

Duncan A. Buell

Chair Emeritus — NCR Chair in Computer Science and Engineering
Department of Computer Science and E
University of South Carolina, Columbia, South Carolina 29208
buell@acm.org
www.duncanbuell.org

Personal: U. S. citizen.

Experience:

September 2022—May 2024: Visiting Assistant Professor, Department of Computer Science, Denison University, Granville, OH. (Taught five courses over four semesters.)

January 2021—present: Chair Emeritus, NCR Chair in Computer Science and Engineering, Department of Computer Science and Engineering, University of South Carolina, Columbia, SC 29208.

July 2009—December 2020: Professor, Department of Computer Science and Engineering, University of South Carolina, Columbia, SC 29208.

October 2000—2009: Professor and Chair, Department of Computer Science and Engineering, University of South Carolina. Duties also included management of the college IT network, computer center, and staff comprising nine instructional labs (250 desktops), cluster computers, file and mail servers, and network infrastructure.

August 2005—July 2006: Interim Dean, College of Engineering and Information Technology, University of South Carolina.

January 1986—September 2000: Center for Computing Sciences, Institute for Defense Analyses, 17100 Science Drive, Bowie, Maryland 20715. (The Center for Computing Sciences was named the Supercomputing Research Center from 1985 through May 1995.)

1979—December 1985: Department of Computer Science, Louisiana State University, Baton Rouge, Louisiana 70803. (Assistant Professor, 1979—1982; Associate Professor with tenure, 1982—1985)

1977—1979: Assistant Professor, Department of Computer Science, Bowling Green State University, Bowling Green, Ohio 43402.

1976—1977: Research Associate, Department of Mathematics, Carleton University, Ottawa, Ontario, Canada K1S 5B6.

Education:

Ph. D. in mathematics (number theory), 1976, University of Illinois—Chicago.

M. A. in mathematics, 1972, University of Michigan, Ann Arbor.

B. S. in mathematics, 1971, University of Arizona, Tucson.

Teaching and Research Interests:

Outreach for expanding the pipeline of computing students.

Digital humanities

Electronic voting systems and computer security

Computational number theory

Information retrieval

Grants Held:

“First-Year Composition as Big Data,” Conference on College Composition and Communication/National Council of Teachers of English, \$9,663, 2/2016-2/2017. (co-PI with PI Chris Holcomb)

“AP Summer Institute in Computer Science,” South Carolina State Department of Education, \$16,475, summer 2014. (PI)

“Expanding Computing Education Pathways Alliance,” National Science Foundation, Mark Guzdial (Georgia Tech) and Rick Adrion (U. of Massachusetts Amherst), PIs, \$6.4M, 10/2012-9/2017. (subcontractor as partner state, \$394,986 to USC)

“AP Summer Institute in Computer Science,” South Carolina State Department of Education, \$17,475, summer 2012. (PI)

“Ghosts of South Carolina College—A Critical Interactive for Engaging Students and Visitors in the History of USC’s Horseshoe,” USC Vice-President for Research ASPIRE-II grant, \$65,185, 5/2012-8/2013. (PI with co-PIs Heidi Rae Cooley and Bob Weyeneth)

“Mobile Geospatial Situational Awareness for Field and Command Staff During the Emergency Response Phase,” Department of Homeland Security \$99,257, 9/2011-5/2012. (co-PI with PI Michael Hodgson)

“History Simulation for Teaching Early Modern British History,” National Endowment for the Humanities, \$49,967, 5/2011-5/2012. (PI with co-PI Heidi Rae Cooley)

“Humanities Gaming: Building Serious Games for Research and Pedagogy,” National Endowment for the Humanities, \$232,096, 5/2010-5/2011. (PI with co-PIs Randall Cream, Simon Tarr, and Heidi Rae Cooley)

“SC STEPS to STEM,” NSF, \$2,035,667, 2007-2012. (co-PI with PI Tim Mousseau and co-PIs Ann Johnson, Loren Knapp, and Jed Lyons)

