

Reprinted From
The New York Times

TUESDAY, MARCH 2, 2004

Did Your Vote Count? New Coded Ballots May Prove It Did

By SARA ROBINSON

More than two centuries of elections in the United States have resulted in paper-based voting systems secured by a multitude of checks and procedures. New electronic voting systems require voters to trust computers and the people who program them, a trust that computer security experts say is unwarranted.

The subject is not hypothetical. Millions of voters will cast ballots on electronic machines today in the biggest test so far of the technology. To address security concerns, researchers are proposing new ways of voting that do not require voter trust in people or software.

"A trustworthy system of elections must rest on one central principle: trust no one," said Dr. Douglas W. Jones, a professor of computer science at the University of Iowa and a member of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems.

Devising such a system is challenging because it would have to satisfy opposing demands. Ideally, each voter should be able to verify that his vote was counted. But also, to ensure that voters could not show others how they voted, there could not be receipts or records of individual voters' actions.

"You have to think of the voter as a potential adversary who might want to sell his vote or be susceptible to coercion," said Dr. Ronald L. Rivest, a professor of computer science at the Massachusetts Institute of Technology.

While traditional paper ballot systems achieve secrecy, each voter has to trust election officials to include his ballot in the final tally. The process is secured by the opposing interests of the major political parties, which work together to monitor every step of the process.

Though this system works reasonably

A New Way to Vote

Cryptographic voting systems devised by Dr. David Chaum and Dr. C. Andrew Neff enable each voter to check to see that his vote was counted.

THE VOTER

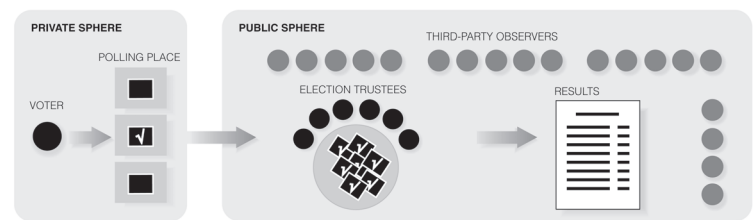
- 1 Votes at a computer terminal.
- 2 Gets a numbered receipt that's encrypted so she cannot use it to prove to a third party how she voted.
- 3 Later, can check that her vote was included in a virtual version of a ballot box on the Internet.
- 4 After the ballots are decrypted, she can see all of them and check the vote count for herself.

Mathematically sophisticated voters can also verify that no votes were lost or altered during the decryption process.

THE POLLING PLACE Must do all the things polling places do now, such as checking that people are registered to vote and ensuring that people vote only once.

ELECTION TRUSTEES Responsible for ensuring ballot secrecy. They decrypt and count votes in a public forum where their actions can be monitored. Trustees work together to decrypt the ballots, remove the serial numbers and shuffle them so the final ballots cannot be traced to individual voters.

INTERESTED OBSERVERS Can verify that the encrypted receipts correctly represent voters' choices. Observers with advanced math skills, along with the voters, can also check the proof that no votes were gained, lost or altered in the ballot decryption process.



The New York Times

well, paper ballots have other problems, experts and voting officials say. People often mark them incorrectly, invalidating their vote, and the ballots are expensive to print and securely store.

New technologies have not inspired total confidence.

Electronic machines are also favored by voters with certain disabilities, because audio functions and other special features allow them to vote unassisted. The problem with current all-electronic systems is that they can be compromised undetectably, and there is no reason to trust that they will correctly count votes, experts say. "It's not a matter of finding better programming languages or writing better software," Dr. C. Andrew Neff, a mathematician and the chief scientist of VoteHere, a company in Bellevue, Wash., said of electronic voting. "Computer systems are inherently insecure."

Thus, the only safe way to vote electronically, computer scientists say, is to use methods that do not require trust in complex software.

One such solution, soon to be mandated

in several states, is a voter-verified paper trail.

Dr. Rebecca Mercuri, a research fellow at the John F. Kennedy School of Government at Harvard, proposed a method that would require voting machines to produce paper printouts of the filled-in ballots, which would be checked by voters before being deposited in the ballot boxes. Only the paper ballots would be counted, bypassing the need to trust the voting machine.

An alternative is the "frog" voting system, proposed in a working paper released by the Caltech/M.I.T. Voting Technology Project in 2001. An all-electronic version of this approach — described by Dr. Rivest, Dr. Shuki Bruck of the California Institute of Technology and Dr. David Jefferson of Lawrence Livermore National Laboratory — would use two different types of electronic voting machines and a simple memory card, the frog.

Before the election, each voter would get a frog filled with all the candidates and other ballot options. Using the first type of electronic machine, which could be at an office or local supermarket, the voter would make his choices, and they would be stored on the frog.

The day of the election, the voter would go to his precinct and take the second step: inserting the frog into a secured "vote

caster” machine. That machine would read the frog and display the voter’s choices on the screen. If he was satisfied, the voter would push a button and cast his vote. The frog would then be “frozen,” so that its data could no longer be altered, and deposited in a ballot box as a backup record.

The first type of voting machine could have audio functions and other features requiring elaborate software. Because its output would be checked by the vote caster, it would not need to be secure. The vote caster would require heavy security, but such a machine could be made so simple, the researchers say, that securing it would be feasible.

With frogs, as with a voter-verified paper trail, voters would still have to trust people to secure the counting process. Mathematical voting systems — developed independently by Dr. Neff and Dr. David Chaum, an independent cryptographer and privacy expert — would ensure that votes were correctly counted, even in the presence of untrustworthy machines and officials.

These systems, based on two decades of cryptography research, would simultaneously satisfy the opposing demands

for ballot secrecy and voter records.

Though the two systems differ in several technical respects, they would have similar overall structures. In each system, the counting process would be performed publicly on the Internet. The voters themselves and third party observers would ensure election integrity, and a group of election officials, called trustees, would protect ballot secrecy.

After voting, each voter would receive a receipt — a record of his choices that would be encrypted, or put into code, and could be deciphered only by a collaboration of all the election trustees. After polls closed, all receipts would be posted on the Internet. Each voter could use his serial number to find the image of his receipt, and make sure it matched the one he carried.

Each trustee would perform one step toward decoding the receipts, and the decrypted ballots would also be posted on the Internet, where anyone could count them, but without serial numbers so they could no longer be traced to individual voters. Still, voters and observers who understood the process could mathematically verify that no ballots were added, lost or altered.

Students at George Washington

University, under the direction of Dr. Poorvi Vora, Dr. Jonathan Stanton and Dr. Rahul Simha, all computer science professors, are working to program Dr. Chaum’s system for a trial student election. Dr. Neff’s company is on the verge of releasing a software version of his system.

Dr. Josh Benaloh, a cryptographer at Microsoft Research, said he was confident that the two systems would be workable and that the security and privacy claims by Dr. Neff and Dr. Chaum were mathematically verifiable.

But other researchers said that the cryptographic approaches would be unlikely to be accepted because they were too complex for most voters to understand.

“You have to trust the cryptographer,” said Dr. Jones of Iowa. “It may be that you could have a crypto-based voting technology that rests on something that could be understood by a high school senior. If that happens, I’ll say ‘huzzah!’ but I don’t think we’re there.”

Dr. Benaloh disagreed. “You don’t have to trust the cryptographer,” he said. “If you’re a conspiracy theorist, you can take the time to educate yourself and gain absolute trust in the system.”