8/14–7/17 | • “SCH: EXP: LifeRhythm: A Framework for Automatic and Pervasive Depression Screening Using Smartphones,” <i>National Science Foundation</i> , \$718,815, PI: Bing Wang, coPIs: Jinbo Bi, Alok Banga, Alexander Russell. |
| 5/11–4/15 | • “AF: Small: Collaborative Research: Representation-theoretic techniques for pseudorandomness and lower bounds”, <i>National Science Foundation</i> , \$249,957, PI: Alexander Russell. |
| 9/09–9/12 | • “Quantum Algorithms on the Algebraic Frontier,” <i>ARO-ARDA</i> , \$200,000, PI: Alexander Russell. Subcontract through the University of California, Santa Barbara. The grant total is \$600,000 awarded to three institutions (UCSB, UNM, and UCONN). Other PIs: Wim van Dam, UCSB; Cristopher Moore, UNM. |
| 9/08–9/11 | • “CDI Type-I: Quantum Diffusion and Quantum Random Walks in Physical Systems,” <i>National Science Foundation</i> , \$550,448, PI: Alexander Russell; coPI: Robin Côté. |
| 9/08–9/10 | • “Collaborative Research: EMT/QIS: Quantum Algorithms and Post-Quantum Cryptography,” <i>National Science Foundation</i> , \$100,000, PI: Alexander Russell. |
| 8/05–8/08 | • “QnTM: The Quantum Complexity of Algebraic Problems,” <i>National Science Foundation</i> , \$120,000, PI: Alexander Russell. |
| 8/05–8/08 | • “QnTM: Quantum Information Processing with Quantum Random Walks,” <i>National Science Foundation</i> , \$300,000, PI: Robin Côté, coPI: Alexander Russell. |
| 1/05–1/08 | • “Quantum Algorithms for Algebraic Problems,” <i>ARO-ARDA Grant 47976-PH-QC</i> . \$200,000, PI: Alexander Russell. This is a subcontract through the University of New Mexico. The grant total is \$600,000 awarded to three institutions (UCSB, UNM, and UCONN). Other PIs: Cristopher Moore, UNM; Wim van Dam, UCSB. |

Research Grants and Fellowships (continued)

- 8/04–8/07 • “Computational Topology for Surface Approximation,” *National Science Foundation*, \$256,000, PI: Thomas Peters, coPIs: Kinetsu Abe, Alexander Russell.
- 9/03–8/06 • “ITR: Cooperative Computing and Adversity,” *National Science Foundation*, \$155,000, PI: Alex A. Shvartsman, coPI: Alexander Russell.
- 9/01–8/06 • “CAREER: Efficient Cryptography with Provable Security Guarantees,” *National Science Foundation*, \$305,000. PI: Alexander Russell.
- 9/02–8/05 • “QuBIC: Quantum Monte-Carlo Algorithms and Quantum Circuit Complexity,” *National Science Foundation*, \$150,000, PI: Alexander Russell.
- 9/02–8/05 • “ITR: Complexity-Theoretic Applications of Fourier Analysis,” *National Science Foundation*, \$125,000, PI: Alexander Russell.
- 9/01–8/06 • “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.
- 8/02–7/04 • “SGER: Computational Topology for Surface Reconstruction,” *National Science Foundation*, \$100,000, PI: Tom Peters, coPIs: Kinetsu Abe, Alexander Russell.
- 9/02–12/02 • MSRI Travel/Research Fellow, 2002 Special Semester on Quantum Computation, *Mathematical Sciences Research Institute*, \$4500.
- 7/02 • “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.
- 9/92–5/95 • NSF Graduate Fellow.

State and Industrial Research Grants

- 5/06–5/18 • “Voting Technology Research Center,” *State of Connecticut, Office of the Secretary of State*, \$3,146,992. PI: Alex A. Shvartsman, coPIs: Laurent Michel, Alexander Russell.
- 9/05–8/07 • “A Framework for Modeling and Analyzing Complex Distributed Systems,” *STTR DARPA - Vermondo, Inc.*, \$111,113, PI: Laurent Michel, coPI: Alexander Russell.
- 7/06–12/06 • “A Secure Framework for WIKIs,” *Serebrum Corporation*, \$20,877. PI: Steven Demurjian, CoPI: Alexander Russell.

Ph. D. Students Graduated

- Murat Osmanoglu, 2015.
- Qiang Tang, 2015. Now a professor at New Jersey Institute of Technology.
- Sixia Chen, 2014. Now a professor at Central Connecticut State University.
- Chadi El-Kari, 2011. Now a professor at University of the Pacific.
- Hang Dinh, 2010. Now a professor at the University of Indiana, South Bend.
- Shashidhar Narasimha, 2010. Now a professor at Sam Houston University.
- Lance Miller, 2009. Now a professor at the University of Arkansas.
- Gorjan Alagic, 2008. Now a postdoc at the University of Copenhagen.
- Kishori Konwar, 2008. Now a research scientist at the University of British Columbia.

Personal Information

- Member ACM/SIGACT, IACR, AMS.