Department of Computer Science and Engineering
University of Connecticut, U-4155
Storrs, CT 06269
acr@cse.uconn.edu
http://russell.engr.uconn.edu/

Home address:
148 Chaffeeville Rd.
Storrs, CT 06268

ALEXANDER C. RUSSELL
Professor of Computer Science

Professional Experience

As of 8/10	• *Professor* Department of Computer Science and Engineering	UNIVERSITY OF CONNECTICUT Storrs, CT
8/03–8/10	• *Associate Professor* Department of Computer Science and Engineering	UNIVERSITY OF CONNECTICUT Storrs, CT
8/99–8/03	• *Assistant Professor* Department of Computer Science and Engineering	UNIVERSITY OF CONNECTICUT Storrs, CT
9/97–8/99	• *Postdoctoral Fellow* Computer Science Division Joint position at: Department of Computer Science	UNIVERSITY OF CALIFORNIA, BERKELEY Berkeley, CA UNIVERSITY OF TEXAS AT AUSTIN Austin, TX
9/96–8/97	• *Postdoctoral Fellow* Department of Computer Science and Numerical Analysis	ROYAL INSTITUTE OF TECHNOLOGY Stockholm, Sweden
As of 8/18	• *Senior Research Fellow*	IOG Hong Kong
9/08–12/18	• *Senior Scientist, Member*	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

- 2023 Election Verification Network (EVN) Research Prize for the IEEE S&P paper "Adaptive Risk-Limiting Ballot Comparison Audits."
- UConn School of Engineering Centennial Term Professor, 2020–2022.
- Member, Connecticut Academy of Science and Engineering; inducted in 2016.
- 2016 AsiaCrypt prize paper, "Cliptography: Clipping the Power of Kleptographic Attacks."
- University of Connecticut Provost's Award for Excellence in Public Engagement, 2010

Honors and Professional Activities (continued)

- Connecticut Secretary of the State Public Service Award, 2009
- Best Paper Award, 29th International Colloquium on Automata, Languages, and Programming (ICALP), 2002.
- National Science Foundation CAREER Award, 2001–2006.
- University of Connecticut School of Engineering Junior Faculty Award 2003.
- University of Connecticut, Departmental Outstanding Faculty Award 2003.
- National Science Foundation Graduate Fellow.
- Member ΦBK.

Selected Professional Activities

- Associate Editor-in-Chief, *Theory of Computing*, 2005–.
- Director, *University of Connecticut Center for Voting Technology Research (VoTeR)*, 2018–.
- Member, SIGACT Committee for the Advancement of Theoretical Computer Science (CATCS), 2017–. (See https://thmatters.wordpress.com/catcs/.)
- Program Committee Member, *Asiacrypt* (ASIACRYPT), 2024.
- Program Committee Member, *Crypto* (CRYPTO), 2023.
- Program Committee Member, *55th ACM Symposium on Theory of Computing (STOC)*, 2023.
- Member, Connecticut Risk-Limiting Audit Working Group, 2021.
- Program Committee Member, *Innovations in Theoretical Computer Science (ITCS)*, 2022.
- Program Committee Member, *Cryptographers' Track RSA Conference (CT-RSA)*, 2021.
- Program Committee Member, *5th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML)*, 2021.
- Program Committee Member, *Cryptographers' Track RSA Conference (CT-RSA)*, 2020.
- Program Committee Member, *ACM Symposium on the Theory of Computing (STOC)*, 2019.
- Program Committee Member, *10th International Conference on Post-Quantum Cryptography (PQCrypto)*, 2019.
- 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.

Honors and Professional Activities (continued)

- 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.

