

# Report on DIMACS\* Workshop on Electronic Voting – Theory and Practice

Presented under the auspices of the  
Special Focus on Communication Security and Information Privacy and  
the Special Focus on Computation and the Socio-Economic Sciences.

Date of workshop: May 26 - 27, 2004

Workshop Organizers:

Markus Jakobsson<sup>†</sup>, RSA Laboratories  
Ari Juels, RSA Laboratories

Report Author:

Margaret McGaley,  
Computer Science Department, NUI Maynooth

Date of Report:

December 9, 2004

---

\*DIMACS was founded as a National Science Foundation Science and Technology Center. It is a joint project of Rutgers University, Princeton University, AT&T Labs-Research, Bell Labs, NEC Laboratories America, and Telcordia Technologies, with affiliated partners Avaya Labs, IBM Research, Microsoft Research, and HP Labs.

<sup>†</sup>Markus Jakobsson's current affiliation is Indiana University Bloomington.

## 1 Introduction

This workshop followed in the footsteps of the highly successful WOTE '01 (Workshop on Trustworthy Elections), organised by David Chaum and Ron Rivest in 2001 at the Marconi Conference Center in Tomales Bay, California <sup>1</sup>. There were 24 speakers and two panel discussions over the two days covering many aspects of electronic voting, from theoretical computer science to real-world implementations. At the end of the second day, David Chaum dubbed this workshop WOTE II.

One topic which arose repeatedly was David Chaum's voter-verifiable voting scheme. In this scheme, the voting machine prints a two-layer copy of the ballot. When the two layers are combined, they show the human readable vote, but the individual layers only bear an encrypted copy. The voter chooses one of the two layers to take home, and destroys the other. The voter can later check that the layer they retain has been counted by going to a public Internet bulletin board. Thus, they know that their vote has been recorded and counted correctly, but cannot prove the fact to anyone else (this protects the system against voter coercion and vote selling). For a more detailed explanation, see *David Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. In IEEE Security & Privacy (Vol. 2, No. 1), pages 38-47, January-February 2004.*

## 2 Workshop Presentations

### 2.1 Some Thoughts on Electronic Voting

Speaker: Ron L. Rivest, MIT Computer Science and Artificial Intelligence Laboratory (CSAIL)

Professor Rivest divided his talk into two sections: 12 "debatable propositions" and a "pedagogical variant" of David Chaum's voting scheme.

He began by pointing out some of the often ignored aspects of the electronic voting debate. He believes that the weakest link in voting systems is probably voter registration, rather than vote collection, which receives all the attention. He highlighted the fact that the voter is not a computer. All too often, computer science papers begin with the phrase "let the voter compute ...". He also called attention to the fact that election management is being outsourced to vendors of electronic voting (e-voting) systems. He said that e-voting is, in effect, proxy voting (voting through a machine).

---

<sup>1</sup><http://www.vote.caltech.edu/wote01/>

Professor Rivest proceeded to describe 12 debatable propositions, arbitrarily phrased so as not to imply support for one or the other side of each argument. These topics included; voter privacy, voting fraud, and the question of making voting software “open source.” Defenders of e-voting systems often note the trust people have in the software running aeroplanes. Professor Rivest responded to this by noting that e-voting software is not developed to the same standard as avionic software.

Support for the use of the open-source model in voting systems is high amongst members of the technology sector. Professor Rivest asked if this model would be as trouble free as is often assumed. What would happen, he asked, if a bug was discovered or announced the day before an election?

He went on to describe a pedagogical variant of Chaum’s voting scheme. He said that this variant is a plausibility argument, originally used to explain the basics of the scheme to a graduate class.

Professor Rivest concluded his talk by challenging academics to fully explore the design space for e-voting. He believes that it would be very worthwhile to explore other voting system designs and architectures; and said that he hopes that we will continue to see new ideas presented as to how one should build voting systems. We have only seen a small number of possibilities explored, both commercially and academically, compared to the full range of possibilities.

In the discussion that followed, the question was raised whether paper was necessary in e-voting for verification. Professor Rivest’s response was that we must force the machine to make a commitment to what vote it is recording and the voter needs tangible evidence that their vote is recorded correctly.

Another member of the audience stated that she believed it is possible to do parallel testing of the system on election day, and that the staff are often available on that day to do this kind of work. Parallel testing in this instance would consist of choosing a random sub-set of the voting machines, and rather than using them in actual polling, carefully scrutinising their behaviour. The idea is to reduce the risk of some malicious set of behaviour being triggered only on election day. Professor Rivest responded that parallel testing almost never happens in the real world. It requires that machines be pulled out on the day of the election, and is a very expensive process.

In light of the difficulty being faced by those promoting voter verified paper ballots, it was asked if it would be possible to convince election officials of the need for cryptographic solutions, such as David Chaum’s scheme. Professor Rivest said that we still need to fully explore the design space – that is, all possible solutions – and new ideas must be allowed to compete. He said that issues of understandability are important, but that these cryptographic solutions are in their early stages.

## 2.2 Evoting in an Untrustworthy World

Speaker: Rebecca Mercuri, John F. Kennedy School of Government, Harvard University

Dr. Mercuri began by explaining that she has extensive real-world election experience, having worked at all levels of election administration. She discussed Michael Shamos' six commandments,

- I Thou shalt keep each voter's choices an inviolable secret.
- II Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote.
- III Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.
- IV Thou shalt report all votes accurately.
- V Thy voting system shall remain operable throughout each election.
- VI Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I.

