Report from Dagstuhl Seminar 11281

Verifiable Elections and the Public

Edited by

R. Michael Alvarez[1], Josh Benaloh[2], Alon Rosen[3], and Peter Y. A. Ryan[4]

1 **Caltech – Pasadena, US,** rma@hss.caltech.edu
2 **Microsoft Research – Redmond, US,** benaloh@microsoft.com
3 **The Interdisciplinary Center – Herzliya, IL,** alon.rosen@idc.ac.il
4 **University of Luxembourg, LU,** peter.ryan@uni.lu

Abstract

This report documents the program of Dagstuhl Seminar 11281 "Verifiable Elections and the Public". This seminar brought together leading researchers from computer and social science, policymakers, and representatives of industry to present new research, develop new interdisciplinary approaches for studying election technologies, and to determine ways to bridge the gap between research and practice.

Seminar 10.–15. July, 2011 – www.dagstuhl.de/11281
1998 ACM Subject Classification K.6.5 Security and Protection
Keywords and phrases Electronic voting, Internet voting, voter verification, verifiable elections
Digital Object Identifier 10.4230/DagRep.1.7.36

1 Executive Summary

R. Michael Alvarez
Josh Benaloh
Alon Rosen
Peter Y. A. Ryan

This seminar brought together leading researchers from computer and social science, policymakers, and representatives from industry to discuss the issue of "Verifiable Elections and the Public". The purpose was to present new research, develop new interdisciplinary approaches for studying election technologies, and to determine ways to bridge the gap between research and practice. This seminar built upon the foundation provided by an earlier Dagstuhl seminar in 2007: Frontiers of Electronic Voting, Seminar number 07311, http://www.dagstuhl.de/07311.

The initial sessions of the seminar were devoted to a conceptual discussion of verifiable voting, and to a summary of the apparent obstacles associated with implementing innovations in election technology. There was a general sense from most seminar participants that while great progress has been made in development of verifiable voting systems, there has not been as much progress towards testing, implementing, and deploying these new voting systems. Additionally, the research community would like to be more involved in policymaking and the practice of election administration. In particular, a panel discussion regarding obstacles to innovation was quite productive, outlining several reasons for this feeling that insufficient progress has been made, including politics, a lack of interest on the part of voters, legal and

Verifiable Elections and the Public, *Dagstuhl Reports*, Vol. 1, Issue 7, pp. 36–52
Editors: Michael Alvarez, Josh Benaloh, Alon Rosen, and Peter Y. A. Ryan
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

regulatory confusion, a lack of sensitivity to the training and incentives of election officials, and a sense that some efforts to innovate have been overly ambitious and complex.

After a productive discussion of obstacles to innovation, seminar participants heard talks about a variety of recent evoting and Internet voting trials and projects. These included talks on developments in Australia, Brazil, India, Estonia, Switzerland, and Norway, as well as discussion of voting technology implementations in two U.S. counties: Cuyahoga, Ohio and Sarasota, Florida. These presentations provided a great deal of real-world information on technological and practical issues regarding the implementation of new voting systems throughout the world.

Substantial time was devoted to the presentation of new voting systems. Some of these presentations regarded innovative new conceptual and hardware schemes, including new protocols for elections and ideas like using smartphones as voting platforms. Other presentations focused on advancement and elaboration of existing voting systems, for example further development of voting systems like Helios, Wombat, Prêt à Voter, and Scantegrity. All of these presentations documented the significant progress that has been made in the scientific community, in terms of development and elaboration of important cryptographic and procedural protocols for voting, as well as new ideas for potential uses of technology in elections.

One of the most exciting new developments since the earlier 2007 Dagstuhl seminar has been the implementation and testing of some of the new voting systems that are under development. These include implementations of Helios and Wombat, and also a systematic usability and understandability project regarding Prêt à Voter. These efforts are providing important data that is aiding in the continued development of these and other related new voting systems.

Voting online continues to expand throughout the world, as was widely discussed during talks on projects in Estonia, Norway, and Switzerland. And many of the talks about new voting systems regarded new protocols that can be deployed online, like the extension of Scantegrity to remote online use ("Remotegrity"). Presentations about these projects came from social scientists, technologists, and policymakers.