Publications

Conference Articles (refereed; in published proceedings)

1. Alexander Russell, Qiang Tang, Jiadong Zhu. Crooked Indifferentiability of the Feistel Construction. Accepted, Asiacrypt, 2024.
2. Ghada Almashaqbeh, Sixia Chen, Alexander Russell. Competitive Policies for Online Collateral Maintenance. Proceedings of the sixth international conference on Advances in Financial Technologies (AFT'24). August, 2024.
3. Benjamin Fuller, Rashmi Pai, and Alexander Russell. The decisive power of indecision: Low-variance risk-limiting audits and election contestation via marginal mark recording. In Davide Balzarotti and Wenyuan Xu, editors, *33rd USENIX Security Symposium, USENIX Security 2024*. USENIX Association, August 2024. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/fuller
4. Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, Vassilis Zikas. Consensus Redux: Distributed Ledgers in the Face of Adversarial Supremacy. Proceedings of 2024 IEEE 37th Computer Security Foundations Symposium (CSF). July, 2024.
5. Peter Gaži, Aggelos Kiayias, and Alexander Russell. Fait Accompli committee selection: Improving the size-security tradeoff of stake-based committees. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023*, pages 845–858. ACM, 2023. DOI: 10.1145/3576915.3623194
6. Peter Gaži, Ling Ren, and Alexander Russell. Practical settlement bounds for longest-chain consensus. In Helena Handschuh and Anna Lysyanskaya, editors, *43rd Annual International Cryptology Conference, CRYPTO 2023*, volume 14081 of *Lecture Notes in Computer Science*, pages 107–138. Springer, 2023. DOI: 10.1007/978-3-031-38557-5_4
7. Aggelos Kiayias, Cristopher Moore, Saad Quader, and Alexander Russell. Adaptively secure random beacons for ungrindable blockchains. In *43rd IEEE International Conference on Distributed Computing Systems, ICDCS 2023*, pages 62–72. IEEE, 2023. DOI: 10.1109/ICDCS57875.2023.00021
8. Benjamin Fuller, Abigail Harrison, and Alexander Russell. Adaptive risk-limiting comparison audits. In *IEEE Symposium on Security and Privacy (SP)*, pages 3314–3331, Los Alamitos, CA, USA. IEEE Computer Society, May 2023. DOI: 10.1109/SP46215.2023.10179424
9. Peter Gaži, Ling Ren, and Alexander Russell. Practical settlement bounds for proof-of-work blockchains. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 1217–1230. ACM, November 2022. DOI: 10.1145/3548606.3559368
10. Sandro Coretti, Aggelos Kiayias, Cristopher Moore, and Alexander Russell. The generals' scuttlebutt: Byzantine-Resilient gossip protocols. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 595–608. ACM, November 2022. DOI: 10.1145/3548606.3560638

Publications (continued)