She noted that they are informally developed heuristics. For instance, secrecy is not always inviolable, 100% accuracy is not the accepted norm.

The Common Criteria for Information Technology Security Evaluation<sup>2</sup> fail to address possible conflicts between the requirements they cover. In e-voting, there is a fundamental conflict between voter privacy and auditability. The Common Criteria offer no help in resolving this conflict, and balancing the two requirements.

Dr. Mercuri noted the use of the word "glitch" in media reports of problems with e-voting machines. The implication is that the problems are minor, when in fact they could be affecting the outcome of elections. She also explained that ballots printed from electronic records, after the close of polls, are not equivalent to ballots printed for the voter to verify. She called such ballots – printed post-election – "hearsay," in the legal sense of the word.

Following the presentation, an audience member asked if the battle for verified voting had already been lost. Dr. Mercuri responded emphatically that this is a democracy. She said that technical problems must be solved in their political, social and commercial context, and integrated solutions are needed.

---

<sup>2</sup><http://csrc.nist.gov/cc/>

### **2.3 Secret-Ballot Receipts; True Voter-Verifiable Elections**

Speaker: David Chaum, SureVote

David Chaum began by saying that the workshop had already been stimulating. He compared it to the workshop WOTE '01, which he said produced the ideas that led to the creation of his voting scheme. At the time, he did not believe that the election world would be interested in his scheme, but recently he has become more interested in making it into a practical reality.

In common with many of the speakers at the workshop, he called for improvements in election administration, highlighting it as an important vulnerability. Dr. Chaum made an historical note that this is not a new area; he wanted to credit the work of Mae Churchill, David Burnham, Ronnie Doggers, Rebecca Mercuri and Peter Neuman.

Receipts that show for whom the vote was cast violate the principle of ballot secrecy. He believes, however, that there is a fruitful and interesting area in schemes that provide voters with a receipt that is only readable within the polling booth.

Dr. Chaum came up with an idea for illustrating his secret-ballot receipts one evening while confined to bed by a severe tooth-ache. The illustration shows how a receipt could exist which proved to the voter that their vote was recorded and counted correctly, but would not prove the contents of that vote to anyone else. This concept is central to his voter-verifiable voting scheme. The illustration is based on the Japanese game “janken,” also known as “paper, scissors, stone.” Dr. Chaum’s slides, available at

<http://dimacs.rutgers.edu/Workshops/Voting/slides/slides.html>, contain an explanation of the scheme.

He believes the problem of e-voting can be broken down into secrecy and unconditional integrity, but that secrecy must take a back seat to integrity. Any scheme is only useful if it can be explained to a high-school class. He suggested that we now have a public policy question: how can we repair public confidence in elections? He submitted that we must offer systems that fundamentally solve the problems. We also need clear standards, and rankings for measurable functional attributes.

### **2.4 Theory vs. Practice in Electronic Voting**

Speaker: Michael Shamos, Carnegie Mellon University

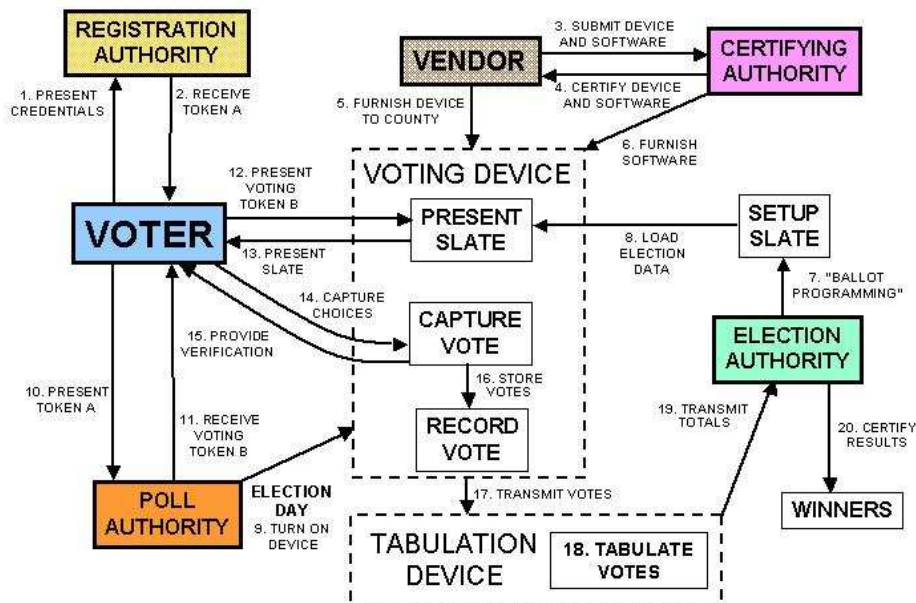
Dr. Shamos began by expressing his concern about the disconnect between researchers and election officials. He believes considerably more communication

is necessary between the two groups. In response to David Chaum's claim that systems must be understandable to a high-school class, Dr. Shamos joked that he would state it more strongly than that: it must be possible to explain it to a state legislature.

He then provided an overview of how voting is administered in the United States including the historical, procedural and legal framework in which e-voting researchers need to know they are working. When discussing the recent California election, which had 135 candidates, he joked that there might be a role for Google in voting.

