STATE OF NORTH CAROLINA

COUNTY OF WAKE

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION
20 CVS 5035

NORTH CAROLINA STATE CONFERENCE	)	
OF THE NAACP, et al.,	)	
	)	
Plaintiffs,	)	
	)	
	)	**AFFIDAVIT OF DUNCAN**
v.	)	**BUELL**
	)	
NORTH CAROLINA STATE BOARD OF	)	
ELECTIONS, et al.,	)	
	)	
Defendants,	)	

AFFIDAVIT OF DUNCAN BUELL

I, Duncan Buell, do hereby say under oath the following:

1. I am of legal age and competent to provide this affidavit. All the information herein is based on my own personal knowledge unless otherwise indicated.

2. My background, qualifications, and professional affiliations are set forth in my curriculum vitae, which is attached as Exhibit A.

SUMMARY

3. The ExpressVote voting system currently being used in North Carolina suffers from many vulnerabilities that threaten the integrity of elections in the state, including (1) it does not produce a voter-verifiable output, (2) it is vulnerable to cyberattacks and hacking, (3) the

protocols normally used by county elections offices are not sufficient to prevent successful hacking attempts from sophisticated actors, and (4) there is no means by which voters can reliably determine whether or not their selections were altered.

4. Barcode-based voting systems like the ExpressVote are not voter-verifiable because the barcode used for tabulation of votes cannot meaningfully be "read" and thus verified by the voter. Voters are no doubt familiar with barcodes used for checkout scanning in retail stores, and some of these do have the decoding of the barcode as numbers. Even if the ExpressVote barcode had these numbers (it does not), the numbers would be meaningless to a voter. The barcode does not encode candidate and contest by name, but rather the x-y coordinate position where the bubble would be filled in for a hand-marked paper ballot equivalent to the electronic version. Even if the barcode had the decoded numbers, voters would not know how to interpret these values unless, say, a poster-sized version of every hand-marked equivalent were available on the wall of the polling place (this is infeasible at vote centers with hundreds of ballot styles), or some version of an x-y coordinate "cheat sheet" were provided to every voter.

5. Because the ExpressVote is a computer and the configuration of the ballot for the voter is done by a USB drive that is itself a computer, a hacked ExpressVote could change votes as represented in the barcode. The voter would not be able to detect this. In addition, there is no reliable way to distinguish a hacked ExpressVote that changed votes from the occasional expected error by the voter in making choices.

6. Although it is frequently stated that devices like the ExpressVote are not connected to the Internet, to someone expert in computer security this is almost certainly false. The transmission of voter registration databases to the counties, the configuration of the ExpressVotes by county officials, and the transmission of results to the media and candidates as votes are tabulated leaves

open several paths for sufficient "connection" to allow remote hacking of the county central computers and by extension the ExpressVote computers.

7. Several studies have shown that the use of voting computers increases waiting time for voters. This means that voters will spend more time in the polling places where they can be exposed to Covid-19 infecting other voters. Although some mitigation can take place by sanitizing equipment, this is not a guarantee against infection and it will increase wait time.

8. I have done extensive analysis of the results presented by the earlier iVotronic voting computers and their corresponding Unity software for use at county election headquarters. My analysis shows a great many software flaws that could only have come from a failure by ES&S to follow best practices for software design and implementation. I have seen some output from more recent ES&S software that suggests that much of the previous (and flawed) software has been incorporated in the newer ElectionWare package to be used at county headquarters for configuring elections and for tabulating results using the ExpressVote voting computers. I see no reason to believe that the truly fundamental (that is, sophomore-level-undergraduate) flaws in the previous system have been fixed in the newer system, and ES&S has failed to provide publicly available information demonstrating that their software now meets a minimal standard for quality.

QUALIFICATIONS AND MATERIALS REVIEWED

9. I am a professor in the Department of Computer Science and Engineering at the University of South Carolina, where I hold the NCR endowed professorship in computer science and engineering.

10. In 1971, I earned a B.S. in mathematics from the University of Arizona. In 1972, I earned an M.A. in mathematics from the University of Michigan. In 1976, I earned a Ph.D. in

mathematics, with an emphasis in number theory, from the University of Illinois at Chicago. A copy of my resume is available on my university website at http://www.cse.sc.edu/duncanbuell.

