AFFADAVIT OF RONALD L. RIVEST

RONALD L. RIVEST, being duly sworn, deposes and says the following under penalty of perjury:

BACKGROUND

1. My name is *Ronald L. Rivest.* I am an Institute Professor at the Massachusetts Institute of Technology in Cambridge, Massachusetts. I have been employed by MIT since the fall of 1974. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Wisconsin.

2. My CV and list of publications are available on my website: `http://people.csail.mit.edu/rivest`.

3. At MIT, my home department is the Department of Electrical Engineering and Computer Science. I have taught courses in computer programming, computer algorithms, cryptography, theoretical computer science, network and computer security, and elections and voting technology.

4. I am a co-author of the best-selling textbook "*Introduction to Algorithms*" (co-authored with Cormen, Leiserson, and Stein).

5. My research interests include algorithms, theoretical computer science, cryptography, machine learning, security, election integrity, and statistical methods for election auditing. I have published numerous research papers, books, and book chapters on these topics.

6. I am perhaps best known for the invention (with Adi Shamir and Len Adleman) of the *RSA public-key cryptosystem*, based on the difficulty of factoring the product of large prime numbers. This cryptosystem is widely used today to provide secure browsing and secure electronic commerce.

7. I have commercialized some of my innovations, founding companies *RSA Security*, *Verisign*, and *Peppercoin* in the security and digital payments spaces.

8. I have received numerous awards, including the prestigious ACM Turing Award (joint with Adi Shamir and Len Adleman); this award is considered by many to be the "Nobel Prize of Computer Science" (there is no actual Nobel Prize in this area).

9. I am member of the National Academy of Engineering and the National Academy of Science.

10. I have supervised graduate and undergraduate theses in many areas, including novel systems for secure voting.

11. I am on the Board of Verified Voting, a non-profit organization devoted to election integrity.

12. I am member of the *CalTech-MIT Voting Technology Project*, which has been working towards improved voting systems since 2001.

13. I am co-founder of the *Workshop on Trustworthy Elections* workshop series (WOTE, now merged with Electronic Voting Technology).

14. I have been a member of the *Technical Guidelines Development Group* (TGDC), an advisory group to the U.S. Elections Assistance Commission for the purpose of developing certification standards for election systems. I chaired the *Security and Transparency* subgroup of the TGDC.

15. I am a co-author and co-inventor (with John Wack) of the notion of "*software independence*" of a voting system: the notion that a voting system should not be vulnerable to suffering undetectable changes in the election outcome due to errors or misbehavior by the voting system software.

16. I am part of the team that fielded the "*Scantegrity*" voting system for two elections in Takoma Park, Maryland. Scantegrity is a novel voting system of the "end-to-end verifiable" type: voters can check on a website after the election to confirm that their ballot was included and counted as intended, without thereby being able to sell their votes(!).

17. I am an advisor to the *StarVote* project in Travis County (Austin) Texas, which will provide high-integrity voting systems to that county, based on both advanced cryptographic operations and statistical auditing methods.

18. I am a collaborator and co-author on the recent report "*The Future of Voting: End-to-End Verifiable Internet Voting — Specification and Feasibility Study*, produced by the Overseas Vote Foundation.

OPINION

19. I feel strongly that the security of voting systems is essential to our democracy—a voting system should accurately reveal the choice of the voters (collectively, not individually!), otherwise our democracy is lost.

20. Moreover, a voting system should not only be *accurate*, it should be *demonstrably accurate*. A voting system should produce *evidence* that is sufficient to convince a loser (and his/her supporters) that he/she lost fair and square.

    Recounts and statistical post-election audits are two powerful tools for examining evidence (paper ballots) to produce a convincing proof that an announced outcome is correct. (Or, if the unofficial outcome is incorrect, for producing a convincing proof that another candidate is the correct winner.)

For our democracy to work well, election systems should produce the best and most convincing evidence that the announced election outcomes are correct. One should ask: what will it take to convince a skeptical supporter of a losing candidate that they really lost?

Evidence of the form, "You must trust the computer here." is not likely to be adequate (nor should it be).

21. I am a strong believer that *all* elections should be based on voter-verified paper ballots, and that statistical post-election audits should be used to check that the announced outcome is consistent with the cast paper ballots.

22. Professor Philip B. Stark and I have recently published an OpEd in USA Today (Nov. 18, 2016, entitled "Still Time for an Election Audit") arguing that performing statistical audits in every state (where possible) for the 2016 U.S. Presidential election would be good practice, and would not be very expensive.

23. I would recommend statistical audits for checking the correctness of the announced election outcome everywhere that paper ballots are used. The nature of the underlying statistics makes these audits quite cheap, except when the margin is very small.

24. When a statistical audit is not possible (say for reasons having to do with election law), then a full recount of the paper ballots can provide the desired assurances.

25. Voting machines are computers, and subject to the same security issues facing any computer system (and more, since privacy of the ballot must also be enforced).

26. We have learned the hard way that almost any computer system can be broken into by a sufficiently determined, skillful, and persistent adversary. There is nothing special about voting systems that magically provides protection against attack.