- “New metrics for characterizing and predicting network behavior,” Subcontract of DARPA funding from Department of Physics and Astronomy, USC, approximately \$400,000, 2003-2006. (co-PI with PI Joe Johnson and co-PI Chin-Tser Huang)
- “Library development and experiments using prototype reconfigurable computing machines,” NSA subcontract from George Washington University, \$399,993, 5/01/04-8/31/06. (PI, co-PIs J. Davis, G. Quan)
- “Gene expression profiles of HPV-transformed cells in vitro and in vivo,” USC Medicine and Engineering Research Fund, \$35,000, 3/15/03-3/14/04. (co-PI with L. Pirisi-Creek and PI J. Rose)
- “Utilization of aggregate network load modules for high-performance computing applications,” Ixia Corporation industrial research contract, \$51,204 and major equipment donation, 1/1/03-8/15/03. (co-PI with PI K. Cameron)
- “Library development and experiments using prototype reconfigurable computing machines,” NSA Lucite subcontract, \$426,574, 4/08/02-4/30/04. (PI with co-PIs J. Davis and G. Quan)
- “Information Systems Security Education at the University of South Carolina,” NSF, \$199,846, 9/01/01-8/31/03. (co-PI with PI C. Farkas and co-PIs C. Eastman, S. Fenner, and J. Johnson)
- “Accelerating computations in statistical genomics through the use of novel hardware and parallelized software,” USC Vice President for Research Opportunity Fund, \$50,000, 2001-2002. (PI with co-PIs László Székely and Peter Waddell)
- “A high performance computer for factoring large numbers,” National Security Agency MDA904-85-H-0006, \$198,296, 1 February 1985-31 January 1987. (co-PI with Walter G. Rudd)
- “An investigation of the CPS factoring method,” National Science Foundation-National Security Agency DCR-8311580, \$58,125, 15 April 1984-30 September 1985.
- “Modelling of generalizations of Boolean query processing in information retrieval systems,” NSF IST-8115146, \$34,722, 1 September 1981-28 February 1983. (co-PI with Donald H. Kraft)
- “Database/data access needs for computerization of well data,” LSU Mining and Mineral Resources Research Institute, Summer Faculty Research Award, 1981.
- “Elliptic curves and class groups of quadratic fields,” NSF MCS78-01943, \$6,700, 15 July 1978-31 December 1979.

Professional Associations:

American Association for the Advancement of Science (Elected a Fellow 2013)
Association for Computing Machinery (Life Senior Member)
American Mathematical Society (Life Member)
Foundation Fellow, The Institute of Combinatorics and its Applications
IEEE (Life Senior Member), IEEE Computer Society
Advisory Board Member, U. S. Vote Foundation
National Center for Science Education, Union of Concerned Scientists

Other Scholarly and Professional Activities (selected):

Member, Board of Reviewers *Journal of Writing Analytics* 2016—present.
Committee Member, Computing Sciences Scholarships and Fellowships Committee, National Science and Engineering Research Council of Canada, 2013-2017. (This committee is the Canadian analogue to the NSF panels that evaluate Graduate Research Fellowship proposals, but it also has funding for postdoctoral positions.)
Appointed by The Honorable Asa Hutchinson, Governor of Arkansas, to the Southern Regional Education Board Commission on Computer Science, Information Technology, and Related Career Fields, 2015.
General co-chair, Election Verification Network annual conference, 2016.
Elected to the Coordinating Committee, Election Verification Network, 2015.
General chair, Election Verification Network annual conference, 2015.
Member of the search committee for the Executive Director of the Computer Science Teachers Association, 2015.
Organizing Committee, Election Verification Network annual conference, 2014.
Consultant on electronic voting technology, League of Women Voters of South Carolina, 2004—present.
Program Chair, Computer Science Teachers Association annual conference, 2011–2015.
National University Representative to the Computer Science Teachers Association, 2008-2010, re-elected for 2010-2012.
Co-Editor in Chief, ACM *Transactions on Reconfigurable Technology and Systems* 2007-2010. (Journal founded with co-EIC Wayne Luk.)
IEEE Workshop/Symposium on Field-Programmable Custom Computing Machines: Co-chair, 1993, 1994, 2006, 2007, 2008, 2009; Program Committee, 1995—2013.
Program Committee, ACM FPGA94, FPGA95, FPGA 2005, Monterey, California.

Program Committee Chair, ANTS VI (Algorithmic Number Theory Symposium), Burlington, Vermont, June 2004.

Advisory board member, IEEE International Conference on Field-Programmable Technology, 2003, 2004.

Guest editor of various special issues of journals.

Associate Editor, *Journal of Approximate Reasoning*, 1986-1992.

ACM National Lecturer, 1982-83.

Phi Beta Kappa, Phi Kappa Phi.

PUBLICATIONS

Submitted:

Matthew Thornburg and Duncan A. Buell, "Understanding nonpartisan roll-off among straight party voters," submitted.

Krystal Werfel, Stanley Dubinsky, Elizabeth Barlow, Sydney Bassard, and Duncan Buell, "The effectiveness of computerized linguistic-based spelling instruction for increasing spelling skills in second grade students," submitted.

D. A. Buell and G. Gay, "Is technology the answer? Software quality issues in electronic voting systems," submitted.

Books:

D. A. Buell, *Fundamentals of Cryptography: Introducing Mathematical and Algorithmic Foundations*, Springer-Verlag, 2021, 279 pages, ISBN: 978-3-030-73492-3. (German translation, done by a computer program, also available.)

D. A. Buell, *Data Structures Using Java*, Jones and Bartlett, 2013, 400 pages, ISBN-13: 978-1-4496-2807-9.

D. A. Buell, J. M. Arnold, and W. J. Kleinfelder, eds., *Splash 2: FPGAs in a Custom Computing Machine*, IEEE Computer Society Press, 1996, 320 pages, ISBN 0-8186-7413-X.