At the same time, there continue to be important questions raised from researchers about voting online, focusing largely on concerns about the security of online voting – specifically including the challenges of making online voting coercion-resistant in a practical, convincing, and usable way. These concerns fueled much discussion during the seminar, and it is clear that more research about the voting systems being currently deployed, and those proposed for use in the near future, is needed.

Concern is growing in the research community about how to maximize the impact of the considerable body of research that has accumulated in recent years. Seminar participants raised concerns about ways to improve the science of studying election technology, as well as methods to improve connections and collaborations between the scientific and policymaking communities. These issues will continue to intensify in the near future, and we hope that the discussions at this Dagstuhl seminar will fuel progress in the development of new scientific opportunities for research and dissemination, as well as closer collaboration between scientists and policymakers.

2 Table of Contents

Executive Summary

Overview of Talks

Panel Discussions

3 Overview of Talks

3.1 Update on U.S. Internet Voting Demo Project, Information on UOCAVA Solutions Summit

David Beirne (Federal Voting Assistance Program, Arlington, US)

URL http://www.dagstuhl.de/mat/Files/11/11281/11281.BeirneDavid1.Slides.pdf

Pursuant to the Military and Overseas Voter Empowerment Act, the United States Department of Defense through its Federal Voting Assistance Program is charged with the conduct of an internet voting demonstration project for a statistically significant population.

3.2 VeriScan

Josh Benaloh (Microsoft Research – Redmond, US)

Verified Optical Scan (or VeriScan) is a voter front end that can be used to build a fully (end-to-end) verifiable election system. It allows voters to use ordinary optical scan ballots and slightly enhanced precinct optical scanners to create a verifiable tally which augments rather than replaces the traditional optical scan tally. The design is simple and familiar to voters and ensures that any discrepancy between the two tallies immediately implicates the optical scanner as malfunctioning. The benefits of full verifiability are obtained with minimal privacy risks – even in the event of complete cryptographic failure.

3.3 Revisiting individual verifiability

Sergiu Bursuc (University of Birmingham, GB)

Joint work of Bursuc, Sergiu; Grewal, Gurchetan S.; Ryan, Mark D.;
Main reference Sergiu Bursuc, Gurchetan Grewal, Mark Ryan, “Trivitas: Voters directly verifying votes,” Proceedings of the VOTE-ID conference, 2011, Springer LNCS, to appear.

Individual verifiability has emerged over the last few years as a fundamental property necessary for the public take-up of E-voting systems. Roughly, it should convince each voter that his vote has been correctly handled by the voting system: by the voting machine, by the communication network, by the bulletin board, by the talliers and by any other party involved in the election. In the end, the voter should be convinced that his vote has been counted in the final tally.

However, individual verifiability in most current E-voting systems is either incomplete (it is not end-to-end: it does not cover all the path traversed by the vote) or is indirect (it relies on trusted third parties, on complex math and/or on dedicated software). It is true that these limitations are due to a tension between individual verifiability and coercion-resistance, but is it really the case that we can not to better?

We propose the notion of audit ballots, that allow the voter to track the handling of an audit vote from the voting phase and up to the counting phase, thus providing more intuitive individual verifiability. Because an audit vote is independent from the real vote of a voter, audit ballots do not compromise coercion-resistance. We show how audit ballots can be introduced in Helios, Prêt à Voter and JCJ/Civitas, without complicating the voter experience.

