

First Voter-Verifiable Election for a Public Office

Breakthrough open-source election system used in official election lets voters audit tally online

Takoma Park, Maryland, November 3, 2009 -- For the first time, a government election will allow voters to check that their private votes are correctly recorded and included in the final tally. Takoma Park, Maryland is running its bi-annual election for mayor and city council using a new system. After casting their optically-scanned ballot at the polling place this Tuesday, voters will be able to check "confirmation codes" for their votes on the city's website.

The codes are revealed, for each oval a voter fills on the ballot, by an invisible ink system akin to that used in children's puzzle books. Voters may, if they wish, note the codes and the ballot serial number while in the booth. Because the codes are separately randomized for each oval and for each ballot, nothing about who a voter has voted for is revealed by the codes on the website.

The cost of the system is significantly lower than that of current systems since it is fully open source, the scanning setup uses commercial off-the-shelf scanners, and all printing is done with office printers.

The Scantegrity technology to be used was developed by cryptographer David Chaum together with researchers from the University of Maryland Baltimore County, The George Washington University, MIT, the University of Ottawa and the University of Waterloo. The group has run a number of elections for universities and other organizations and also successfully demonstrated Scantegrity last April during a public mock election administered by Takoma Park's Board of Elections.

Student members of the project won first prize in the National Science Foundation sponsored University Student Voting Competition in 2007, and the Scantegrity system has evolved from there. A broader research community has grown around proposals for such "voter-verifiable" election systems. The number of academic conferences on the subject has seen an increase from one every two years during the early part of the decade to two every year for the last few years and the National Institute of Standards also held a related workshop in October.

Before the election, encrypted items of data were posted on the election website. Some will not be decrypted, but the individual keys needed to decrypt others will be posted after the close of polls. Which keys will be revealed depends not only on the results and confirmation codes, but also on impossible-to-predict statistics of a set of high-tech stocks. This lets anyone verify a full public audit ensuring that the official election results are consistent with the confirmation codes published on the website.

"Something I find particularly exciting about the technology," says David Chaum, "is that it is robust enough to be used anywhere in the world -- scanners at polling places can speed posting of results, but with centralized scanning polling places need only pens, ballots and ballot boxes."

"We learned a lot from working with the Board of Elections of Takoma Park, who generously shared with us the wisdom obtained from running real elections," says Prof. Poorvi L. Vora of The George Washington University, "it's one thing to develop a voting system, it's quite another to have one that can be used in a real election."

"This represents a significant step in the evolution of election systems," says Prof. Ronald L. Rivest of MIT, "and though we've worked hard within the constraints of this volunteer project, it is a first step for a whole range of promising new types of such systems."

#####