D. A. Buell, *Binary Quadratic Forms: Classical Theory and Modern Computations*, Springer-Verlag, 1989, 247 pages, ISBN 0-387-97037-1.

Proceedings editor:

D. A. Buell and K. Pocek, eds., *Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines*, IEEE Computer Society Press, 2009, 309 pages, ISBN 978-0-7695-3716-0.

- D. A. Buell and K. Pocek, eds., *Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines*, IEEE Computer Society Press, 2008, 324 pages, ISBN 978-0-7695-3307-0.
- D. A. Buell and K. Pocek, eds., *Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines*, IEEE Computer Society Press, 2007, 358 pages, ISBN 0-7685-2940-2.
- D. A. Buell and K. Pocek, eds., *Proceedings of the IEEE Symposium on Field-Programmable Custom Computing Machines*, IEEE Computer Society Press, 2006, 355 pages, ISBN 0-7695-2661-6.
- D. Buell, ed., *Algorithmic Number Theory*, Proceedings of the sixth international symposium (ANTS VI), *Lecture Notes in Computer Science 3076*, Springer-Verlag, 2004, 451 pages, ISBN 3-540-22156-5.
- D. A. Buell and J. T. Teitelbaum, eds., *Computational Perspectives in Number Theory: Proceedings of a conference in honor of A. O. L. Atkin*, American Mathematical Society, 1997, 232 pages, ISBN 0-8218-0880-X.
- D. A. Buell and K. Pocek, eds., *Proceedings of the IEEE Workshop on FPGAs for Custom Computing Machines*, IEEE Computer Society Press, 1994, 199 pages, ISBN 0-8186-5490-2.
- D. A. Buell and K. Pocek, eds., *Proceedings of the IEEE Workshop on FPGAs for Custom Computing Machines*, IEEE Computer Society Press, 1993, 224 pages, ISBN 0-8186-3890-7.

Journal Articles and Book Chapters:

- Adam Schmidt, D. A. Buell, and Laura Albert, “Optimal consolidation of polling locations”, *Manufacturing and Service Operations Management*, to appear.
- Susan Lang, D. A. Buell, and Norbert Elliot, “Computer-assisted corpus analysis: An introduction to concepts, processes, and decisions”, *IEEE Transactions on Professional Communication*, v. 66, Issue 1, 2023, pp. 94-113, DOI 10.1109/TPC.2022.3228026.
- D. A. Buell, “A parameterized family of quadratic class groups with 3-Sylow subgroups of rank at least three,” *The Ramanujan Journal*, v. 59, 2022, pp. 955-965.
- C. Holcomb and D. A. Buell, “First-year composition as ‘Big Data’: Towards examining student revisions at scale,” *Computers and Composition*, v. 48, 2018, pp. 49-66.
- H. R. Cooley and D. A. Buell, “Building Humanities Software that Matters:

- The case of *Ward One* ” Mobile App,” *Making Things and Drawing Boundaries: Experiments in the Digital Humanities*, Jentery Sayers, ed., *Debates in the Digital Humanities*, Matthew K. Gold and Lauren F. Klein, series editors, University of Minnesota Press, 2017, pp. 272-287.
- D. A. Buell and G. S. Call, “Class pairings and isogenies on elliptic curves,” *Journal of Number Theory*, v. 167, 2016, pp. 31-73.
- H. R. Cooley and D. A. Buell, “*Ghosts of the Horseshoe*, a Mobile Application: Fostering a New Habit of Thinking about the History of University of South Carolina’s Historic Horseshoe,” *Annual Review of Cultural Heritage Informatics*, v. 1, 2014, pp. 193-212.
- D. A. Buell, “An Analysis of Long Lines in Richland County, South Carolina,” *USENIX Journal of Election Technology and Systems*, v. 1, issue 1, August 2013, pp. 106-118.
- D. A. Buell and H. R. Cooley, “Critical Interactives: Improving public understanding of public policy,” *Bulletin of Science, Technology, and Society*, v. 32, issue 6, December 2012, pp. 486-493, DOI:10.1177/0270467612469073.
- D. A. Buell, “Ideal composition in quadratic fields: From Bhargava to Gauss,” *The Ramanujan Journal*, v. 29, 2012, pp. 31-49. (DOI 10.1007/s11139-012-9400-z)
- Y. Kopylova, D. A. Buell, C.-T. Huang, and J. Janies, “Mutual information applied to anomaly detection,” *Journal of Communications and Networks*, v. 10, 2008, pp. 89-97.
- P. Saha, E. El-Araby, M. Huang, M. Taher, S. Lopez-Buedo, T. El-Ghazawi, C. Shu, K. Gaj, A. Michalski, and D. Buell, “Portable library development for reconfigurable computing systems: A case study”, *Parallel Computing*, v. 34, 2008, pp. 245-260.
- T. El-Ghazawi, E. El-Araby, M. Huang, K. Gaj, V. Kindratenko, D. Buell, “The promise of high-performance reconfigurable computing,” *IEEE Computer*, February 2008, pp. 69-76.
- D. A. Buell, “Number theory,” *The Handbook of Information Security*, Volume 2, John Wiley, 2006, pp. 532-547.
- D. A. Buell, “The Advanced Encryption Standard,” *The Handbook of Information Security*, Volume 2, John Wiley, 2006, pp. 498-509.
- D. A. Buell and R. Sandhu, “Identity management,” *IEEE Internet Computing*, v. 7, no. 6, November/December 2003, pp. 26-28. (guest editors’ introduction).