Dr. Shamos believes that any voting scheme which relies on poll workers working correctly is doomed to failure. This is why he prefers schemes like David Chaum's: what happens to the vote between casting and counting is irrelevant. He expressed dislike of optical-scan voting systems, saying many of them rely on infra-red light – which is prone to both cheating and error – and that he could provide a catalogue of ways of tampering with optical-scan voting systems. He said that smart cards as voting tokens are “one of the worst.”

## The Voting Process



The above diagram from his presentation shows the voting process. He said we could have spent the rest of the workshop just discussing vulnerabilities of one of the arrows in this diagram.

Dr. Shamos went on to describe some of his experiences in dealing with vendors. He believes that, contrary to the claims of vendors, the only trade secret in their software is the number of bugs. He says that every system seems to have a “change anything you want” card. These cards are often introduced for testing and election setup purposes. When vendors are asked to remove this capability from the system they have been known to simply remove it from the documentation.

Dr. Shamos recommended that researchers be very careful in the language they use, reminding us that not only the technology, but also the language describing it, must be understood by the state legislature. He advised against the use of words such as “homomorphic” as they might be misunderstood.

He believes that the biggest open problem is absentee voting. Many voters are disenfranchised in every election because they are unable to get to the polling station to cast their vote. He also mentioned that anyone interested in protocols would find lots to be worked out in each step of the voting process.

## **2.5 European Online Voting Experiences**

Speaker: Andreu Riera i Jorba, Universitat Autònoma de Barcelona, Spain

Dr. Riera began by saying that complexity is not the best ally for security. He described Scytl’s Internet voting system Pnyx – pointing out that it is intended to be an alternative to postal voting. He went on to give an overview of three experiments in Europe. The first was an Internet voting system used in the Swiss Canton of Neuchâtel, the second was Internet voting for the 2003 Elections to the Parliament of Catalonia, and the third was Madrid Participa – an e-participation project.

## **2.6 Providing Trusted Paths Using Untrusted Components**

Speaker: Andre Dos Santos, Georgia Institute of Technology

Andre dos Santos put forward an idea that it might be possible to use hard Artificial Intelligence problems to reduce the need for trust in voting machines. He suggested that encoding the vote in a format which was human-readable, but not machine readable, could provide a way to limit the power of the voting machine so that it could not maliciously alter votes.

## **2.7 Trustworthy Elections without Paper Ballots**

Speaker: Andy Neff, VoteHere, Inc.

Dr. Neff began by saying that the science of e-voting exists, but that it is hidden away in the academic literature. He believes that communicating this science to those who influence policy is at least as hard as the science itself.

He said that detecting and correcting errors is the real goal. While it is painful to look at election problems, by examining where things have gone wrong in the past we can improve election systems and the discussion will have been to our ultimate benefit.

Dr. Neff was very concerned by the trend towards legislation calling specifically for a paper trail. Legislation should not rely on a single solution, it should rather lay down suitable requirements.

## **2.8 E-voting with Vector Ballots : Homomorphic Encryption with Write-ins and Shrink-and-Mix Networks**

Speaker: Aggelos Kiayias, University of Connecticut

Aggelos Kiayias described a way to combine mix-nets – which make practically no assumption about the nature of the ballot, but are relatively slow – with homomorphic encryption – for which ballots must have a specific structure, but which is fast. This combination would allow voters to make their choice of the listed candidates or write-in their preferred candidate. Since write-ins rarely materially effect the outcome of an election, it would even be possible to release tentative results while the calculation of write-in ballots was still being performed.

After the presentation, Dr. Kiayias was asked if this scheme would allow the authorities to know who had cast a write-in vote. He responded that yes, there would be some privacy loss in that respect.

## **2.9 How Hard is it to Manipulate Voting?**

Speakers: Edith Elkind, Princeton University  
and Helger Lipmaa, Helsinki University of Technology

Edith Elkind presented her work with Helger Lipmaa on the problem of dishonest voters. In many systems, it is possible for voters to vote dishonestly – i.e. not according to their genuine preferences – and thereby gain extra influence from their vote. As a result, the election results would not reflect the true distribution

of preferences in the society. In fact, according to a 1971 theorem by Gibbard-Satterthwaite, every non-dictatorial aggregation rule with three or more candidates is manipulable.

We cannot make this manipulation impossible, but we can make it harder. One way to do this is to add a preround, where candidates are paired-off against one-another, and the winner passes through to the next round. It is important that the pairings (or “preround schedule”) are fairly chosen. The innovation proposed by Ms. Elkind and Professor Lipmaa is that the votes themselves should be used to choose pairings for the preround. Central to the fair choice of preround schedule is a one-way function using the vote data as input. There is no need for a trusted source of randomness, since calculating the votes necessary for a particular schedule requires the inverting of the one-way function.

There are some open problems with this approach, listed by Ms. Elkind in her final slide:

- Average-case hardness seems hard to achieve using a preround. Are there other approaches?
- What is the maximum fraction of manipulators we can tolerate?
- We can prove the security of the voting system against 1/6 of all voters colluding to manipulate the results. Is this optimal?
- These results are for specific protocols. Can more general proofs be developed?

## **2.10 Towards a Dependability Case for the Chaum E-voting Scheme**

Speaker: Peter Ryan, University of Newcastle, U.K

Peter Ryan is concerned by the popularity of what he called “thank you for your vote, have a nice day” style voting systems. He is a member of the security strand of the DIRC (Dependability Interdisciplinary Research Collaboration) project. E-voting was chosen by DIRC as a good example of a system which has both secrecy and integrity requirements.