11. Matthias Fitzi, Aggelos Kiayias, Giorgos Panagiotakos, and Alexander Russell. Ofelimos: Combinatorial optimization via proof-of-useful-work - A provably secure blockchain protocol. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference (CRYPTO)*, volume 13508 of *Lecture Notes in Computer Science*, pages 339–369. Springer, 2022. DOI: 10.1007/978-3-031-15979-4_12.
12. Christian Badertscher, Peter Gaži, Iñigo Querejeta-Azurmendi, and Alexander Russell. A composable security treatment of ECVRF and batch verifications. In Vijayalakshmi Atluri, Roberto Di Pietro, Christian Damsgaard Jensen, and Weizhi Meng, editors, *Computer Security - ESORICS 2022 - 27th European Symposium on Research in Computer Security*, volume 13556 of *Lecture Notes in Computer Science*, pages 22–41. Springer, 2022. DOI: 10.1007/978-3-031-17143-7_2
13. Manuel M. T. Chakravarty, Sandro Coretti, Matthias Fitzi, Peter Gaži, Philipp Kant, Aggelos Kiayias, and Alexander Russell. Fast isomorphic state channels. In Nikita Borisov and Claudia Diaz, editors, *Financial Cryptography and Data Security - 25th International Conference (FC 2021)*, volume 12675 of *Lecture Notes in Computer Science*, pages 339–358. Springer, March 2021. DOI: 10.1007/978-3-662-64331-0_18
14. Luke Demarest, Benjamin Fuller, and Alexander Russell. Code offset in the exponent. In Stefano Tessaro, editor, *2nd Conference on Information-Theoretic Cryptography, (ITC 2021)*, volume 199 of *LIPIcs*, 15:1–15:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, July 2021. DOI: 10.4230/LIPIcs.ITC.2021.15
15. Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Dynamic ad hoc clock synchronization. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2021*, volume 12698 of *Lecture Notes in Computer Science*, pages 399–428. Springer, October 2021. DOI: 10.1007/978-3-030-77883-5_14
16. Aggelos Kiayias, Saad Quader, and Alexander Russell. Consistency of proof-of-stake blockchains with concurrent honest slot leaders. In *40th IEEE International Conference on Distributed Computing Systems, ICDCS 2020*, pages 776–786. IEEE, November 2020. DOI: 10.1109/ICDCS47774.2020.00065
17. Matthias Fitzi, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ledger combiners for fast settlement. In Rafael Pass and Krzysztof Pietrzak, editors, *18th International Conference on Theory of Cryptography (TCC)*, volume 12550 of *Lecture Notes in Computer Science*, pages 322–352. Springer, 2020. DOI: 10.1007/978-3-030-64375-1_12
18. Peter Gaži, Aggelos Kiayias, and Alexander Russell. Tight consistency bounds for Bitcoin. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, pages 819–838. ACM, 2020. DOI: 10.1145/3372297.3423365
19. Gorjan Alagic, Christian Majenz, and Alexander Russell. Efficient simulation of random states and random unitaries. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 12107 of *Lecture Notes in Computer Science*, pages 759–787. Springer, 2020. DOI: 10.1007/978-3-030-45727-3_26
20. Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 12107 of *Lecture Notes in Computer Science*, pages 788–817. Springer, 2020. DOI: 10.1007/978-3-030-45727-3_27
21. Erica Blum, Aggelos Kiayias, Cristopher Moore, Saad Quader, and Alexander Russell. The combinatorics of the longest-chain rule: Linear consistency for proof-of-stake blockchains. In Shuchi Chawla, editor, *Proceedings of the 2020 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1135–1154. SIAM, 2020. DOI: 10.1137/1.9781611975994.69

Publications (continued)

22. Saad Quader and Alexander Russell. Graph Realization on a Random Embedding. In Proceedings of the 31th Canadian Conference on Computational Geometry 2019 (CCCG), August 8-10, 2019.
23. Sherman S. M. Chow, Alexander Russell, Qiang Tang, Moti Yung, Yongjun Zhao, and Hong-Sheng Zhou. Let a non-barking watchdog bite: Cliptographic signatures with an offline watchdog. In Dongdai Lin and Kazue Sako, editors, *Proceedings of 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC)*, volume 11442 of *Lecture Notes in Computer Science*, pages 221–251. Springer, 2019. DOI: 10.1007/978-3-030-17253-4_8.
24. Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros Genesis: Composable proof-of-stake blockchains with dynamic availability. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, (CCS)*, pages 913–930. ACM, 2018. DOI: 10.1145/3243734.3243848.
25. Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Correcting subverted random oracles. In Hovav Shacham and Alexandra Boldyreva, editors, *38th Annual International Cryptology Conference (CRYPTO)*, volume 10992 of *Lecture Notes in Computer Science*, pages 241–271. Springer, 2018. DOI: 10.1007/978-3-319-96881-0_9
26. Peter Gaži, Aggelos Kiayias, and Alexander Russell. Stake-bleeding attacks on proof-of-stake blockchains. In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 85–92, June 2018. DOI: 10.1109/CVCBT.2018.00015.
27. Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In Jesper Buus Nielsen and Vincent Rijmen, editors, *37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, volume 10821 of *Lecture Notes in Computer Science*, pages 66–98. Springer, 2018. DOI: 10.1007/978-3-319-78375-8_3.
28. 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.
29. 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
30. 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.
31. 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.
32. 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. Additionally presented at Theory of Quantum Computation, Communication and Cryptography (TQC) 2017.
33. 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. (AsiaCrypt prize paper.)