- X. Feng, D. A. Buell J. R. Rose, and P. J. Waddell, "Parallel algorithms for Bayesian phylogenetic inference," *Journal of Parallel and Distributed Computing*, v. 63, 2003, pp. 707-718.
- M. N. Huhns and D. A. Buell, "Trusted autonomy," *IEEE Internet Computing*, v. 6, no. 3, May/June 2002, pp. 92-95.
- D. A. Buell and Kenneth L. Pocek, "Custom computing machines: An introduction," *The Journal of Supercomputing*, v. 9, 1995, pp. 219-230 (guest editors' introduction to a special issue).
- D. A. Buell and Veikko Ennola, "On a parameterized family of quadratic and cubic fields," *Journal of Number Theory*, v. 54, 1995, pp. 134-148.
- A. Bremner and D. A. Buell, "Three points of great height on elliptic curves," *Mathematics of Computation*, v. 61, 1993, pp. 111-116.
- D. A. Buell and R. L. Ward, "A multiprecise integer arithmetic package," *The Journal of Supercomputing*, v. 3, 1989, pp. 89-107.
- J. Young and D. A. Buell, "The twentieth Fermat number is composite," *Mathematics of Computation*, v. 50, 1988, pp. 261-263.
- D. A. Buell, "Integer squares with constant second difference," *Mathematics of Computation*, v. 49, 1987, pp. 635-644.
- D. A. Buell, "Factoring: Algorithms, computers, and computations," *The Journal of Supercomputing*, v. 1, 1987, pp. 191-216.
- D. A. Buell, "Class groups of quadratic fields II," *Mathematics of Computation*, v. 48, 1987, pp. 85-93.
- D. A. Buell and R. H. Hudson, "Sequences in power residue classes," *International Journal of Mathematics and Mathematical Statistics*, v. 9, 1986, pp. 261-266.
- D. M. Chiarulli and D. A. Buell, "Parallel microprogramming tools for a horizontally reconfigurable architecture," *International Journal of Parallel Programming*, v. 15, 1986, pp. 151-162.
- D. A. Buell, "A problem in information retrieval with fuzzy sets," *Journal of the American Society for Information Science*, v. 36, 1985, pp. 398-401.
- D. A. Buell, "A retrieval system for well information data," *Computers and Geosciences*, v. 10, 1984, pp. 205-209.
- D. A. Buell, "The expectation of success using a Monte Carlo factoring method—some statistics on quadratic class numbers," *Mathematics of Computation*, v. 43, 1984, pp. 313-327.
- D. A. Buell and R. H. Hudson, "On runs of consecutive quadratic residues and quadratic nonresidues," *BIT*, v. 24, 1984, pp. 243-247.

- D. A. Buell and R. H. Hudson, "Solutions of certain quaternary quadratic forms," *Pacific Journal of Mathematics*, v. 114, 1984, pp. 23-45.
- D. A. Buell, R. H. Hudson, and K. S. Williams, "Extension of a theorem of Cauchy and Jacobi," *Journal of Number Theory*, v. 19, 1984, pp. 309-340.
- D. H. Kraft and D. A. Buell, "Fuzzy sets and generalized Boolean retrieval systems," *International Journal of Man-Machine Studies*, v. 19, 1983, pp. 45-56. (Reprinted in *Readings in Fuzzy Sets for Intelligent Systems*, Didier Dubois, Henri Prade, and Ronald Yager, eds., San Mateo: Morgan Kaufmann, 1993.)
- D. A. Buell, "An analysis of some fuzzy subset applications to information retrieval systems," *Fuzzy Sets and Systems*, v. 7, 1982, pp. 35-42.
- D. A. Buell, "A general model of query processing in information retrieval systems," *Information Processing and Management*, v. 17, 1981, pp. 249-262.
- D. A. Buell and D. H. Kraft, "Threshold values and Boolean retrieval systems," *Information Processing and Management*, v. 17, 1981, pp. 127-136.
- D. A. Buell and D. H. Kraft, "A model for a weighted retrieval system," *Journal of the American Society for Information Science*, v. 32, 1981, pp. 211-216.
- D. A. Buell, P. A. Leonard, and K. S. Williams, "Note on the quadratic character of a quadratic unit," *Pacific Journal of Mathematics*, v. 92, 1981, pp. 35-38.
- D. A. Buell and K. S. Williams, "An octic reciprocity law of Scholz type," *Proceedings of the American Mathematical Society*, v. 77, 1979, pp. 315-318.
- D. A. Buell and K. S. Williams, "Maximal residue difference sets modulo p ," *Proceedings of the American Mathematical Society*, v. 69, 1978, pp. 205-209.
- D. A. Buell, "Elliptic curves and class groups of quadratic fields," *Journal of the London Mathematical Society, Series 2*, v. 15, 1977, pp. 19-25.
- D. A. Buell, "Small class numbers and extreme values of L -functions of quadratic fields," *Mathematics of Computation*, v. 31, 1977, pp. 786-796.
- D. A. Buell, H. C. Williams, and K. S. Williams, "On the imaginary bicyclic biquadratic fields of class-number 2," *Mathematics of Computation*, v. 31, 1977, pp. 1034-1042.