Professor Ryan believes that more attention must be given to the socio-economic issues surrounding e-voting, particularly voter trust and understanding. He pointed out that bulletin-board schemes such as David Chaum’s require that voters have web access, something which is not equally spread among people from different socio-economic backgrounds.

It is necessary to do a formal analysis of the system, and to construct a full risk analysis. But the system must also be put in its real-world context. What legal and procedural rules are necessary to make the system actually function? There is a difficult balance to be found between, on the one hand, aborting elections too

easily and therefore making them very impractical and, on the other hand, allowing the possibility of significant, undetected corruption. There are many unsolved problems with the design of a real-world implementation of Dr. Chaum's scheme.

Future work identified by Professor Ryan includes:

- Do a formal analysis of the scheme (and variants),
- Construct a full risk analysis/dependability case,
- Elucidate the goals and requirements; technical, social, political, legal, economic,
- Investigate social threats to the scheme,
- Do a sociological study of collusion,
- Determine to what extent fairness and absence of bias is achieved,
- Investigate to what extent public trust could be established, maintained, undermined,
- Construct mental models,
- Organise trials.

## **2.11 The Exact Multiplicative Complexity of Counting Votes**

Speaker: Rene Peralta, Yale

Rene Peralta described a bulletin-board based voting scheme where the only information released is the final outcome. Voters cast their votes on unforgeable and untraceable ballots released by a trusted registration authority. These ballots are encrypted, and then posted onto a public bulletin board. The result is calculated by a circuit which has the encrypted votes as its input.

Professor Peralta went on to calculate the multiplicative complexity of this circuit. He explained that he was surprised to find an exact complexity, because he had begun by searching for the bounds on the complexity.

## **2.12 Panel Discussion – Paper Trails**

A panel discussion of the issue of paper trails included contributions from the following speakers: Rene Peralta, Rebecca Mercuri, Josh Benaloh, David Chaum, Barbara Simons, Andy Neff, Doug Jones, Dan Wallach, Ron Rivest and Tom Jacob.

Peralta began the discussion by saying that the requirement for auditability has morphed into a requirement for paper trails. He said that laws mandating the inclusion of paper trails are a recipe for disaster.

Mercuri pointed out that she did not come up with the Mercuri method because she is overly fond of paper, or because she wanted a dual system, but because she was concerned about the unauditable nature of the system that was being introduced in her electoral area at the time.

Benaloh is concerned about the tendency to equate paper with verifiability. It is possible, he said, to lose verifiability when you have paper and to have verifiability without paper. It is necessary to have some artifact, but not necessarily paper.

Chaum asked how you could have commitment from the machine without paper.

Benaloh responded that some artifact which was both human and machine readable would be best. But he reiterated that we must avoid the emphasis on paper. He also voiced concern about the legislation being introduced which specifically mandates paper.

Neff said that it may be useful to distinguish between physical tokens as official records and ballots.

Simons said that this is a question of language. She said that “paper or paper equivalent” was probably a better phrase than “human readable artifact.” She also distinguished between the words “receipt” and “ballot.” She said this is a technical problem which has become seriously politicised. The motivation behind the actions of agitators, she said, is not that they want paper, but that they do not want DRE (Direct Recording Electronic) voting machines. There is a lot of money at stake, and hence there are vested interests, which causes difficulties for campaigners. She asked whether optical-scan systems might be the best solution, since adding printers to DREs is horrible. She noted that election officials do not want recounts, and that as technical people in a political arena we must be careful what we say.

Chaum responded that optical-scan machines see infra-red, which can cause many problems. He also pointed out that the time delay between a call for recount and the recount itself may provide an opportunity for tampering with ballots.

Jones said he was worried by a rhetorical technique often seen today. People say “here is the way we do it, and it is horrible. The alternative – if carried out correctly – would be great.” The alternative must not be any more idealised than the reality it is replacing.

Wallach said that he felt the need to take an extreme position. He made a “modest proposal”: that DREs should simply be banned and we should use precinct based optical-scan systems. He said they are dirt-cheap, that they catch undervotes and overvotes and they are transparent.

Chaum said that he takes issue with the idea that optical-scan systems report undervotes. Optical-scan systems as advanced as that would effectively be DREs.

Jones pointed out that optical-scan machines are now based on visible light, rather than the infra-red light used by older systems. He said that all the economic

studies that exist seem to have been done by vendors. He believes that an academic needs to do a serious study of the economics of various systems.

Mercuri said that all counties that have DREs have optical-scan machines for counting absentee ballots, but Chaum responded that those machines were used for centralised scanning, not precinct scanning.

Mercuri asked if the cryptography community could put a digital signature or something on the ballots. Chaum did not think this was a good idea. He said that yet another copy of the same vote would create more opportunity for inconsistency.

Jacob, an election official in Dallas, confirmed that optical-scan systems only kick back overvotes. He noted the difference between theory and practice. Frequently during an election he will be asked by voters why their vote was kicked back by the machine. It seems that voters care less about privacy than we do.

Simons asked whether separate vote-marking and scanning machines might be the best solution. She gave the example of the Vogue machine, which she said is HAVA (Help America Vote Act) compatible.