3.4 Attacking and fixing privacy in Helios

Veronique Cortier (INRIA – Nancy, FR)

Joint work of Cortier, Veronique; Smyth, Ben;
Main reference Veronique Cortier, Ben Smyth, "Attacking and Fixing Helios: An Analysis of Ballot Secrecy," Proceedings of the IEEE Computer Security Foundations Symposium (CSF 2011), pages 297–311, 2011.
URL http://dx.doi.org/10.1109/CSF.2011.27

Helios 2.0 is an open-source web-based end-to-end verifiable electronic voting system, suitable for use in low-coercion environments. In this talk, we analyse ballot secrecy and discover a vulnerability which allows an adversary to compromise the privacy of voters. The vulnerability exploits the absence of ballot independence in Helios and works by replaying a voter's ballot or a variant of it, the replayed ballot influences the election outcome, introducing information that can be used to violate privacy. We demonstrated the practicality of the attack by breaking privacy in a mock election using the current Helios implementation. Moreover, the feasibility of an attack is considered in the context of French legislative elections and, based upon our findings, we believe it constitutes a real threat to ballot secrecy in such settings.

We present a fix and show that our solution satisfies a formal definition of ballot secrecy using the applied pi calculus. In addition, we discuss the relationship between independence and privacy properties.

3.5 CRAVE: A Challenge Response Application to Voting Electronically

Jeremy Epstein (SRI – Arlington, US)

Internet voting is widely promoted in the U.S. as a way to improve voter turnout, especially by military and overseas voters, but security has been the primary obstacle to adoption, especially for marked ballot return. In this presentation we describe CRAVE, a variant on code voting using commercially available low-cost challenge-response devices as a means to allow accurate marked ballot return, even in the face of malware running in the voter's browser or elsewhere on her computer. The goal of CRAVE is to explore the range of user interfaces that can be used successfully by voters that improve security in the real world; it is not intended to address the full range of voting characteristics such as those addressed by cryptographic End-to-End systems.

3.6 Validation of User Models: Should e-voting machine development be driven by Murphy's Law?

Paul Gibson (Telecom – Evry, FR)

Verifying that an e-voting system works correctly requires making assumptions about the environment in which the system is used.

In particular, one must model the users of the system and validate that this model corresponds to some reality. However, from our experience in developing a novel voting interface, we have observed that such models are particularly difficult to build and validate. Through a number of iterations and experimental observations we planned to converge towards a better user model, and - as a consequence - a better user interface.

Unfortunately, our understanding of the voting system environment has been recently compromised when we considered untrusted users: those users whose behaviour cannot be trusted to follow the assumptions that we make. It appears that no matter how much one anticipates the behaviour of untrusted users, Murphy's law for user modelling rules supreme: "If your model of user behaviour can be invalidated it will be invalidated".

3.7 Secure Internet Voting on an Untrusted Platform

Rolf Haenni (Bern University of Applied Sciences, CH)

Many different electronic voting protocols have been developed during the last two decades. Most of them assume the secure platform problem to be solved.

Applying them for voting over the Internet with voters using their PCs or notebooks is therefore problematic. Malicious software installed on these devices can easily harm the integrity and secrecy of the vote. One approach to solve the secure platform problem in this context is to distribute trusted devices to the voters. We discuss the design and the properties of such a device from a practical perspective in terms of usability, security, and cost.

3.8 Security Problems in India's Electronic Voting System

J. Alex Halderman (University of Michigan, US)

Joint work of Wolchok, Scott; Wustrow, Eric; Halderman, J. Alex; Prasad, Hari K.; Kankipati, Arun; Sakhamuri, Sai Krishna; Yagati, Vasavya; and Gonggrijp, Rop

Main reference Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, Rop Gonggrijp, "Security Analysis of India's Electronic Voting Machines," Proc. 17th ACM Conference on Computer and Communications Security (CCS'10), pp. 1–14, Chicago, IL, October 2010

URL http://indiaevm.org

India uses paperless electronic voting machines (EVMs) for its state and national elections. These machines use a simple embedded system architecture that makes them considerably different from the complex electronic voting systems found in the U.S. and Europe (where almost all prior research has focused). Despite growing suspicions of fraud, Indian authorities have never permitted a serious, independent review of the machines' security.

Hyderabad-based engineer Hari Prasad spent a year trying to convince election officials to complete such a review, but they insisted that the government-made machines were "perfect," "infallible," and "tamperproof." Then, in February 2010, an anonymous source gave him access to one of the machines for study. E-voting researchers J. Alex Halderman from the University of Michigan and Rop Gonggrijp from the Netherlands join him in India for the study. The team discovered that, far from being tamper-proof, the machines suffer from serious weaknesses that could be exploited to alter national election results.