D. A. Buell, "Class groups of quadratic fields," *Mathematics of Computation*, v. 30, 1976, pp. 610-623.

Refereed Conference Proceedings:

H. R. Cooley and D. A. Buell, "Ghosts of the Horseshoe: A Mobile Critical Interactive for Social Engagement," Interactive Narratives, New Media and Social Engagement International Conference, Toronto, Ontario, October 2014.

D. A. Buell and H. R. Cooley, "Ghosts of the Horseshoe: A Critical Interactive," Software demo presented at *HASTAC 2013*, Toronto, Ontario, April 2013.

D. A. Buell and H. R. Cooley, "Desperate Fishwives: On the Origins of 'Critical Interactives'," *Proceedings, Games, Learning, and Society*, Madison, Wisconsin, June 2012, pp. 391-396.

D. A. Buell, E. Hare, F. Heindel, C. Moore, B. Zia, "Auditing a DRE-based election in South Carolina," *Proceedings, USENIX Workshop on Electronic Voting Technology/Workshop on Trustworthy Elections 2011*, San Francisco, California, August 2011.

S. Shida, Y. Shibata, K. Oguri, and D. A. Buell, "An optimization method of DMA transfer for a general purpose reconfigurable machine", *Proceedings, International Conference on Field Programmable Logic and Applications*, 2008, pp. 647-650.

X. Feng, D. A. Buell, K. W. Cameron, "PBPI: A high performance implementation of Bayesian phylogenetic inference," *Proceedings, Supercomputing 2006*, Tampa, Florida, November 2006.

E. A. Michalski and D. A. Buell, "A scalable architecture for RSA cryptography on large FPGAs," *Proceedings, FPL 06*, Madrid, Spain, 28-30 August 2006.

C. L. Cathey, J. D. Bakos, and D. A. Buell, "A reconfigurable distributed computing fabric exploiting multilevel parallelism," *Proceedings, IEEE Symposium on Field Programmable Custom Computing Machines*, Napa, California, April 2006.

A. Michalski, D. Buell, and K. Gaj, "High-throughput reconfigurable computing: Design and implementation of an IDEA encryption cryptosystem on the SRC-6e reconfigurable computer", *Proceedings, International Conference on Field Programmable Logic and Applications*, 2005, pp. 681-686.

G. Quan, J. Davis, S. Devarkal, and D. A. Buell, "High-level synthesis for

- large bit-width multipliers on FPGAs: A case study,” *Proceedings*, Third IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Jersey City, New Jersey, September 2005, pp. 213-218.
- D. A. Buell, “Calibrating entropy functions applied to computer networks,” *Proceedings of the Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, St. Petersburg, Russia, September 2005, *Lecture Notes in Computer Science #3685*, V. Gorodetsky, I. Kottenko, and V. Skormin, eds., Berlin: Springer-Verlag, 2005, pp. 76-87.
- L. Cordova and D. Buell, “A novel high-level dynamic hardware-software remapping technique for mission critical reconfigurable computers,” *Proceedings of the Military and Aerospace Programmable Logic Devices (MAPLD) conference*, Washington, DC, 7-9 September 2005.
- S. Akella, D. A. Buell, and L. Cordova, “The DARPA data transposition benchmark on the SRC-6,” *Proceedings of the Military and Aerospace Programmable Logic Devices (MAPLD) conference*, Washington, DC, 7-9 September 2005.
- D. Buell, S. Akella, G. Quan, J. Davis, and L. Cordova, “Programming FPGAs from C: Experiences with the SRC-6,” *Proceedings of the Military and Aerospace Programmable Logic Devices (MAPLD) conference*, Washington, DC, 7-9 September 2005.
- L. Cordova, D. A. Buell, and S. Akella, “The DARPA dynamic programming benchmark on a reconfigurable computer”, *Proceedings, IEEE Symposium on Field Programmable Custom Computing Machines*, Napa, California, April 2005, pp. 327-328.
- D. A. Buell, D. Caliga, J. P. Davis, G. Quan, “The DARPA boolean equation benchmark on a reconfigurable computer,” *Proceedings of the Military and Aerospace Programmable Logic Devices (MAPLD) conference*, Washington, DC, 8-10 September 2004.
- Quan, G., A. Michalski, D. Buell, and J. Davis, “The DARPA sorting benchmark on the SRC platform,” *Proceedings of the Military and Aerospace Programmable Logic Devices (MAPLD) conference*, Washington, DC, 8-10 September 2004.
- D. A. Buell, J. P. Davis, G. Quan, S. Akella, S. Devarkal, P. Kancharla, E. A. Michalski, H. A. Wake, “Experiences with a reconfigurable computer,” *Proceedings, Engineering of Reconfigurable Systems and Algorithms*, Las Vegas, NV, 21-24 June 2004.