11. I have been programming computers for more than 50 years and have been employed as a computer scientist since 1977. My experience includes work with computers, computer applications, computer operations, management of large computer networks, including networks utilizing the Internet, and in presentation of computing technology solutions to the general public.

12. Prior to moving into my current position, I was employed for just under 15 years, with various job titles and duties, at the Supercomputing Research Center, later named the Center for Computing Sciences, of the Institute for Defense Analyses (IDA), a Federally Funded Research and Development Center supporting the National Security Agency (NSA). Our primary mission at SRC/CCS was to conduct research on high performance computing systems and computational mathematics to ensure that those computing systems would be suitable for use by NSA, since the NSA workload has technical characteristics different from most high-end computations like weather modelling. While at IDA, I played a leading role in a group that received a Meritorious Unit Citation from Director of Central Intelligence George Tenet for what was then "the largest single computation ever made" in the United States intelligence community.

13. Since 2000, I have been a Professor in the Department of Computer Science and Engineering at the University of South Carolina. From 2000 to 2009, I served as Chair of that department. During 2005-2006 I served as Interim Dean of the College of Engineering and Information Technology at the University of South Carolina. In my management capacity as department chair, my duties also included management of the college's information technology

staff and its network and computer center, which included 9 instructional labs with approximately 250 desktop computers. I was also responsible for management and operation of cluster computers, file and mail servers, and the college's network infrastructure.

14. In 2013, I was elected a Fellow of the American Association for the Advancement of Science. In 2016, I was appointed to the NCR Chair in Computer Science and Engineering at the University of South Carolina.

15. My current research interests include electronic voting systems, digital humanities, computer security, computational number theory, and text analysis. Over the past 40 years, I have published articles in peer-reviewed journals and/or lectured and taught on each of these topics.

16. Since about 2004 I have worked with the League of Women Voters of South Carolina as an unpaid consultant on the issue of electronic voting systems. South Carolina used statewide the ES&S iVotronic direct recording electronic (DRE) voting computers and the corresponding Unity software. Beginning in summer 2010, I worked with Frank Heindel, Chip Moore, Eleanor Hare, and Barbara Zia on acquisition by FOIA of the election data from the 2010 elections in South Carolina and on the analysis of that data. That work, based on data acquired by FOIA, culminated in an academic paper that I presented at the annual USENIX EVT/WOTE (Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) conference in August 2011.

17. My work with the LWVSC has continued. I have acquired and analyzed the data from the 2012, 2014, 2016, and 2018 elections in South Carolina, and I have also analyzed ES&S DRE-voting system data in more limited quantities from Colorado, Kansas, North Carolina, Pennsylvania, and Texas.

18. I have probably done more extensive analysis on ES&S election data than anyone else in the world outside of employees of ES&S. This has come largely because South Carolina has declared all the election data to be public record and made it available and because the use state wide of a single system has made meaningful and possible a statewide comparison of usage of the voting system.

19. I have conducted research on polling place operations and county-level central tabulation operations in South Carolina, which has included assessing wait times and voting times with voting computers (like DREs and BMDs). I have been a poll observer and have watched voter behavior and poll workers[1] in using both DREs and BMDs.

20. I was appointed by South Carolina Governor Henry McMaster to the Richland County Board of Voter Registration and Elections in the spring of 2019 and continue to serve on that board as a commissioner. In that role I have had the opportunity to be educated about and to observe the operation of the ES&S ExpressVote 2.1 voting computers that were acquired in summer 2019 for statewide use in South Carolina and which have replaced the iVotronic system.[2]

21. I have reviewed technical manuals for the ExpressVote computers and the technical details of the 2019 (successful) bid by ES&S for the South Carolina statewide purchase of ExpressVote computers. As a member of the Richland County Board of Voter Registration and Elections, I have observed elections conducted using ExpressVotes in November 2019 and the Presidential Preference Primary in February 2020.

SIMILARITIES BETWEEN ES&S SYSTEMS

[1] South Carolina refers to most poll workers as “poll managers” and refers to the person in charge of polling place operations as a “poll clerk”. I will combine both and refer to them more generically as “poll workers”.

[2] I have not, however, been exposed to material marked as “confidential” by the South Carolina State Election Commission.