Months of hot debate about these findings have produced a growing consensus that India's electronic voting machines should be scrapped, as well as nascent efforts to create a better system. There have also been more disturbing developments: Prasad was arrested and jailed in August by authorities demanding to know the identity of the anonymous source.

He has since been released on bail, and received the Electronic Frontier Foundation's Pioneer Award for his work.

In this talk, Halderman will describe the design and motivations behind India's electronic voting system, the technical problems, and the implications of the machines' security weaknesses for voting technology in India and beyond. He'll also discuss some of the formidable practical challenges that India and many other democracies face in conducting elections. Designing voting systems that provide transparency and security under these constraints presents many open problems.

3.9 Digital Democratization: Suffrage Expansion and the Decline of Political Machines in Brazil

F. Daniel Hidalgo (University of California, US)

Transitions to democracy often included institutional reforms that extended the franchise and reduced the capacity of incumbent governments to fraudulently manipulate elections. While existing studies have provided substantial insight on the broad effects of institutional reforms, there is little systematic and comparable evidence on which democratizing reforms were most consequential for political representation, as well as precise comparisons of their effects. To provide such evidence, I exploit the phased adoption of electronic voting in Brazil, a reform that I find increased the effective franchise in legislative elections by about 33% and eliminated fraud in the vote counting process.

Because the reform was initially implemented in municipalities with an electorate over an arbitrary threshold, I study its effects using a "regression discontinuity" design, which ensures a high degree of internal validity. The two distinct effects of electronic voting - the enfranchisement of illiterates and other low information voters and the elimination of fraud - had consequences for the composition of the national legislature. Against the predictions of recent economic models of democratization, I find that the enfranchisement of illiterates and other low information voters caused a small increase in the vote shares of right-wing candidates. More importantly, newly enfranchised voters were dramatically more likely to cast a "party list" or partisan ballot as opposed to a personal or candidate ballot, which benefitted Brazil's more programmatic and ideologically coherent parties. In states with hegemonic conservative parties, I find that the introduction of electronic voting induced a roughly 20 percentage point swing against "political machine" candidates, which I attribute to the elimination of fraud. In these states, new voting technology resulted in a sharp increase in political competition and harmed right-of-center candidates.

Overall, I argue that the most important consequences of the reform was the strengthening of Brazil's major parties and a weakening of dominant subnational conservative political machines.

3.10 Internet Voting in the United States

Candice Hoke (Cleveland State University, US)

Within the United States, 60% of the States have approved voting methods for overseas civilian and military voters that utilize the public internet for the return of voted (marked) ballots. While most States require voting systems to undergo independent testing of their vendors' claims of security, voter privacy, accuracy and resiliency, the States have generally not conceptualized these internet- facing systems as voting systems. The internet voting systems have thus escaped independent certification reviews.

The largely unregulated free market approach permits vendors to overstate the security, privacy and other attributes of these systems, and to conceal flaws, needed mitigations, and defense in depth security steps needed for secure operation of the systems. The Federal agency's advocacy of all-electronic elections before the technology was proven to have reached high assurance standards has played a major, regrettable role.

3.11 An Efficient Implementation of a Highly Sound Voter Verification Technique on a Smart Card and its Application to Internet Voting

Rui Joaquim (Polytechnic Institute of Lisbon/INESC-ID – Lisboa, PT)

Joint work of Joaquim, Rui; Ribeiro, Carlos; Ferreira, Paulo
Main reference Rui Joaquim, Carlos Ribeiro, Paulo Ferreira, "Towards Trustworthy Internet Elections," INESC-ID Tec. Rep. 9/2011, February 2011.
URL http://www.inesc-id.pt/ficheiros/publicacoes/7135.pdf

Uncontrolled Internet voting is the most challenging scenario for electronic voting as the voter uses an insecure/uncontrolled platform to vote. We present a solution to the insecure platform problem of Internet voting using a tamper resistant device (e.g. smart card). However, we do not just move the trust assumptions from the PC to the tamper resistant device, we have completely removed all trust assumptions on the election integrity from both the PC and the tamper resistant device by adding a highly sound voter verification technique to the vote encryption [1]. Moreover, our system also uses a code voting approach to communicate the voter's choice to the tamper resistant device, which enables the voter to vote privately even when using public computers, e.g. computers at a public library or at a cybercafé.