- S. Akella, D. A. Buell, J. P. Davis, and Heather A. Wake, "Porting EDIF netlists to the Viva environment," *Proceedings*, Military and Aerospace Programmable Logic Devices (MAPLD) conference, Washington, DC, 9-11 September 2003.
- P. Kancharla and D. A. Buell, "The Advanced Encryption Standard on the HC 36m reconfigurable computer," *Proceedings* of the Military and Aerospace Programmable Logic Devices (MAPLD) conference, Washington, DC, 9-11 September 2003.
- S. Devarkal, D. A. Buell, J. P. Davis, and G. Quan, "Elliptic curve arithmetic addition on reconfigurable hardware," *Proceedings* of the Military and Aerospace Programmable Logic Devices (MAPLD) conference, Washington, DC, 9-11 September 2003.
- D. A. Buell, S. Devarkal, and H. A. Wake, "Reconfigurable computing machines and their applications in computational number theory," *High Primes and Misdeameanours: A Conference in Honor of Hugh Williams, Fields Institute Communications*, volume 41, pp. 123-148, Fields Institute, Toronto, 2004.
- H. Wake and D. A. Buell, "Congruential sieves on a reconfigurable computer," *Proceedings*, IEEE Symposium on Field Programmable Custom Computing Machines, Napa, California, April 2003, pp. 11-18.
- D. A. Buell, J. P. Davis, and G. Quan, "Reconfigurable computing applied to problems in communications security," *Proceedings* of the Military and Aerospace Programmable Logic Devices (MAPLD) conference, Laurel, Maryland, 10-12 September 2002.
- D. A. Buell, C. Farkas, M. N. Huhns, J. R. Rose, and M. G. Valtorta, "Information reputation in an environment of ubiquitous computing," Phoenix Conference on Information Warfare, Colorado Springs, Colorado, September 2001.
- D. A. Buell, "The last exhaustive computation of class groups of complex quadratic number fields," *CRM Proceedings and Lecture Notes*, v. 19, 1999, pp. 35-53. (*Proceedings* of the Fifth Conference of the Canadian Number Theory Association.)
- N. D. Bronson and D. A. Buell, "Congruential sieves on FPGA computers," in *Proceedings of Symposia in Applied Mathematics #48*, Walter Gautschi, editor, American Mathematical Society, Providence, 1994, pp. 547-552.
- J. M. Arnold and D. A. Buell, "VHDL programming on Splash 2," in *More FPGAs*, Will Moore and Wayne Luk, editors, Abingdon EE & CS

- Books, Oxford, England, 1994, pp. 182-191. (*Proceedings*, International Workshop on Field-Programmable Logic, Oxford, 1993.)
- J. M. Arnold, D. A. Buell, D. Hoang, D. V. Pryor, N. Shirazi, M. R. Thistle, "Splash 2 and its applications," *Proceedings*, International Conference on Computer Design, Cambridge, 1993, pp. 482-486.
- J. M. Arnold, D. A. Buell, and E. G. Davis, "Splash 2," *Proceedings*, Fourth Annual ACM Symposium on Parallel Algorithms and Architectures, San Diego, 1992, pp. 316-322.
- D. A. Buell, "The interplay between algorithms and architectures: Two examples," *Proceedings*, Frontiers of Supercomputing II, Los Alamos, New Mexico, 1990.
- D. M. Chiarulli, W. G. Rudd, and D. A. Buell, "DRAFT—A dynamically reconfigurable processor for integer arithmetic," *Proceedings*, 7th International Symposium on Computer Arithmetic, Urbana, Illinois, 1985, pp. 309-317.
- D. A. Buell, "On a problem involving partitions," *Congressus Numerantium*, v. 44, 1984, pp. 191-200.
- D. H. Kraft and D. A. Buell, "Advances in a Bayesian decision model of user stopping behavior for scanning the output of an information retrieval system," *Research and Development in Information Retrieval* (Proceedings of the 3rd joint BCS/ACM symposium), Cambridge: University of Cambridge, 1984, pp. 421-433.
- W. G. Rudd, D. A. Buell, and D. M. Chiarulli, "A high performance factoring machine," *Proceedings*, 11th Annual International Symposium on Computer Architecture, Ann Arbor, Michigan, 1984, pp. 297-300.
- D. A. Buell and D. H. Kraft, "LIARS—A software environment for testing query processing strategies," *Lecture Notes in Computer Science #146*, G. Salton and H.-J. Schneider, eds., Berlin: Springer-Verlag, 1983, pp. 20-27.
- D. A. Buell, "On the computation of unitary hyperperfect numbers," *Congressus Numerantium*, v. 34, 1982, pp. 191-206.
- D. A. Buell and D. H. Kraft, "Generalizations of Boolean query processing," *Proceedings*, ACM '82 Conference, Dallas, Texas, 1982.
- D. A. Buell and D. H. Kraft, "Evaluation of fuzzy retrieval systems," *Proceedings*, Annual Meeting of the American Society for Information Science, Washington, D. C., 1981.
- D. A. Buell and D. H. Kraft, "Performance measurement in a fuzzy retrieval environment," *ACM SIGIR Forum*, v. 16, 1981, pp. 56-62. (Pro-