22. There have been several versions of voting systems from ES&S that use some version of the ExpressVote hardware and some version of the accompanying software for the ExpressVote, for the DS200, DS450, and/or DS850 optical scanners, and for the ElectionWare software used at county headquarters for configuring an election for the ExpressVotes and the scanners and for tabulating results at the close of an election.

23. This case concerns version 5.2.4.0 of the system. This is the version that was EAC certified on 5 June 2018, using ElectionWare 4.7.1.1. There have been eight newer certifications since 5.2.4.0 was certified, including three major updates to ElectionWare. The South Carolina system that was originally delivered was version 6.0.2.0, EAC certified October 2018. Version 6.0.4.0 was certified 3 May 2019, and Version 6.1.0.0 was certified 24 September 2019. I am in possession of a set of manuals for ExpressVote voting computers and accompanying scanners and for ElectionWare version 4.6 (earlier than the North Carolina version being considered), dated 2013 and 2014. I have not had the opportunity to review manuals either for 5.2.4.0 or for the version used in South Carolina.

24. I acknowledge that I have not yet read in detail the manuals for the 5.2.4.0 system that is approved for use in North Carolina; I would if it was available to me but it is not available to the general public. However, my understanding from the earlier manuals and from the recent use by South Carolina is that very little of the basic software features and capabilities has changed, and thus that my knowledge is as up to date as would be needed. It is virtually unknown in the software industry for basic capabilities included in an earlier version to be deleted in an intermediate version and then reinstated in a later version. These kinds of changes are usually restricted to human factors issues and not to the fundamental manner in which the software does what it is purported to do.

25. From a careful reading of the earlier (ElectionWare 4.6) manuals as well as the specifics of the bid to South Carolina, it does not appear that there is any reason to believe that major changes in the software have occurred, and thus that the 5.2.4.0 version for North Carolina differs very little from the manuals I have read or from the system I have experience in observing. The substantive change with Version 6.1.0.0 is to run on a Windows 10 operating system rather than on Windows 7 that has been declared obsolete by Microsoft, but this is unlikely to have involved major changes to the functionality of the programs.

BARCODES ARE NOT VOTER-VERIFIABLE

26. A primary problem with barcode-based BMDs is that they are not "voter-verifiable". The word "verifiable", in any dictionary usage, means that a person (in this case, the voter) can determine the truth of, or prove the truth of, that which is "verified". Certainly it is *possible* for a voter to "verify" the truth of the text of her choices *as printed* on the ballot card. However, that text may or may not be connected to the tabulation of her vote by the election system.

27. What is encoded in the barcodes for the ExpressVote system is not the candidate-contest pair for which candidate should get a vote for which contest. Rather, what is encoded are the x-y coordinates on what would be the position of the fill-in bubble for that candidate, for that contest, on a hand-markable paper ballot that the voter would have received if she had asked for a paper mail-in absentee ballot. Even if the voter were able to decode the barcode, the barcode information would be useless in determining for whom she was voting unless she had access to the x-y coordinates from the hand-markable version of the ballot.

28. The barcodes are, therefore, "readable" by a voter, but not "verifiable" by a voter, without a complete presentation of the paper version of that ballot style for that voter. In practice, that will never happen, and thus the barcodes will never be "verifiable" by a voter. This

is, and should be, sufficient reason to reject a barcode-based voting system for any jurisdiction that claims that voters can "verify" their ballot selections.

29. An additional problem with barcode-based systems is that the summary text that is provided to the voter indicates only the selections made by the voter, not the entire list of options that were available to the voter. This can be especially problematic for textual items like constitutional amendments, because all that is displayed is "yes" or "no".

BARCODES CAN BE HACKED, AND VOTERS CANNOT DETECT HACKING

30. A second problem with BMDs using barcodes, and with most BMDs in general, including the ExpressVote, is that individual voters will have no basis on which to declare that an "error" has been made by the BMD and not by the voter herself. As has been made clear by Stark [Stark 2019], there is no reliable way to detect hacked BMDs. "Errors" in the ballot cards would be noticed anecdotally by voters, but no test could exist that errors were not voter errors instead of malware in the BMD. The only reliable test that BMDs were performing correctly is second-party observation of actual cast votes, and that violates the voter's right to anonymity.