References

1 Rui Joaquim and Carlos Ribeiro. *An Efficient and Highly Sound Voter Verification Technique and its Implementation.* Vote-ID 2011, Tallinn, Estonia, 2011. To appear.

3.12 Encoding complex ballots

Hugo Jonker (University of Luxembourg, LU)

Various end-to-end verifiable systems have been proposed in recent years. These systems often rely on a predefined way of filling in the ballot. However, election systems vary from country to country, and sometimes from region to region. We illustrate the problem by means of two non-trivial systems (Luxembourgian general elections and German bundesland elections). In both systems, voters not only get to express multiple benefits, but can vote multiple times for the same candidate. In addition, there are shortcut options (voting for all members of one party).

We outline one approach to reconcile the existing voter experience (which may be enshrined in law) with the Prêt à Voter system.

3.13 How to Store Some Secrets

Reto Koenig (Bern University of Applied Sciences, CH)

The key idea of coercion-resistant electronic voting protocols is to allow voters to deceive the adversary with faked credentials. Keeping up the deception under all possible circumstances requires the voter to remember multiple high-entropy credentials. This obviously states a hard problem for the human brain. We introduce the concept of a secret storing system, which allows users to conveniently store multiple high-entropy credentials with low-entropy passphrases in one single storage. Both the credentials and the passphrases can be chosen freely and independently. We propose a concrete realisation of such a system using interpolation polynomials over prime fields.

3.14 Election Observation of New Voting Technologies

Robert Krimmer (OSCE – Warszaw, PL)

The use of information and communication technologies in elections has expanded considerably in recent years. This development has however not been uniform across the OSCE. A growing number of participating States have introduced New Voting Technologies (NVT) or are considering it, while others have stopped and returned to traditional voting methods. NVT have raised questions about the compliance of these new electronic systems with OSCE commitments and international obligations for democratic elections. As a result, a number of international organizations and institutions, including ODIHR, have been paying increased attention to this issue.

Transparency and observation are cornerstones of OSCE election-related commitments. They are necessary to ensure that votes are cast by secret ballot or by equivalent free voting procedure, and that they are counted and reported honestly with the official results made public.

However, NVT poses new challenges to the traditional and broadly accepted concepts of transparency and accountability of election processes to election administrators, voters and election observers. Hence, concerns about security and secrecy of the ballot as well as the reliability of electronic voting have become the subject of public debate in a number of countries, thereby influencing public perceptions and confidence in elections in general. NVTs have so far not reached the same level of universal acceptance, trust and confidence as paper voting. But NVT can help offer additional functionalities to elections that paper ballots cannot, for instance in cases when counting is complicated due a large numbers of concurrent elections, voting for the blind, etc.

Observing elections using NVT is a challenge. Electronic events are more difficult to observe because specialized technical skills are needed. Electronic voting consists of technological components that are not readily nor easily understood by the average observer. There is a need for an ODIHR approach to NVT in a methodological framework that dovetails with ODIHR overall methodological approach to election observation. It should also support election advisers in their daily work regarding developments with regards to NVT.

3.15 Verification, Security, and Voter Understanding

Morgan Llewellyn (IMT – Lucca, IT)

Joint work of Culnane, Chris; Heather, James; Llewellyn, Morgan; Schneider, Steve; Srinivasan, Sriram; Xia, Zhe (Joson)

Currently, a variety of voting schemes seek to increase voter confidence by allowing voters to verify that their vote has been recorded. Each of these voting systems assume that the gain in confidence from verifying their vote is greater than any potential loss of confidence resulting from voter beliefs that the verification process may reveal vote choice. Why this assumption may be natural to computer scientists, it is possible that many voters do not understand event basic ballot security features. It is in this context that we test individual understanding of random candidate ordering in a Prêt à Voter style ballot form.