ceedings of the Fourth Annual International ACM SIGIR Conference, Oakland, California, 1981)

- D. A. Buell, "Computer computation of class groups of quadratic fields," *Congressus Numerantium*, v. 22, 1978, pp. 3-12. (Text of invited address at the Eighth Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, September 1978)

Patent:

- U. S. Patent number 4,748,585, "Processor utilizing reconfigurable process segments to accommodate data word length," held jointly with Donald M. Chiarulli and Walter G. Rudd.

Technical Reports and Other Publications:

- D. A. Buell, "An Analysis of the 11/06/2012 Richland County General Election," Draft reports for the League of Women Voters of South Carolina and submitted to the Richland County Board of Elections and Voter Registration, 11/23/2012, 12/02/2012, and 12/19/2012, available at <http://www.lwvsc.org/votingtechnology.html>.
- D. A. Buell, "An Audit of the South Carolina 2012 Republican Presidential Preference Primary of January 21, 2012 (Interim Report 2/24/2012)," available at <http://www.lwvsc.org/votingtechnology.html>.
- K. Dohi, Y. Shibata, T. Hamada, T. Masada, K. Oguri, and D. Buell, "Implementation of a programming environment with a multithread model for reconfigurable systems", *ACM SIGARCH Computer Architecture News*, v. 38, 2011, pp. 40-45.
- R. Schnabel, D. Buell, J. Goode, J. S. Moore, and C. Stephenson, "An open dialogue concerning the state of education policy in computer science", *ACM SIGCSE Bulletin*, v. 40, 2008, pp. 114-115.
- D. A. Buell and C. Bays, "Electronic voting machines in South Carolina," white paper prepared for the National Research Council, Computer Science and Telecommunications Board, project on electronic voting, 2004.
- J. P. Davis, D. A. Buell and S. Akella, "SoC methods and architecture for realizing fast cryptographic computing engines," (USC Technical Report CSCE TR-2002-002).
- D. A. Buell and N. Shirazi, "The Splash 2 Tutorial," SRC Technical Report TR-92-87, 1992.
- D. A. Buell, "Sorting on Splash 2," SRC Technical Report TR-92-78, 1992.

- D. A. Buell, "Broadcast and total exchange in supertoroidal networks," SRC Technical Report TR-91-48, 1991.
- D. A. Buell, "Supertoroidal networks, FFT butterflies, and cube-connected-cycles." SRC Technical Report TR-91-45, 1991.
- D. A. Buell and J. Young, "Some large primes and the Sierpinski problem," SRC Technical Report TR-88-004.
- D. A. Buell, *et al.*, "Parallel algorithms and architectures: Report of a workshop," *The Journal of Supercomputing*, v. 1, 1988, 301-325.
- D. A. Buell, "A note on long Cunningham chains," LSU Computer Science Technical Report 85-027.
- D. A. Buell, "On determining the rank of certain elliptic curves," LSU Computer Science Technical Report 84-023.
- D. A. Buell and R. H. Hudson, "Sequences in power residue classes," (extended version of the paper with the same title) LSU Computer Science Technical Report 84-003.
- D. A. Buell and R. H. Hudson, "On runs of consecutive quadratic residues and quadratic nonresidues," (extended version of the paper with the same title) LSU Computer Science Technical Report 83-017.
- D. A. Buell, "The new cryptography," LSU Computer Science Technical Report 82-022.
- D. A. Buell, "Some factorings from the Cunningham Table," LSU Computer Science Technical Report 82-013.
- L. J. Waguespack and D. A. Buell, "A language for the specification of software directly as trees," LSU Computer Science Technical Report 82-005.
- K. S. Williams and D. A. Buell, "Is there an octic reciprocity law of Scholz type?," *The American Mathematical Monthly*, v. 85, 1978, pp. 483-484.