31. Detection of hacking is also hampered by the fact that most voters do not check the printed ballot card. As has been observed by DeMillo, Kadel, and Marks [DeMillo 2018], and tested as an experiment by Bernhard et al. [Bernhard 2020], voters do not check the card, even when they are encouraged to check the card. The experiment by Bernhard et al. also showed that voters reported only a small fraction of the total number of "errors" on the printed ballot card. Finally, we remark that there is with the ExpressVote no permanent record of the voter's intent; the image presented on the screen and what the voter views, with boxes checked by the voter, is ephemeral and disappears completely.

32. A major consideration with regard to hacking is that software can be configured to hide the existence of hacking, especially in a situation in which not all the results need to be corrupted. It would be easy (and expected) that malware in the ExpressVote that would record votes other than what the voter saw on the screen would do so only some of the time, at random, in the small quantity that would change the outcome of an election expected to be close.

33. The assumption that hacking would be likely is not mere speculation. The Department of Homeland Security and the Federal Bureau of Investigation released a joint bulletin in 2019 announcing their determination that Russa had done reconnaissance and hacking efforts against state election networks, including that of North Carolina, in 2016. The "Mueller Report" described the capability and efforts of Russia to interfere in the 2016 election, and there are ongoing reports that interference is planned for November 2020. As one of the "battleground" states, North Carolina should expect to be attacked.

34. Hacking an ExpressVote-based election system, if done by skilled adversaries, would be virtually impossible to detect. The best of malware designers know how to insert the malware, perform the subversion of the computation, and then erase all record of the malware's being in the system. Indeed, in virtually all the hacks of existing election equipment, the ability to remove all trace of the malware's having been in place has been a routine part of the hack. This is especially insidious in technology use in an election, because there is no externally-available ground truth against which to corroborate the results obtained from the computers. Notwithstanding pre-election and election-day polling bringing results into question, the actual results of an election are only and exactly what is tabulated after the polls close.

35. A security review by ATSEC, an information security company, for the state of California, found a number of vulnerabilities in version 5.2.1.0 of the ES&S voting system. A

number of these vulnerabilities were, in my opinion, quite egregious, things that I would not have permitted undergraduate computer science students to do without being marked down. They include hard-coded passwords, a failure to update the code with security patches, a failure to use full disk encryption or to encrypt the files on the removable USB drives, and the use of default configurations.

36. These are routine security problems that are usually observed in conducting a post-mortem after a hack or a breach. They are problems that we teach undergraduates to address if they wish to be considered knowledgeable in computer security. Although the ATSEC review for California was of a slightly earlier version (5.2.1.0 and not 5.2.4.0), at the very least the 5.2.4.0 version should not be adopted without a detailed demonstration that all these vulnerabilities have been removed in the version that North Carolina would plan to adopt.

VOTING SYSTEMS THAT USE THE EXPRESSVOTE ARE OFTEN CONNECTED TO THE INTERNET

37. Election officials, including those at the state and county level in South Carolina, often state that voting systems like the ExpressVote cannot be hacked because they are never connected to the Internet. Although it is narrowly true that the ExpressVotes are not *directly* connected to the Internet, in the sense that a desktop computer has a wired connection or a laptop has a wireless connection, that is not the only “connection” that is a concern. The following is a description of ways in which a county’s ExpressVote computers or the optical scanners could be indirectly connected to the Internet and are thus subject to hacking and malware.

38. In each case, although these could be argued to be hypothetical, the indirect connection would seem to be the most natural thing for election officials to do, and thus the burden of proof would lie on the election officials to demonstrate conclusively the absence of that indirect connection. The potential for this kind of indirect connection was sufficiently significant that it

was specifically warned against in the National Academies' report (page 87): "Malware is not easily detected. It can be introduced into systems via … removable media with ballot definition files …".

39. Internet connection capabilities exist in Texas counties using the ExpressVote. The agreement between Travis County, Texas, and ES&S, filed for the record on 7 August 2018, for version 5.2.2.0, includes a diagram dated 5 December 2017 of the election system connected to the Internet for reporting of results. A similar agreement for the state of Michigan, effective date 1 March 2017, lists prices for landline and wireless modems for the DS200 scanners. Internet connection capability would seem to be a standard part of the ES&S offering.