Publications (continued)

34. 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 Soceity, 2016. DOI: 10.1109/WH.2016.7764553
35. 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
36. 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 Soceity, June 2016. DOI: 10.1109/CHASE.2016.27
37. 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
38. 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.
39. 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 Soceity, 2015. DOI: 10.1109/ICDCS.2015.17
40. 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 Soceity, 2014. DOI: 10.1109/ICDCS.2014.44
41. Sixia Chen, Cristopher 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
42. 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
43. 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. ACM: 2480362.2480702
44. 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
45. 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

Publications (continued)

46. 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.
47. Hang Dinh, Cristopher 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.
48. 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.
49. 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 Interational Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, page 3. ACM, 2011. DOI: 10.1145/2107502.2107506.
50. 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.
51. 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.
52. 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)*.
53. 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.
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.

Publications (continued)

59. 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.
60. 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.
61. 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.
62. 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.
63. Kinetsu Abe, Justin Bisceglio, 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.
64. 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
65. 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.
66. 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.
67. 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.
68. 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.
69. Chryssis 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.
70. Chryssis 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.
71. 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.
72. 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.

Publications (continued)

73. 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.
74. 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.
75. 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. ACM: 647087.757013
76. Chyssis 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.
77. 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.
78. 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.
79. Chryssis Georgiou, Alexander Russell, and Alexander A. Shvartsman. The complexity of distributed cooperation in the presence of failures. In Franck Butelle, editor, *Procedings of the 4th International Conference on Principles of Distributed Systems (OPODIS)*, Studia Informatica Universalis, pages 245–264. Suger, 2000
80. 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
81. 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
82. 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
83. 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
84. 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
85. 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
86. 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

87. 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
88. 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 Soceity, 1997. DOI: 10.1109/ICC.1997.595003
89. 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
90. 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
91. 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
92. 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. ACM: 646757.705517

Journal Articles (published or in-press)

1. Chinmaey Shende, Soumyashree Sahoo, Stephen Sam, Parit Patel, Reynaldo Morillo, Xinyu Wang, Shweta Ware, Jinbo Bi, Jayesh Kamath, Alexander Russell, Dongjin Song, and Bing Wang. Predicting symptom improvement during depression treatment using sleep sensory data. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 7(3):121:1–121:21, 2023. DOI: 10.1145/3610932
2. Shweta Ware, Chaoqun Yue, Reynaldo Morillo, Chao Shang, Jinbo Bi, Jayesh Kamath, Alexander Russell, Dongjin Song, Athanasios Bamis, and Bing Wang. Automatic depression screening using social interaction data on smartphones. *Smart Health*, 26:100356, 2022. ISSN: 2352-6483. DOI: 10.1016/j.smhl.2022.100356. URL: https://www.sciencedirect.com/science/article/pii/S2352648322000903
3. Reynaldo Morillo, Yanyuan Qin, Alexander Russell, and Bing Wang. More the merrier: Neighbor discovery on duty-cycled mobile devices in group settings. *IEEE Transactions on Wireless Communications*, 21(7):4754–4768, 2022. DOI: 10.1109/TWC.2021.3133099
4. Aaron Abrams, Henry Landau, Zeph Landau, Jamie Pommersheim, James Propp, and Alexander Russell. Germ order for one-dimensional packings. *Online Journal of Analytic Combinatorics*, 16(4):18, 2021. URL: https://hosted.math.rochester.edu/ojac/vol16/238.pdf
5. 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. *IEEE Trans. Big Data*, 7(2):355–370, 2021. DOI: 10.1109/TBDATA.2018.2872569
6. Sixia Chen, Reynaldo Morillo, Yanyuan Qin, Alexander Russell, Ruofan Jin, Bing Wang, and Sudarshan Vasudevan. Asynchronous neighbor discovery on duty-cycled mobile devices: models and schedules. *IEEE Trans. Wirel. Commun.*, 19(8):5204–5217, 2020. DOI: 10.1109/TWC.2020.2990764
7. Shweta Ware, Chaoqun Yue, Reynaldo Morillo, Jin Lu, Chao Shang, Jayesh Kamath, Athanasios Bamis, Jinbo Bi, Alexander Russell, and Bing Wang. Large-scale automatic depression screening using meta-data from wifi infrastructure. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(4), December 2018. DOI: 10.1145/3287073