Chaum compared this system to a system called incavote, developed by Caltech/MIT. He said that this is not a panacea.

Benaloh said that proactive verification is better than passive. He asked: if the system is verifiable, rather than verified, how many voters would spot the difference?

Jacob compared two systems, one of which asked voters to review their vote before casting. He said that undervotes were significantly lower when the voter was asked to review their vote.

## **2.13 The Politics of Good Voting Systems**

Speaker: Rob Richie, Center for Voting and Democracy

Mr. Richie said it was great to see such good discussion on this topic. He began by talking about voting rights. While the Voting Rights Act had recently improved race rights, there is still no constitutional right to vote in the United States. Current voting systems are bad, but the old systems they replaced were also bad; all too often, according to Mr. Richie, new ideas are used without adequate examination. He believes sincere people should be on the same side. In the early years of the United States, not many adults could vote. Some states had wider suffrage than others. The United States constitution still does not have an affirmative right to vote. In fact, the money released under HAVA is the first United States Federal money ever to be spent on voting.

Mr. Richie believes that we do democracy on the cheap. If we built our roads in the same way we do our democracy, he said, the speed limit would change

every 10 miles. The United States' decentralisation of authority over electoral systems causes many problems. One result is that the best voting machines do not necessarily rise to the top.

He discussed instant-runoff voting, which prevents very unpopular parties from getting into power, but does accommodate minority parties. David Chaum asked at this point whether it was true that in one area, a law had been passed to use instant-runoff, but that it had not been used. Mr. Richie replied that it was true. In that particular instance, election officials had to work with the vendor of the e-voting system in use there. The vendors claimed that there would be large delays partly because of the need for certification, despite the fact that the older system had not been certified. They dragged their heels, according to Mr. Richie. A law suit was brought, but the judge decided that it was not possible to force the vendors if they said they could not produce the system in time.

Mr. Richie mentioned Condorcet and Approval voting. He believes that instant-runoff voting would be a good system to use in the United States. He said that it has a history, and that voters would have an intuitive understanding of the idea that they rank candidates in order of preference. On the other hand, some aspects of the system are hard to explain, for instance the eventual winning candidate may only get 10% of the first preference votes. He said that Proportional Representation of one kind or another is the international norm. It gives good party representation. Winner-takes-all systems, on the other hand, discriminate by race and so on.

In the discussion that followed, Dr. Chaum asked if there is a connection between the voting system used in a country and the number of political parties there. Mr. Richie responded that yes, there is some connection, though there are other factors including gerrymandering and non-competitive races.

Dan Wallach said that he agreed with a lot of what Mr. Richie had said. He asked how we can make change happen. Mr. Richie said that typically reform groups set the bar low. People need to believe that changes will have an effect. We need to establish a vision between groups, and support incremental successes.

Dan Wallach asked if the existence of DRE systems helps the Center for Voting and Democracy to argue for the introduction of these changes. Mr. Richie said that that would have been his expectation, but that has not been the experience.

## **2.14 Rice University “Hack-a-Vote” Project**

Speaker: Dan Wallach, Rice University

Dan Wallach began by describing what he calls “faith-based voting.” He said it results from reliance on independent testing authorities.

He then described the “hack-a-vote” project, which was an assignment he gave

to a graduate class. The project was based on an idea of David Dill's, which he had after becoming frustrated with trying to explain to election officials that computers are not trustworthy. It was to be a piece of software that would demonstrate this fact, but Dr. Wallach felt it became unnecessary after the Diebold scandal.

He then decided to turn it into a "cool adversarial student project," which he said the students love. The class had to insert changes into the source to alter the result of an election or simply create a denial of service attack. They then had to find the code changes inserted by other groups. There was a rule against using the command *diff* (to automatically find differences between two versions of the source code) which the students honoured.

Dr. Wallach gave a live demonstration of how one small code-change could allow the voter to give a signal and then vote multiple times. This change was done by giving a variable the same name as the name of a class, so that the variable was used instead of a static *method* of that class.

After the presentation, Rebecca Mercuri said that she had run a project to create a voting system. She said that common errors included failure to clear the screen. Dan Wallach said that he is currently trying to figure out how to do the same project with a sophomore class. He said that it was much easier to do it with graduate students, who are trying to prove themselves.

## **2.15 Citizen Verified Voting: An Implementation of Chaum's Voter Verifiable Scheme**

Speaker: Poorvi Vora, George Washington University

Poorvi Vora presented an implementation of Chaum's voting system as described in Chaum's original paper. The authors are currently in the process of making the software open source.

She said that it is not necessary that voters check their own receipts against the bulletin board. They could hand over their receipts to some group that they trusted, for instance the League of Women Voters, and that group could check receipts they received. Although voter authentication was outside the scope of the project, she said that some voter registration/authentication protocols would be of interest.

There was then a demonstration of their prototype implementation of Chaum's scheme using commonly available hardware and operating system software.

## **2.16 Voting Technology in Brazil: an Assessment**

Speaker: Jeroen Van de Graaf, CENAPAD-MG/CO, Brazil

Jeroen Van de Graaf discussed a system which uses a modification of Chaum's scheme using overprinting instead of two transparent sheets. He believes that this will be a cheaper solution. He presented several possible encodings.