40. It is routine in many states for the statewide voter registration database to have an online version of the database. This permits voters to enter their personal information and verify the polling place and upcoming ballot choices, among other things. It is routine, and done in South Carolina, and almost certainly true in any state that does not have same-day registration, that the county's up-to-date voter registration database is transmitted from the state office to the county only just prior to an election. That county database is then loaded at county headquarters, by county staff, onto electronic pollbooks for use in precinct polling places.

41. This provides the first opportunity for indirect connection to the Internet. The county database is certain to be transmitted electronically. If this transmission comes from a pristine copy of the state database, from a computer kept offline an updated only through very strict protocols to prevent infection, and if this transmission were done on one-time media (like CD/DVD disks), then this would not be a connection to the Internet.

42. If, however, the transmission is made from a database that is kept online, even with security practices in place, then the data delivered to the county does come as an Internet connection, and the claim of "not connected" is only as good as the security practices in place.

43. The second vulnerability comes in configuring the scanners, ExpressVotes, and e-pollbooks at county headquarters. This is a substantial task in a large county. In my own county, Richland, with about 265,000 registered voters, we will configure about one thousand ExpressVotes and more than150 scanners and e-pollbooks for each of the 149 precincts and satellite voting locations, with about 100 different ballot styles requiring individual configurations[3,4]. The scale of this is not much different from what I have been told in discussions with officials in Memphis, Tennessee, in Colorado, and in Birmingham, Alabama.

44. Configuration in any large county cannot be done manually, and thus the configuration of ballot styles for the ExpressVotes (or for any BMD from any vendor) is done from a computer at county headquarters, using USB memory drives for at least the ExpressVotes and the scanners. If the computer doing the configuration has ever been connected (directly or indirectly) to the Internet, then malware could exist that could propagate to a hacked configuration of the ExpressVotes or the scanners, or both. If this is the computer that has received the voter registration database in a manner that connects that database indirectly to the Internet, then in fact the county's central computer has been connected to the Internet.

45. ES&S asserts in its documentation that the neither the ExpressVote nor the scanner stores any information. They presumably function as computers with built-in programs but that use the USB drives as their only memory for retrieving configuration (ballot styles, and such) and

[3] We use the term "satellite location" instead of the more common term "vote center".

[4] The South Carolina e-pollbooks are a version local to the state. Only one e-pollbook in a precinct will have the database, and the others will connect with a wired connection. Other pollbook systems might require the database on each pollbook, which would double or triple the number of installations.

storing event logs and results. That is, all the memory for data storage for the ExpressVotes and the scanners is part of the memory of the USB drives, not internal to the ExpressVotes or the scanners. This means that it is absolutely critical that the USB drives have never been connected to a computer that has been connected to the Internet, and thus critical that the computer that loads the configuration data onto the USB drives has never been connected to the Internet. The storage of votes and results is done only on the USB drives, and that storage is controlled by software on the USB drives themselves, so it is crucial that the programs on the USB drives that control what results are stored have not been tampered with.

46. The third major vulnerability regarding connection to the Internet comes after polls are closed and results are being tabulated. In the system I have witnessed in Richland County, the USB drives from the scanners (which contain the results from each precinct) and from the ExpressVotes are plugged into the central tabulation computer (which is the same computer that configured the USB drives prior to the election), and the results data from the USB drives is uploaded for central tabulation. This permits county-wide results to be accumulated.

47. The agreements between ES&S and Travis County, Texas, and the state of Michigan, include the ability for a second USB drive from the scanners to be used to upload data through the Internet for reporting to the media, candidates, and the state headquarters. That configuration, as presented in the ES&S agreements, requires doubling the number of computers at county headquarters from two (one, plus a backup) to four (one and a backup not connected to the Internet, and one and a backup connected to the Internet). This does not seem to be the normal mode of operations, even for a moderately large county such as Richland.

48. The vulnerability exists because candidates and the media want results throughout Election Night, in real time, so the partial results are produced at intervals for the public. Were I

to design a process for this, I would have the (unconnected) computer write those results to a CD/DVD disk to be taken to a computer connected to the Internet for upload and public viewing. I would then shred the disk, and I would use a new disk for the next upload and display to the public.