Publications (continued)

8. Jin Lu, Chao Shang, Chaoqun Yue, Reynaldo Morillo, Shweta Ware, Jayesh Kamath, Athanasios Bamis, Alexander Russell, Bing Wang, and Jinbo Bi. Joint modeling of heterogeneous sensing data for depression assessment via multi-task learning. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2(1):21:1–21:21, 2018. DOI: 10.1145/3191753
9. 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
10. 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
11. 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
12. 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
13. 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
14. 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
15. 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
16. Seda Davtyan, Kishori M. Konwar, Alexander Russell, and Alexander A. Shvartsman. Dealing with undependable workers in decentralized network supercomputing. *Theoretical Computer Science*, 561, Part B:96–112, 2015. DOI: 10.1016/j.tcs.2014.10.015. Special Issue on Distributed Computing and Networking
17. 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
18. 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
19. Sixia Chen and Alexander Russell. Online metric tracking and smoothing. *Algorithmica*, 68(1):133–151, 2014. DOI: 10.1007/s00453-012-9669-8
20. 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
21. 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
22. 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
23. Cristopher Moore and Alexander Russell. Approximating the permanent via nonabelian determinants. *SIAM Journal on Computing*, 41(2):332–355, 2012. DOI: 10.1137/100806709
24. 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

Publications (continued)

25. 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
26. 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
27. 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
28. 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
29. 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
30. 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
31. 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: 10.1145/1644015.1644034
32. 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
33. 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
34. 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. ACM: 1410885.1410909
35. 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. ACM: 1362744.1362749
36. 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
37. 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. ACM: 1328865.1328877
38. 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
39. Kinetsu Abe, Justin Bisceglio, 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. ACM: 1226616.1226619
40. 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

Publications (continued)

41. 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. URL: http://stacks.iop.org/1367-2630/8/i=8/a=156
42. 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
43. 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
44. 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. ACM: 1195997.1196005
45. 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. ACM: 1064628.1064938
46. 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. ACM: 985557.985560. Special issue for ICALP 2002
47. 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
48. 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. ACM: 1045979.1045995
49. 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. Special issue for SODA 2004
50. 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
51. 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. ACM: 1018448.1018452
52. 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. ACM: 998277.998295
53. 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
54. 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. Special issue for STOC 1999
55. 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. ACM: 945266.945268
56. 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. ACM: 603645.603656. URL: http://portal.acm.org/citation.cfm?id=603645.603656
57. 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. ACM: 569473.569479. Special issue for FOCS 1998
58. 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

Publications (continued)

59. 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
60. 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
61. 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. JSTOR: 2589379
62. 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
63. S. Ravi Kumar, Alexander Russell, and Ravi Sundaram. Approximating Latin square extensions. *Algorithmica*, 24(2):128–138, 1999. DOI: 10.1007/PL00009274
64. 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
65. Alexander Russell and Ravi Sundaram. Symmetric alternation captures BPP. *Computational Complexity*, 7(2):152–162, November 1998. DOI: 10.1007/s000370050007. ACM: 306576.306608
66. 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. ACM: 287396.287535
67. 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. ACM: 261591.261594
68. Alexander Russell. Necessary and sufficient conditions for collision-free hashing. *Journal of Cryptology*, 8(2):87–99, 1995. DOI: 10.1007/BF00190757
69. 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
70. 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. ACM: 104724.104733

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.

Publications (continued)

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.

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.

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

Federal Research Grants

8/19–7/23 • "SCH: Personalized Depression Treatment Support by Mobile Sensor Analytics," *National Institute of Health*, $1,028,460, four PIs: Jinbo Bi, Jayesh Kamath, Alexander Russell, and Bing Wang.

8/18–7/21 • "Theory and Practice of Cryptosystems Secure Against Subversion," *National Science Foundation*, $300,000, PI: Alexander Russell.