## **2.17 Electronic Voting Systems – Is Brazil Ahead of its Time?**

Speaker: Pedro Rezende (represented by Jeroen van de Graaf)

Dr. Van de Graaf discussed voting in Brazil on behalf of Pedro Rezende. He described the "urna" which is the name of the voting machines used in Brazil, and gave a short history of e-voting in Brazil. The Brazilian voting machines do provide a voter-verified paper audit trail. However, Dr. Van de Graaf was concerned that most voters would not verify their vote, and that it might be difficult to motivate people to do an audit recount of the printed ballots.

He believes that the system could be improved if the source code were simplified and statistical methods used to detect fraud. He issued a challenge to the computer science community to develop solutions that will also work in poor countries.

## **2.18 On Mark-Sense Scanning**

Speaker: Douglas Jones, University of Iowa

Knowing that much of the discussion at the workshop would centre around paper trails and auditability, Doug Jones made his presentation on transparencies, using an overhead projector. He discussed the Australian ballot – the standardised paper ballot that lists all candidates for office – calling it "a trivial technology, but a sophisticated system." The paper Australian ballot actually had a relatively short life in the United States, though it returned in the form of punch cards and mark sense ballots in the 1960s.

He showed a table with many of the threats posed to paper voting systems, and the defenses that were developed to deal with them. For example, to defend against ballot box stuffing, poll workers compare the number of voters marked on the poll-book with the number of ballots cast. To reduce the number of clerical errors, ballots are sorted before being counted (as bank tellers do with bank notes).

This was followed by a description of scanning technology. He made it clear that scanning technology has greatly improved; the problems noted by Dr. Shamos

are not present in modern systems. He went on to show that the definition of a vote is not consistent across the board. Whatever the legal description, it is effectively whatever the machine recognises, since machines are doing the counting. He then compared precinct count optical scan systems, which give individual voters a second chance to get their vote correct, with central count optical scan systems. Next, he dealt with human factors, such as poor ballot design.

Finally, he gave an overview of some problems that the iVotronic system has had in Miami. He described the temporary solution which will be used in the upcoming elections.

### **3 Internet Voting**

#### **3.1 SERVE Project**

Speaker: Barbara Simons

Barbara Simons gave an overview of the SERVE project, and the conclusions to which she, David Jefferson, Avi Rubin and David Wagner came in their report on the security of the system. SERVE is short for Secure Electronic Registration and Voting Experiment, and it was intended to provide a means of remote voting to some United States military personnel in the November 2004 United States presidential elections. It was cancelled in February 2004 for security reasons.

Dr. Simons began with a hypothetical situation set in 2008 in which a virus has successfully cast doubt on the results of a presidential election. She used this to illustrate some of the concerns raised in the SERVE report.

She believes that the push towards Internet voting comes, to some extent, from a belief that it will increase voter turnout. She reacted strongly to the accusation that those raising concerns are reducing voter confidence. She believes that Internet voting should not be introduced unless and until experiments have shown it to be secure. However she also believes that it is not possible to do a meaningful experiment, since there is no incentive for outside forces to try to influence an experimental election, but if it is a real election, then it is not an experiment.

In the discussion that followed, Dr. Simons was asked why the military did not use its own secure network in the SERVE project. She responded that the military cannot be in control of elections, but they do not want to hand over access to their secure network to election officials.

She was then asked if she felt that the response from the military to the SERVE report had been very quick. She said that perhaps some people there understood the concerns raised by the report. They may have been influenced by the fear of a debacle. They were already behind schedule on the project. However, she felt that

it was still astounding that within nine days of receiving the report, the project was no longer to be a part of the real elections. The report did get a lot of press, and was seen by Congress.

### **3.2 Tree Homomorphic Encryption with Scalable Decryption**

Speaker: Moti Yung, Columbia University

Moti Yung described his joint work with Aggelos Kiayias on tree homomorphic encryption with scalable decryption, and how that work could be applied to e-voting.

He described the basic homomorphic encryption model as having a bush structure. Such a model is not adequately scalable, however. Different factors such as the number of votes involved, and geography, make it unsuitable. The idea Dr. Yung presented was to spread the model over a tree structure. This ensures that the voter's privacy is not violated unless the whole user trust path is corrupt. It works for arbitrary election structure, size and distributions.

This model provides scalable decryption for elections. Multi-level decryption distributes trust among several parties.

### **3.3 A Voting System Based on Future Technologies – A Quantum Voting System**

Speaker: Tatsuaki Okamoto, NTT Labs, Japan

Tatsuaki Okamoto described a quantum voting system. Almost all cryptosystems are based on number theoretic systems. However, if and when a quantum computer is realised, all those cryptosystems will be broken.

Dr. Okamoto reminded us that quantum bitstrings cannot be copied, so quantum ballots cannot be copied. He then gave an overview of quantum cryptography, which assumed the existence of a quantum infrastructure. The voting system was constructed around a quantum bulletin board of q-ballots. It can offer correct anonymous ballots with overwhelming probability.

### **3.4 Lessons from Internet Voting During 2002 FIFA WorldCup Korea/Japan(TM)**

Speaker: Kwangjo Kim, Information and Communications University, Korea

Kwangjo Kim described the Internet voting project "VOTOPIA," which ran during the 2002 world cup in Japan/Korea. The system is based on Public Key In-

fracture. Dr. Kim provided diagrams outlining the system including registration, voting and counting and the setup of the servers. He provided some screen shots of the client-side of the system, and some statistics both of unsuccessful attacks on the system and of the results of the voting.