49. This one-way transmission of results (from an unconnected computer to a connected computer) is not what seems to be normal in many jurisdictions across the country. What seems to be more normal is that transmission is made not with a one-time CD/DVD disk, but using yet another USB drive that is then brought back from the connected computer to the "unconnected" computer.

50. As mentioned above, it is exactly this insecure indirect connection to the Internet that was specifically warned against in the report from the National Academies of Science, Engineering, and Medicine [National Academies 2018]. USB drives are in fact tiny computers, which can be programmed and reprogrammed and whose programming (not the data they record, but the program that records the data) can be infected with malware.

51. These connections, either direct or indirect, can also lead to compromise, corruption, or hacking, from both vendor and third-party insiders, or through vendor or third-party insiders with internet connections to the election system, and there is ample evidence that third-party contractors are given remote (internet) access to the election system. This was learned recently in Georgia as part of the Curling litigation. There are records of last-minute connections to the Durham County (NC) voter registration system prior to the 2016 election. Going further back to Venango County (PA), the election office's IT staff person was only part-time with elections and administered the election software system from a remote connection from his regular job.

52. Two remarks are in order. The first is that there is a very broad attack surface for an election. The movement of data from a state database to county-level computers to hundreds of scanners, ExpressVotes, and e-pollbooks leaves open any number of places where naivete about computer security or simply complacency or carelessness would provide a path for malware to enter the process.

53. Second, security for elections is subject to what is known as the "watering hole" phenomenon. The opportunity for corrupting an election happens at very obvious times, in the run-up to the election itself. The election configuration must be finalized by 45 days prior to Election Day in order to meet UOCAVA requirements. Voting computers and ballot styles must be configured prior to the beginning of absentee balloting. Tabulation of results is prepared for in the days prior to Election Day. Those who would corrupt elections do not need to be constantly changing things inside the "unconnected" computer. They need only be able to gain access, leave their ability dormant, and then use that access at the appropriate times to corrupt an election.

VOTING ON THE EXPRESSVOTE IN THE COVID-19 ERA

54. There have been concerns raised around the country about whether elections held in person are going to be safe or whether they will lead to significant spikes in Covid-19 infections. This is, and should be, a great concern to voters and to election officials and the poll workers who would be serving during an election.

55. Safety is a concern both for the voters and for election officials and poll workers, as I have recently observed in the 9 June 2020 primary in Richland County and elsewhere in the state. All jurisdictions I have talked with had trouble getting enough poll workers. In Richland County, we had just over half as many poll clerks and poll managers as we should have had

(based on state law). We combined precincts into polling places, and we observed all the problems one could predict when too many voters are voting at a single location with insufficiently many poll workers and hardware resources.

56. A major health concern should be simply the time that voters will spend at the polling place in close quarters with a large number of other voters. It has been documented that jurisdictions that use voting computers suffer from longer lines than do jurisdictions using hand marked paper ballots [Stewart 2009, Stewart 2015]. This is in part due to the fact that expanding capability for voters casting ballots in parallel with other voters requires only more private table space with when voters vote on hand marked paper. Expanding capability using voting computers is expensive and cannot/will not be done as needed during Election Day. Funding of elections being what it is, one finds it rare that jurisdictions buy more than the minimum number of computers needed.

57. An additional contribution to longer lines is the basic setup time for using a voting computer like the ExpressVote. With hand marked paper, a voter is given the appropriate ballot and is then free to vote, no further intervention or assistance by poll workers is needed. With the ExpressVote and scanners, there is an automatic delay for each voter of about six seconds for insertion of the ballot card, and a delay of about the same length for extracting the ballot card. Unless there are e-pollbooks in use that print the ballot style barcode at the top of the ballot card when the voter checks in, there is an additional delay while the poll worker selects the right ballot style.

58. In Richland County, for absentee voting (resembling a North Carolina vote center), with 149 different precincts, I measured in a November 2019 election and the February 2020 Presidential Preference Primary this selection time at about eight seconds, and in both cases,

there seemed to be only one ballot style in my precinct, which should have made selection very simple. That setup time would be longer for vote centers (as are used extensively in North Carolina) and in general elections when precincts could have multiple ballot styles.