Students Supervised, 2000-present:

- Connor Bain, B.S.C.S. Honors Thesis 2015, joint supervision with H. R. Cooley.
- Richard Walker, Ph.D. 2014, joint supervision with H. R. Cooley.
- Andrew Ball, B.S.C.S. Honors Thesis 2013, "Augmented Reality for 'Ghosts of the Horseshoe'."
- John Hodgson, M.S. 2012, "Desperate Fishwives: History Simulation for Teaching Early Modern British History."
- Maliek McKnight, B.S.C.S. Honors Thesis 2012.

- Xizhou Feng, Ph.D. 2006, “High performance, Bayesian-based phylogenetic inference framework.”
- Soumya Ragunathan, M.S. 2005, “Snort processing on a reconfigurable computer.”
- Heather Wake, B.S. Honors Thesis 2004, “Porting EDIF netlists for congruential sieves to the Viva environment.”
- Feng Yue, M.S. 2003, “A parallel implementation of UPGMA algorithm.”
- Pradeep Kancharla, M.S. 2003, “The Advanced Encryption Standard on a reconfigurable computer.”

Other Selected Presentations:

- Seminar presentations on critical interactives with Dr. H. R. Cooley: Coastal Carolina University, September 2014; Wake Forest University, February 2013; University of North Carolina Asheville, February 2013; University of Arizona, October 2012.
- Invited panel presentation, Election Verification Network annual conference, Santa Fe, New Mexico, March 2012.
- Seminar presentations on gaming and the humanities, with Dr. H. R. Cooley, Georgia Tech, February 2012.
- Invited lecture, Discrete Mathematics and Algorithms conference, Clemson University, October 2010.
- Visiting Lectures, Department of Mathematics, University of Florida, November 2010.
- Tutorial, SC2006 (Supercomputing), Tampa, Florida, November 2006.
- Keynote address, Reconfigurable Systems Summer Institute, NCSA, Urbana, Illinois, July 2006.
- Tutorial, SC2005 (Supercomputing), Seattle, Washington, November 2005.
- Keynote address, Reconfigurable Systems Summer Institute, NCSA, Urbana, Illinois, July 2005.
- Seminar presentation in the Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, New York, 24 February 2005.
- Seminar presentation in the Department of Electrical and Computer Engineering, Binghamton University, Binghamton, New York, 10 February 2005.
- Panel presentation, Ohio Supercomputer Center, Springfield, Ohio, 5 October 2004.

- Seminar presentation in the Department of Computer Science, University of New Orleans, 30 September 2004.
- Seminar presentation in the Department of Computer Science, University of Pittsburgh, November 2004.
- Tutorial, SC2004 (Supercomputing), Pittsburgh, Pennsylvania, November 2004.
- Tutorial, SC2003 (Supercomputing), Phoenix, Arizona, November 2003.
- Tutorial, SC2002 (Supercomputing), Baltimore, Maryland, November 2002.
- Tutorial on reconfigurable computing, MAPLD 2003, Washington, DC, September 2003.
- Phoenix 2001 Conference on Information Warfare, Colorado Springs, Colorado, September 2001.
- Institute for Mathematics and its Applications Workshop on Data Mining and Industrial Applications Minneapolis, Minnesota, November, 1996.
- Invited address, Canadian Number Theory Association, Ottawa, Ontario, August, 1996.
- Invited address, Third FPGA/PLD Design Conference, Tokyo, Japan, July, 1995.
- Technology 2002 (National Technology Transfer Conference), Baltimore, Maryland, December, 1992.
- Fourth ACM Symposium on Parallel Algorithms and Architectures, San Diego, California, June, 1992.
- Fall Lecturer, Oregon Council for Advanced Technology Education, Corvallis—Eugene—Portland, October 1990.
- Invited panel presentation, Frontiers of Supercomputing II, Los Alamos, New Mexico, August 1990.
- Invited short talk at the Regional Meeting of the American Mathematical Society, Mobile, Alabama, May 1985.
- Eleventh Annual International Symposium on Computer Architecture, Ann Arbor, Michigan, June 1984.
- Fourteenth Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, September 1984.
- Invited talk at the Sino-American Symposium on Fuzzy Mathematics and Analysis with Applications to Electric Power Systems, Beijing, China, July 1984.
- Fifteenth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Baton Rouge, Louisiana, March 1984.

Invited short talk at the Annual Meeting of the American Mathematical Society, Denver, Colorado, January 1983.

Invited short talk at the Summer Meeting of the American Mathematical Society, Toronto, Ontario, August 1982.

Fifth Annual ACM SIGIR Conference, Berlin, Germany, May 1982.

Eleventh Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, October 1981.

Fourth Annual ACM SIGIR Conference, Oakland, California, May-June 1981.

Invited address at the Eighth Manitoba Conference on Numerical Mathematics and Computing, Winnipeg, Manitoba, September 1978.