### **3.5 A Network Voting System Using a Mix-net in a Japanese Private Organization**

Speaker: Kazue Sako, NEC, Japan

Kazue Sako began by describing the current state of e-voting in Japan. She said that problems in trials have made the government less enthusiastic about the introduction of e-voting.

The system Dr. Sako described was intended for use by a private company, rather than public sector elections. The votes are cast over the network and anonymised by a verifiable mix-net. The system has been used for voting and anonymous surveys.

Technically, the scheme she described is not zero knowledge, since a distinguisher can distinguish between a real protocol and a simulated result for any input  $x$ . She submitted, however, that perhaps this calls for a new notion in security (she did not offer a name). Since a distinguisher who knows the input does not need to learn anything from the proof, perhaps the Zero Knowledge Interactive Proof definition is too strong. The new notion put forward is that the distinguisher does not learn anything from the protocol that he could not have learned in some other way. The scheme described satisfies this notion.

### **3.6 An Unconditionally Secure Electronic Voting Scheme**

Speaker: Akira Otsuka, Tokyo University, Japan

Akira Otsuka described a voting scheme which assumes an adversary with infinite computing power. It relies on a trusted initialiser upon whom the whole scheme depends. A suggested extension is to distribute the single trusted initialiser.

### **3.7 Some Issues in Election Verification**

Speaker: Josh Benaloh, Microsoft Research, United States

Josh Benaloh wrapped up the workshop before the final panel. He wanted to provide an unbiased summary of what had been said before.

He began by asking: what do we really want in a voting system? He listed the following requirements:

- Verification
- Robustness
- Privacy
- Non-coercibility

He reiterated his point from the previous day's panel, that paper is not the same thing as verifiability. Voter verified paper audit trails are limited, he said. Once you lose sight of your vote, you will not see it again. He asked if we can strive for end to end voter verifiability, or even universal verifiability.

He pointed out the importance of separating ballot creation from vote casting. He claimed that there is an unavoidable problem with any machine-assisted ballot creation. We cannot distinguish between a faulty machine and a lying voter. When a voter makes a claim that a machine is faulty, the election official will always be faced with this dilemma. This problem is mitigated where ballot creation and vote casting are separated.

He said that with a well-designed, cryptographically verifiable scheme, there will be no need for trust in people at all for integrity and verifiability. He believes that transparency is the most legitimate complaint against cryptography. He was not as concerned as some about public satisfaction with cryptographic schemes. He said that the public were happy with e-voting machines until experts kicked up a fuss, and he believes that if the experts were satisfied, the public would be satisfied.

Finally he identified the following challenges. We need to:

- agree on terminology: e.g. proofs of protocols and proofs of implementations are very different things,
- distinguish better between wholesale, retail fraud and privacy compromise,
- find better ways to deal with human factors problems,
- find conceptually simpler ways to tally - for the sake of transparency and public understanding.

## **4 Concluding Panel**

The concluding panel was organized by Sanford Morganstein, Populex Corporation. The other participants were Andy Neff, Barbara Simons, Rebecca Mercuri and Doug Jones.

Morganstein asked each panellist to answer two questions:

- 1) Why have we not solved the voting problems of Florida 2000?

2) Why are we focusing on vote counting and not on registration?

Mercuri began by saying that this workshop was an appropriate setting for these questions. She said that she had loved the dialogue and discussion at the workshop, and is proud of her contribution to the field. One reason the problems of 2000 are not solved is that it has been difficult to convince scientists that this is a difficult problem. She is heartened that we now agree that it is difficult. She reiterated the difference between theoretical proof and “proof” of implementation.

Simons said that e-voting is the perfect example of technology meeting public policy. With regards to why the problems of 2000 have not been fixed, she said that many people have not yet woken up to the issue. She told a story of a time she went to educate a public official about DREs. He had a large book of results of focus groups on his desk, but had never consulted with computer scientists. Officials do not know what questions to ask, and trust the vendors. One area that she feels is being ignored is the danger of centralised voter databases. HAVA requires a centralised database of voters. This was well-intentioned, but has serious security implications. Who has access to the system? How is it audited? What are the recovery procedures? What about the danger of ID theft? These things must be discussed. Here there is an advantage, in that these databases have not yet been implemented.

Jones said that he became involved in election administration in the same way Shamos did: he volunteered for a position and was the only volunteer. In response to the question of why things have not changed, he said things have changed, but not in what is delivered to the voter. He believes the bar has been raised. Election officials are asking difficult questions. They are realising that they must be skeptical. Vendors have not responded uniformly. One result of this rise in skepticism is that more difficult questions are being asked of new products. He said that the mathematics of cryptography is hard to communicate. Homomorphic encryption is really cool, but really difficult to explain. Some of his students thought it had no possible application. He very much liked the “rock, paper, scissors” analogy, given by David Chaum (see section 2.3), since it was so easy to communicate. He said he was glad to see skepticism rising, and pressure being put on vendors to improve the quality of their products and increase their openness.