59. Longer lines therefore, especially with six-foot distancing required, will mean voters spend more time waiting to vote and thus more time in a position to become infected by others.

60. Perhaps a greater concern is that of sanitizing the election equipment itself. It has been determined that ExpressVote computers will work if one uses a Q-tip to "press" the virtual buttons; an actual finger touch is not necessary. This would permit an inexpensive way to diminish Covid-19 virus buildup on the screens. But this in itself is not a guarantee that the screens would not accumulate virus. One could expect poll workers to be careful and consistent, but it is unlikely that all voters would be equally so. Although a Q-tip could be used to obviate the need for finger touch, a Q-tip that was handled by the voter while waiting in line will easily pick up virus from the voter's hand and transfer it to the screen.

61. I have been told that the ES&S document dated March 2020 is still the official document from the vendor regarding cleaning and disinfecting the ExpressVotes, and this document is inadequate. The instructions are lightly to dampen a soft cloth with isopropyl alcohol, and then to wipe the screen gently. The guidance specifically warns against using too much fluid or harsher disinfecting chemicals. Taken together, I read it as reasonable guidance for maintaining clean voting equipment under normal circumstances, but really quite weak in the present situation with Covid-19.

SOFTWARE IS HARD TO GET RIGHT, AND QUESTIONS ABOUT ES&S SOFTWARE QUALITY ARE LEGITIMATE

62. Although the usual term is “voting machine”, the proper term that should be used for devices like the ES&S ExpressVote is “voting computer”. These are not mechanical devices like the lever machines of past elections; these are computers running third party operating systems (Windows Embedded in the case of the ExpressVotes delivered to South Carolina), with internal memory that stores vendor-written programs, and software that accesses data and configuration information from external USB storage devices that are plugged into the ExpressVote via standard USB interfaces.

63. The ES&S ExpressVote is a computer, just as the previous hardware offering from ES&S, the iVotronic, was a computer, and it needs to be treated as such. They are different computers, but they are still both computers, with all the caveats and flaws that come with computers running software. The central tabulation computer running ElectionWare is also a computer, running third party software as well as ES&S-developed software. The EVEREST report done for the state of Ohio, released in December 2007, stated that the iVotronic system (identical to what was used in South Carolina), including the Unity central tabulation, configuration, and report software, had more than 500 thousand lines of code, written in nine different programming languages, running on multiple hardware platforms. This was a complicated computer system.

64. The ExpressVote and ElectionWare system is unlikely to be any simpler than the iVotronic, since it must accommodate the ExpressVote 2.1 either in BMD-only or in BMD-and-tabulation mode, the DS200 optical scanners used in precincts use the Linux operating system, the DS450 scanners usually used in larger jurisdictions, and ElectionWare running on a Windows computer.

65. Although much of the ElectionWare software, as well as the software running in the ExpressVote, the DS200 scanner, and the DS450 scanner is likely rewritten, questions should continue about the quality of the ES&S software and the ability to determine what problems have occurred, should problems or challenges to results occur.

66. I have analyzed the event logs from the DS200 and the DS450 scanners used in Richland County in the 9 June 2020 statewide primary election. Although all my prior experience with ES&S event logs has included their use of codes for events, none of the DS450 events, produced as part of scanning absentee-by-mail ballots, have codes. All the codes in that data are simply "Undefined". Although this in and of itself might not be a problem, it would at the very least make it more difficult to audit the results from the DS450, and what it really suggests is that either through design or carelessness, a substantial step backward was taken with the DS450 in writing software that tracks the computation performed. A robust and clear recording of events, with codes, is necessary in order to understand and have confidence that the software modules through which the computation proceeded are exactly as they should be, with no modifications from the code provided by the vendor and checked for veracity prior to use. I find it also disconcerting that one of the scanners used was alleged to have serial number 000000000. I acknowledge that the nature of conducting elections makes it imperative that the equipment function in the distributed locations (the precincts) on Election Day, even if they have been misconfigured, but the inability to audit data suggests a lack of high-quality software practices.

67. More insidious in the ES&S software, and indicative of a failure to observe standard best practices in software development, is the apparent possibility for the list of contests as seen by the tabulation computer at county headquarters to be different from the list as seen on the ExpressVote in the polling place.