8/18–7/21 • "Quantum-Secure Cryptography and Fine-Grained Quantum Query Complexity," *National Science Foundation*, $274,898, PI: Alexander Russell.

8/17–7/20 • "Advanced Algorithmic Tools for Discovery in Cognitive Radio Networks," *National Science Foundation*, $250,000, PI: Alexander Russell.

8/14–7/17 • "LifeRhythm: A Framework for Automatic and Pervasive Depression Screening Using Smartphones," *National Science Foundation*, $718,815, PI: Bing Wang, coPIs: Jinbo Bi, Alok Banga, Alexander Russell.

5/11–4/15 • "Representation-theoretic techniques for pseudorandomness and lower bounds", *National Science Foundation*, $249,957, PI: Alexander Russell.

Research Grants (continued)

9/09–9/12 • "Quantum Algorithms on the Algebraic Frontier," *ARO-ARDA*, $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 • "Quantum Diffusion and Quantum Random Walks in Physical Systems," *National Science Foundation*, $550,448, PI: Alexander Russell; coPI: Robin Côté.

9/08–9/10 • "Quantum Algorithms and Post-Quantum Cryptography," *National Science Foundation*, $100,000, PI: Alexander Russell.

8/05–8/08 • "The Quantum Complexity of Algebraic Problems," *National Science Foundation*, $120,000, PI: Alexander Russell.

8/05–8/08 • "Quantum Information Processing with Quantum Random Walks," *National Science Foundation*, $300,000, PI: Robin Côté, coPI: Alexander Russell.

1/05–1/08 • "Quantum Algorithms for Algebraic Problems," *ARO-ARDA* Grant 47976-PH-QC. $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.

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 • "Cooperative Computing and Adversity," *National Science Foundation*, $155,000, PI: Alex A. Shvartsman, coPI: Alexander Russell.

9/02–8/05 • "Quantum Monte-Carlo Algorithms and Quantum Circuit Complexity," *National Science Foundation*, $150,000, PI: Alexander Russell.

9/02–8/05 • "Complexity-Theoretic Applications of Fourier Analysis," *National Science Foundation*, $125,000, PI: Alexander Russell.

8/02–7/04 • "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.

9/01–8/06 • "CAREER: Efficient Cryptography with Provable Security Guarantees," *National Science Foundation*, $305,000. PI: Alexander Russell.

9/01–8/06 • "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.

State and Industrial Research Grants

5/23–5/24 • "Voting Technology Research Center," *State of Connecticut, Office of the Secretary of State*, $1,160,000. PI: Alexander Russell, coPI: Benjamin Fuller, Laurent Michel.

5/18–5/23 • "Voting Technology Research Center," *State of Connecticut, Office of the Secretary of State*, $2,044,576. PI: Alexander Russell, coPI: Benjamin Fuller, Laurent Michel. (This is the continuation of the center grant below, though I now direct the center and am PI. For brevity, this accounts for four back-to-back one-year grants.)

5/06–5/18 • "Voting Technology Research Center," *State of Connecticut, Office of the Secretary of State*, $3,146,992. PI: Alex Shvartsman, CoPIs: Laurent Michel, Alexander Russell. (For brevity, this accounts for 12 back-to-back one-year grants.)

7/18-6/20 • "Ungrindable blockchains," *Input Output HK*, $46,664. PI: Alexander Russell.

Research Grants (continued)

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

- Luke Johnson, 2023. Now a professor at Gonzaga University.
- Jiadong Zhu, 2022.
- Saad Quader, 2020. Now at Google.
- Murat Osmanoglu, 2015. Now a professor at Ankara University.
- Qiang Tang, 2015. Now a professor at University of Sydney.
- Sixia Chen, 2014. Now a professor at Adelphi Univeristy.
- 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 scientist at NIST and research scientist at UMD, College Park.
- Kishori Konwar, 2008. Now a research scientist at MIT.

Personal Information

- Member ACM/SIGACT, IACR.
- US citizen.