Neff said that VoteHere Inc. has been working on the problem since 1998. His number one concern is the lack of progress at addressing Benaloh’s first challenge: agree on terminology and fundamentals. He sees two camps: one camp sees the possibility for technological transparency, the other is stuck in the certification of systems. This division is unfortunate. He said that we may have more to offer democracy than anyone else in our lifetimes. He believes that we will not be listened to if we cannot agree. He responded to Rebecca Mercuri’s concerns, saying that she must accept that some problems have been solved. He said that cryptog-

raphy, in and of itself, will not fix privacy, much as paper ballots will not. There are problems with privacy for which it is difficult to imagine solutions, for example camera phones. He believes that privacy may not be as important as integrity anyway. On the matter of registration: there is a marked contrast between the processes of voting and getting a passport. With cryptography, could we have strong authentication at the poll site?

Mercuri said that she does talk about a better ballot box. She carries plastic pieces to demonstrate Chaum's scheme around in her pocket. She does understand the mathematics, but wants to hold the bar very high. She believes that by serving as a skeptic, she helps us all to figure out how to convince others.

Neff believes that we have addressed 80% of the threats and 100% of the really bad threats. Mercuri disagreed.

Simons said that she had been thinking about educational programs all across the United States. While she did not have time to organise such a thing, anyone who was interested should contact her.

A member of the audience asked if the problem is the Balkanisation of the market, and if activists should focus on lobbying for more federal control. Mercuri responded that she and others had been trying.

Simons suggested that what should have been a technical issue has become politicised. Officials do not want to admit mistakes, and there are advocates with vested interests. The immediacy of the 2004 elections is blinding people to thinking beyond that.

Jones believes that 2004 may be the most honest in United States history; 2000 raised the bar. People are very skeptical, and there will be a lot more oversight.

Simons raised the possibility that the concerns raised by activists will be used to discourage certain communities from voting. Tom Jacob responded from the floor that we know for certain that Florida 2000 reduced turnout amongst some minorities in 2002.

Simons asked what tactics the community can develop to reduce the damage caused by DREs in the future.

A member of the audience asked where the panellists saw the potential for future research.

Mercuri said that the key topics are transparency, trust and security. She suggested that there may be applications for existing e-voting research in other fields. She asked how we can reduce the need for trust, and increase the transparency of voting systems. The CERT®Coordination Center exists for viruses, but there is nothing similar to anonymously report problems with voting machines.

Jones highlighted human factors questions. He said that this is a huge area. A good place to begin would be in simplifying the code base of existing systems; he asked why it is so immense. He believes this is a big problem, as it is easier to trust

smaller systems. We should seek end to end verifiability. He said that even if it is not possible to achieve, we could get a lot closer to that goal.

Neff believes that the focus of research should be less voting specific. We need a common language, and a formalism for expressing threats and countermeasures. He said that consistent terminology would be great.

A member of the audience asked if the new generation understand the dangers of e-voting better.

Simons said that her instinct is that those of us who know computers are more distrustful of them. This is in contrast to the position outlined by, for example, the League of Women Voters.

Mercuri recounted an incident in which she asked 11th grade students if they thought American Idol was fair, they said “no way,” they were sure it was all rigged. Even though people believe that American Idol is rigged, they still participate. She wonders if something of the same phenomenon is going on with voting.

The panellists were asked if we should offer incentives to vote.

Morganstein said that social scientists see this differently than computer scientists do. One professor has said that there is something about the process that connects us, and which is lost in e-voting.

Jones said that lever machines offer sheer physicality which generates trust, even if that trust is unjustified. Neff asked if lever machines were trusted from their introduction. Jones responded they were, in fact, seen as an end to corruption.

An audience member said that he believed some people need to realise that they cannot do cryptography. He said that we need communities of wise people to tell us what is good.

Jones disagreed, saying that cryptographers have a real obligation to explain and prove their work to people. There is a big difference between telling someone that they cannot do rocket science and telling them they cannot understand a rocket. He pointed out that many people do not realise that they do not understand cryptography.

Mercuri said that vendors have done terrible damage to themselves and others with fraud. There is a difference between fraud and stupidity. We must demand accountability.

Neff said that the solution will not be to make everyone understand, but to be unified in our understanding.

## **5 Open Problems and Research Challenges**

Several themes ran through the presentations, most of them to do with unsolved problems. It was generally agreed that there was much work to be done on the practical usability of David Chaum's voting scheme. Several people voiced concern about the disconnect between researchers and election officials. The only way solutions will be implemented in the real world is if communication between the two groups improves.

The area of voter registration was mentioned several times as an area generally neglected in electronic voting research. Professor Rivest went so far as to say that it is the weakest link in the voting process. A classic example of the failure of this link is the registration of dead voters in the 1960 United States Presidential election. Professor Rivest also said that there was considerable potential to more fully explore the design space, and that research to date had been narrowly focused.

Perhaps the most commonly raised issue was voter understanding. Cryptography tends to be somewhat impenetrable to the layman, but if the voter does not understand the security protocol, he cannot trust it. Andy Neff said that much of the necessary science is out there, but that it is hidden in the academic literature.

The development of a common language and formalism was raised as a necessary step towards a common understanding of the problems of e-voting, which could lead to a unified stance on several issues. Andy Neff believes that the computer science community will not be heard on this topic until we can agree amongst ourselves.

Finally, human factors such as usability have so far been somewhat neglected in e-voting research. It is vital that interfaces help voters to indicate their vote correctly and quickly. The special needs of some voters must be accommodated.

## **6 Acknowledgements**

The author and the DIMACS Center acknowledge the support of the National Science Foundation under grants number CCR 03-14161 and SES 03-51165 to Rutgers University.