Individual understanding of the ballot form was done through a series of experiments conducted at the University of Surrey. The goal of the experiments was to test individual understanding of the security features provided by randomized candidate ordering. Results indicate that a clear majority of participants understand the security features of randomized candidate ordering. However, results also reveal that some individuals did not fully understand the ballot security features and highlight the potential for attacks on user confidence resulting from large N.

3.16 The Limits of Theory: Assumptions on Which We Base Voting Protocol Security

Tal Moran (Harvard University, US)

One of the contributions of computer science theory to voting security is the notion of "security reductions": the idea that we can reduce the security of a complex system to the security of simpler components. This makes practical verification of security a more tractable problem: if we can prove a security reduction, it is enough that we check the individual components to be convinced that the system as a whole is secure. At the end of the day, however, we are always left with security "axioms": basic assumptions that we cannot reduce further on which the security of the system relies.

When we evaluate and compare voting systems, in addition to looking at what they provide, we should also be thinking about the basic assumptions they rely on.

I'll describe some of the common assumptions on which we base end-to-end verifiable voting systems and discuss their relation to reality.

3.17 Running mixnet-based elections with Helios

Olivier Pereira (UC Louvain-la-Neuve, BE)

Joint work of Bulens, Philippe; Giry, Damien; Pereira, Olivier
Main reference Philippe Bulens, Damien Giry, Olivier Pereira, "Running Mixnet-Based Elections with Helios," Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE '11), 2011.
URL http://www.usenix.org/event/evtwote11/tech/

The Helios voting system is an open-audit web-based voting system that has been used by various institutions in real-stake elections during the last few years. While targeting the simplicity of the election workflow, the homomorphic tallying process used in Helios limits its suitability for many elections (large number of candidates, specific ballot filling rules, . . .).

We present a variant of Helios that allows an efficient mixnet-based tallying procedure, and document the various choices we made in terms of election workflow and algorithm selection. In particular, we propose a modified version the TDH2 scheme of Shoup and Gennaro that we found particularly suitable for the encryption of the ballots.

Our Helios variant has been tested in two multi-thousand voter elections. The lessons taken from the first of these elections motivated some changes into our procedure, which have been successfully experimented during the second election. Voter survey data are also presented.

3.18 Wombat in the wild

Ben Riva (Tel Aviv University, IL)

We present a new electronic voting system called Wombat. Wombat is designed to be similar to the current Israeli paper based elections and it combines a paper based voting system with an electronic one, in a way that both systems complete each other.

We show the highlights of the protocol, briefly describe its implementation, and talk about a pilot we ran in a student council election with over 2000 voters.

3.19 Prêt à Voter with Confirmation Codes

Peter Y. A. Ryan (University of Luxembourg, LU)

Main reference to appear in the proceedings of EVT/WOTE 2011

A scheme is presented in which a Pretty Good Democracy style confirmation code mechanism is incorporated into Prêt à Voter. The idea is to provide voters with an immediate, easy to use confirmation at the time of casting of the correct registration of their receipt on the Web Bulletin Board. As with PGD, the registration and revelation of the confirmation code is performed by a threshold set of Trustees. Verification of the registration of the vote is now part of the vote casting and therefore more immediate and convenient for the voters.

The scheme presented here is thus more convenient while maintaining the level of verifiability of conventional Prêt à Voter. It also means that we are less reliant on the diligence of voters in later performing checks on the Bulletin Board. It seems probable that this confirmation code mechanism will provide voters with greater confidence that their vote will be accurately tallied.