68. This apparently is the problem that occurred in Northampton County, Pennsylvania, in its 2019 election. A change in the manner in which candidates were presented to voters was present in the ExpressVote XL, and an informational box was present on the ExpressVote screen explaining the change. Because tabulation takes place based on x-y coordinates, and (apparently) because the presentation on the ExpressVote was done with different software than was the presentation on the central tabulation computer, one candidate's votes were entirely tabulated for the informational box seen by the voters. This is doubly a flaw in software design. It is a fundamental rule of software design not to write two blocks of code to do the same thing (because they will diverge at some point and cause errors), and yet this can only be the cause of this error.

69. The fact that it is possible to have one version of the ballot in the ExpressVote and one version in the central tabulation computer indicates bad software design. This problem was mentioned in the EVEREST report. There are obviously two different software modules that configure the ballots, one for the ExpressVote and one for the central computer. This should not happen for exactly the reason seen in this error, that the two modules can produce conflicting or different output. There should be one software module that creates configuration data in two places.

70. These matters of software design are not arcane. Writing good software is difficult. Programmers tend to write code as if things will always work. Software should, however, be written as if the assumption was that it would never work. These are messages I present routinely to sophomore undergraduates in the third-semester course I have taught perhaps ten times, a course I only partly humorously refer to as "learning to program like an adult". The fact that I have observed errors in the ES&S software for which I would deduct points if they

appeared in sophomore level homework programs should speak volumes about what to expect in terms of software quality from ES&S.

71. We know that ES&S has produced software with errors in it that have led to votes being miscounted or uncounted. We can also see highly questionable output of the reporting modules. Two specific instances stand out.

72. From all these errors, problems, failures, and human factors issues, I am unable to state that ES&S follows good practices in design, testing, and quality control for its software. I have never seen the software, and I have not seen their design specifications or implementation records, so it is not clear that I can declare that they do not have good practices for design, development, and testing. I can state as my professional opinion, however, that I do not believe the observed problems would have happened if best practices (as I teach them to undergraduates) had been followed.

73. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

This, the 3 day of July, 2020

Duncan A Buell
[NAME]

I, the undersigned notary public, hereby certify that DUNCAN BUELL personally appeared before me this day and acknowledged the due execution of this AFFIDAVIT.

Witness my hand and official seal, this the 3 day of July, 2020.

Notary Public

My commission expires 06·14·2021 , 20___.

CORTNEY P NICK
NOTARY
PUBLIC
SOUTH CAROLINA

References

M. Bernhard, A. McDonald, H. Meng, J. Hwa, N. Bajaj, K. Chang, and J. A. Halderman, “Can voters detect malicious manipulation of ballot marking devices?” Proceedings, IEEE Symposium on Security and Privacy, 2019.

R. DeMillo, R. Kadel, and M. Marks, “What voters are asked to verify affects ballot verification: A quantitative analysis of voters’ memories of their ballots”, 2018, available at https://ssrn.com/abstract=3292208.

National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy*, 2018.

Philip B. Stark, “There is no reliable way to detect hacked ballot-marking devices”, arXiv:1908.08144v1, 21 August 2019.

Charles Stewart III, “Election technology and the voting experience”, Midwest Political Science Association annual meeting, 2009.

Charles Stewart III, “Managing polling place resources”, Caltech/MIT Voting Technology Project report, 2015.

Duncan A. Buell
Professor, Department of Computer Science and Engineering
NCR Professor of Computer Science and Engineering
University of South Carolina, Columbia, South Carolina 29208
buell@mailbox.sc.edu, 803-777-7848, www.cse.sc.edu/duncanbuell

Personal: 69 years old, U. S. citizen.

Experience:

July 2009—present: 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.

Computing Interests:

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 with co-PIs J. Davis and 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)
Advisory Board Member, Overseas Vote Foundation
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
National Center for Science Education, Union of Concerned Scientists

Other Scholarly and Professional Activities (selected):

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.)

Member, Board of Reviewers *Journal of Writing Analytics* 2016—present.

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. (Founded this journal with Wayne Luk, the other co-EIC.)

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:

Krystal Werfel and Stanley Dubinsky and Elizabeth Barlow and 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, *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:

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.

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, “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.

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. Kotenko, 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. (Proceedings 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 algoritm."

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.