    The computer systems of voting systems vendors and of election officials must be included in any list of potentially vulnerable systems.

    An attacker may be able to place malware in the source code of a voting system before it is compiled and delivered to an election jurisdiction. (This may be for the firmware of the voting system, or for other election-specific software.) Current voting system certification procedures are not adequate to detect sophisticated injection of malware into a voting system. It is not possible, even in principle, to have a certification procedure that can detect whether a voting system will ever produce an erroneous result (this is due to a powerful result known as Rice's Theorem). The voting system software *when delivered* may contain malware capable of affecting the announced election outcome.

This malware may be set to be triggered when a particular event occurs—perhaps something based on the date, the jurisdiction, or the pattern of choices made in an early-cast "trigger" vote. The malware may lay dormant during so-called "logic and accuracy" testing, only to be activated during the actual election.

While such an attack may naively seem unlikely or implausible, it is not the sort of attack that is beyond the resources of a powerful nation-state, and may be likely or plausible today depending on political circumstances. The "Stuxnet" attack on Iranian nuclear facilities demonstrated that even computers that are not connected to the internet may be successfully attacked.

27. Voting system software may be maliciously designed, may contain bugs, or may be changed or replaced at some point during the pre-election roll-out of equipment.

28. It is important to realize that *it is not feasible to verify the correct operation of voting system software, even given the source code.*

    Certification source code review and pre-election logic and accuracy testing are useful but weak tools for uncovering errors and bugs. These tools provide no proofs of correct operation, particularly when the errors or bugs may be maliciously devised to avoid detection.

    Perhaps someday this situation will improve here. But current voting systems are only partially tested, and in general unverified, for correct operation.

29. Even if we had correctly operating software, the following fact gives one pause. It is important to realize that *current voting systems are not designed to allow election officials to verify that the software running on their voting systems is indeed the software that is supposed to be running on those voting systems.*

    While I was serving on the TGDC, we contemplated rules that would have required voting systems to allow such checks, but abandoned the effort due to their cost and complexity.

    There is no way with current scanners and voting systems to easily "read out" the loaded software and confirm that it is the intended software. (And a corrupt system may even lie about what software has been loaded.)

30. One is thus forced to the conclusion that *one can not really trust voting system software very far.* One is reminded of the Reagan maxim, "*Trust but verify.*"

    In order to verify that an election outcome is correct, one is forced to abandon putting any trust in the voting system itself, and instead work directly with the "primary inputs" to the election: the cast paper ballots.

31. It is important to note that when the election is close (as WI appears to be), changing just a few votes in every precinct may suffice to swing the election. An attack need not make dramatic changes—it may suffice for the attacker's purpose just to "put one's thumb on the scale a bit".

32. Beyond the general principles enunciated above, there are aspects of the current 2016 U.S. Presidential election that seem sufficient to cause concern, and thus to increase the motivation to double-check that the voting systems have operated correctly.

33. I should emphasize that I have no particular evidence of manipulation or tampering of the ballots or the results of the 2016 U.S. Presidential election. While pre-election polls and post-election polls may seem to some to be particularly suspicious to count as sufficient evidence, for me the best and only real evidence would derive from the examination of the paper ballots via a post-election statistical audit or recount.

34. The extent to which Russian hackers have allegedly attempted to access U.S. election-related systems gives one reason for being especially careful. In the past, vendors and election officials may have felt comfortable that their systems were secure against the "script kiddies" that vandalized insecure computer systems. (A "script kiddie" is a inexperienced hacker who knows only how use attack scripts he has found on the internet.) Being secure today against a sophisticated nation-state is an entirely different matter.

35. A statistical post-election audit (or, if that is impossible, a recount) of the paper ballots provides really the only effective way to determine whether an announced election outcome is correct.

36. It is important to emphasize that an audit or a recount really *must* look at the paper ballots. Otherwise one is not examining the primary election data (the cast ballots themselves) but only derivative secondary data that may have been corrupted by faulty or malicious software.

37. A hand-count of paper ballots, as part of a recount of statistical audit, is the only way to ensure that faulty software has not corrupted the announced election outcome.

38. Re-running the same software on the cast ballots does nothing to help confirm the announced election outcome. One would expect a faulty system running on the same inputs to produce the same faulty outcome.

39. There may be other valid motivations for performing a recount or statistical audit of the paper ballots, such as providing a deterrent to adversaries in the future. For the present purposes, however, one should focus on checking that the announced outcome for the current election is correct.

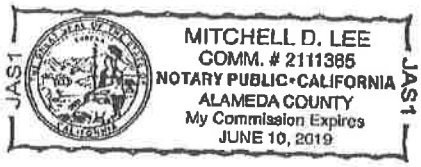
This affidavit was executed on the 28th day of November, 2016 in

Berkeley, California

Ronald L. Rivest

RONALD L. RIVEST

Sworn to before me this 28th day of November, 2016.



Notary Public

My Commission Expires: Jun 10 2019