3.20 Focus Groups Study on Prêt à Voter

Steve Schneider (University of Surrey, GB)

Joint work of Schneider, Steve; Llewellyn, Morgan; Culnane, Chris; Heather, James; Srinivasan, Sriramkrishnan; Xia, Zhe
Main reference Steve Schneider, Morgan Llewellyn, Chris Culnane, James Heather, Sriramkrishnan Srinivasan, Zhe Xia, "Focus Groups Study on Prêt à Voter 1.0," Proceedings of RE-Vote: International Workshop on Requirements Engineering for Electronic Voting Systems Trento, Italy, 2011.
URL http://www.computing.surrey.ac.uk/personal/st/S.Schneider/papers/2011/RE-Vote11.pdf

This presentation discussed the findings of a series of four focus group sessions carried out in the UK on a variant of the original Prê tà Voter verifiable voting system prototype implementation. The aim of these sessions was to investigate users' ability to use the system, to discover any inadequacies of the system, and to gauge the participants' understanding of its security mechanisms. Participants were asked to use the system to cast a vote, to audit their ballot forms and to confirm online that their vote had been received.

The groups also discussed general issues around security in election systems.

While voters were able to cast their votes reliably, some displayed less understanding of the security procedures they were required to carry out.

3.21 Some ideas about receipt-free cast-as-intended Internet voting for preferential elections

Vanessa Teague (The University of Melbourne, AU)

We discuss whether a remote electronic voting system might provide both strong privacy properties and strong verification that the vote was cast as intended.

We speculate on some weaker alternatives to full receipt freeness and how they might be achieved. For example, it seems reasonable to expect that the voter cannot produce a proof that can be sent to a remote party who was unable to tap the voter's communications. We compare the approach with others that achieve similar objectives based on credentials or codes. Our primary motivation is the difficulty of using either the Juels- Catalano-Jakobsson method or voting codes for preferential voting.

3.22 Internet Voting in Estonia

Alexander Trechsel (European University Institute, IT)

Joint work of Trechsel, Alexander; Vassil, Kristjan

Recent years has seen an increasing interest in Internet voting from the point of view of political scientists as well as from the perspective of policy makers. Some have argued that the introduction of e-voting boosts electoral participation by bringing down the barriers hindering electoral turnout. Others have kept a more pessimistic view, claiming that e-voting affects only those few who are highly engaged in politics already. This study aims to shed light on the topics beyond this debate. In particular, our objective is to analyze the determinants that lead some citizens to opt for e-voting and others for traditional means of participation. We ask the question of who is voting online and how can we explain the choice of the voting channel? On the basis of five e-enabled elections in Estonia we demonstrate that the introduction of internet voting has a modest effect on aggregate levels of turnout. On the individual level we find that choosing to vote online is associated with trust toward e-voting system, as well as higher levels of computer literacy. Additionally we find that the language cleavage remains an important predictor of internet voting in Estonia. Interestingly, as time has passed since the first e-enabled elections we find that traditional determinants of e-voting, such as age, gender, urban residence, income, etc, gradually loose their power.

3.23 What happened in Sarasota?

Dan Wallach (Rice University, US)

URL http://www.cs.rice.edu/~dwallach/pub/sarasota07.pdf

The November 2006 race for Florida's 13th Congressional District resulted in a 369 vote margin of victory for the winning candidate with more than 18,000 undervotes recorded on the ES&S iVotronic touch-screen voting machines used in Sarasota County. This talk summarizes what happened, what theories might explain it, and what steps were taken at the time and afterward to understand the mystery.

3.24 Swiss Elections to the National Council: First trials with e-voting in elections at federal level

Anina Weber (Federal Chancellery – Bern, CH)

Main reference Anina Weber, Geo Taglionoi, “Swiss Elections to the National Council: First trials with e-voting in elections at federal level,” Dagstuhl Preprint Archive, arXiv:1109.2489v2 [cs.CY]
URL http://arxiv.org/abs/1109.2489v2

On October 23rd 2011, around 22,000 voters will be authorized to cast their votes electronically in occasion of the elections to the National Council. These are the first trials ever with e-voting in elections at federal level in Switzerland. Four cantons are going to conduct trials with this new channel. Only Swiss voters living abroad will be authorized to participate.

The Swiss Confederation pursues the long term goal of the introduction of e-voting as a third, complementary voting method in addition to voting in person at the polling station and postal voting.

3.25 Verifiable voting with everlasting privacy

Jeroen van de Graaf (Federal University of Minas Gerais, Brazil, BR)

Main reference van de Graaf, Jeroen, “Voting with unconditional privacy: CFSY for booth voting,” unpublished manuscript
URL http://eprint.iacr.org/2009/574

We study the Cramer, Franklin, Schoenmaker and Yung internet voting protocol for the booth setting. In this protocol, so called Pedersen commitments are used to define an unconditionally hiding commitment scheme. Because of its homomorphic properties, they are particularly suited for voting protocols with unconditional privacy.

In fact, a survey shows that almost all these protocols use, or could benefit from, these commitments. Though not novel cryptographically speaking, the protocol presented is interesting from a voting perspective, because it is simple enough to be understood by non-cryptographers, yet has many desirable properties, such as unconditional privacy, correctness under the discrete log assumption, individual and universal verifiability, and (optionally) ballot casting assurance.

In addition, we discuss interesting relations to and/or simplifications, of several other protocols, such as the booth voting protocol of Moran and Naor, SplitBallot, MarkPledge and Scratch & Vote.

4 Panel Discussions

4.1 What are the obstacles to improving the integrity of election systems?

This panel discussion was held the first afternoon of the seminar. Moderated by Michael Alvarez, participants in the discussion were David Beirne, Candice Hoke, Robert Krimmer and Alexander Trechsel.

Participants

- Michael Alvarez
  CalTech – Pasadena, US
- David Beirne
  Federal Voting Assistance
  Programm, Arlington, US
- Jonathan Ben-Nun
  Tel Aviv University, IL
- Josh Benaloh
  Microsoft Res. – Redmond, US
- Sergiu Bursuc
  University of Birmingham, GB
- Michel Chevallier
  Republique et Canton de
  Genéve, CH
- Veronique Cortier
  INRIA – Nancy, FR
- Christopher Culnane
  University of Surrey, GB
- Stéphanie Delaune
  ENS – Cachan, FR
- Jeremy Epstein
  SRI – Arlington, US
- Paul Gibson
  Telecom – Evry, FR
- Rop Gonggrijp
  Amsterdam, NL
- Rolf Haenni
  Bern University of Applied
  Sciences, CH
- J. Alex Halderman
  University of Michigan, US
- James Heather
  University of Surrey, GB
- F. Daniel Hidalgo
  University of California, US
- Candice Hoke
  Cleveland State University –
  Cleveland, US
- Rui Joaquim
  Polytechnic Institute of
  Lisbon/INESC-ID – Lisboa, PT
- Hugo Jonker
  University of Luxembourg, LU
- Reto König
  Bern University of Applied
  Sciences, CH
- Steve Kremer
  ENS – Cachan, FR
- Robert Krimmer
  OSCE - Warszaw, PL
- Manuel J. Kripp
  E-Voting.CC – Viennna, AT
- Miroslaw Kutylowski
  Wroclaw University of
  Technology, PL
- Gabriele Lenzini
  University of Luxembourg, LU
- Helger Lipmaa
  Cybernetica AS, EE
- Morgan Llewellyn
  IMT – Lucca, IT
- Symeon Meichanetzoglou
  University of Luxembourg, LU
- Tal Moran
  Harvard University, US
- Maina Olembo
  TU Darmstadt, DE
- Olivier Pereira
  UC Louvain-la-Neuve, BE
- Ben Riva
  Tel Aviv University, IL
- Mark D. Ryan
  University of Birmingham, GB
- Peter Y. A. Ryan
  University of Luxembourg, LU
- Steve Schneider
  University of Surrey, GB
- Vanessa Teague
  The University of Melbourne, AU
- Jacques Traore
  Orange Labs – Caen, FR
- Alexander Trechsel
  European University Institute, IT
- Jeroen van de Graaf
  Federal University of Minas
  Gerais, Brazil, BR
- Kristjan Vassil
  European University Institute, IT
- Dan Wallach
  Rice University, US
- Anina Weber
  Federal Chancellery – Bern, CH
- Douglas Wikström
  KTH Stockholm, SE
- Filip Zagórski
  George Washington Univ., US
- Xia Zhe
  University of Surrey, GB