Electronic elections, winter 2007

MICHAEL NÜSKEN

4. Exercise sheet
Hand in solutions until Sunday, 13 January 2007.

Exercise 4.1 (Become an expert). (3 points)

Adopt an electronic election scheme and become an expert for it!

The following choice from Sampigethaya & Poovendran (2006) may serve as a starting point. Everybody should take care of

- a single article
- presenting a complete election scheme.

We will use your expertise in the course and try to shed more light on the various issues that we only touched so far.

Pick your three favorites. As there is so much literature, we shouldn't have a collision. Send me unique identifiers for your top three. 3

We will decide on the experts in the following tutorial.

My suggestion would be that there should be one expert for the Estonian system and one for either the Australian, the Swiss, the Austrian or the American test system. Have a look at the conferences for pointers. Further, at least two or three as different as possible schemes should be covered.

The following articles are evaluated in Sampigethaya & Poovendran (2006):

- Chaum (1981) http://doi.acm.org/10.1145/358549.358563.
- Chaum (1988a) http://www.springerlink.com/content/qvlct2w6ludhpnq3/.
- Boyd (1990) http://www.springerlink.com/content/q5bqvlwjdj426lff/
- Sako and Killian (1995) http://www.springerlink.com/content/jhf7ccxn2fj2gf
- Chaum (2004) http://doi.ieeecomputersociety.org/10.1109/MSECP.2004.126 http://courses.csail.mit.edu/6.897/spring04/Chaum-SecretBallotRecei
- Cohen Benaloh and Fischer (1985) FOCS'85, not online. http://cs-www.cs.yale.edu/homes/fischer/pubs/tr416.pdf
- Cohen Benaloh and Yung (1986) http://doi.acm.org/10.1145/10590.10595
- Iverson (1992) http://www.springerlink.com/content/gpb9fff1wg53l52g/
- Sako and Killian (1994) http://www.springerlink.com/content/894fuqn5pma8d4
- Cramer et al. (1996) http://www.springerlink.com/content/879h7g6ldre6ehhe/
- Cramer et al. (1997) http://www.springerlink.com/content/51kyn10xan6nb0jh/ http://www.win.tue.nl/~berry/papers/euro97.pdf
- Schoenmakers (1999) http://www.springerlink.com/content/64h702nww7fuy03d http://citeseer.ist.psu.edu/schoenmakers1999simple.html
- Hirt and Sako (2000) http://www.springerlink.com/content/vrwq2k6gvbd3341x http://citeseer.ist.psu.edu/418947.html
- Baudron et al. (2001) http://doi.acm.org/10.1145/383962.384044
- Lee and Kim (2002) http://www.springerlink.com/content/91cf7ct3b9mmu9qa/ http://citeseer.ist.psu.edu/557992.html
- Kiayias and Yung (2002) http://www.springerlink.com/content/yrbpfvk23bq2e
- Damgård and Jurik (2001) http://www.springerlink.com/content/n4xfj9ecyyte http://citeseer.ist.psu.edu/383099.html
- Fujioka et al. (1993) http://dx.doi.org/10.1007/3-540-57220-1_66
- Baraani-Dastjerdi et al. (1995) http://citeseer.ist.psu.edu/baraani-dastjerdi
- Okamoto (1997) http://dx.doi.org/10.1007/BFb0028157, http://citeseer.ist.psu.edu/okamoto97receiptfree.html

- Juang et al. (2002) http://comjnl.oxfordjournals.org/cgi/content/abstract/45
- Golle et al. (2002) http://www.springerlink.com/content/3qt06r066jdebm2b/, http://crypto.stanford.edu/~pgolle/papers/pop.pdf
- Lee et al. (2003) http://www.springerlink.com/content/7ty2qy8ywrkyx8er/, http://citeseer.ist.psu.edu/659898.html
- Kiayias and Yung (2004) http://www.springerlink.com/content/wx1tn04w0dp3x5d http://citeseer.ist.psu.edu/651003.html
- Juels and Jakobsson (2002) http://doi.acm.org/10.1145/1102199.1102213, http://citeseer.ist.psu.edu/555869.html
- Acquisti (2004) http://citeseer.ist.psu.edu/acquisti04receiptfree.html, http://eprint.iacr.org/2004/105.pdf,

Some talks of the conferences Vote-ID 2007, Electronic Voting 2006, Electronic Voting in Europe 2004 also describe election schemes. But have a look yourself:

- Alkasar & Volkamer (2007). Vote-ID 2007: First Conference on E-Voting and Identity http://www.sirrix.de/content/pages/voteid.program.htm
- Krimmer (2006): Krimmer (Ed., 2006) Electronic Voting 2006. http://www.e-voting.cc/stories/2510688/main
  - E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world (Ülle Madise, Tarvi Martens)
  - Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed (Nadja Braun, Daniel Brändli)
  - Contributions to traditional electronic voting systems in order to reinforce citizen confidence (Ana Gómez, Sergio Sánchez, Emilia Pérez Belleboni)
  - A preliminary question: Is e-voting actually useful for our democratic institutions? What do we need it for? (Jordi Barrat Esteve)
  - How e- voting technology challenges traditional concepts of citizenship: an analysis of French voting rituals (Laurence Monnoyer-Smith)
  - The electoral legislation of the Basque autonomous community regarding electronic vote (Rosa M. Fernández, Esther González, José Manuel Vera)

  - E-Voting in Brazil - The Risks to Democracy (José Rodrigues-Filho, Cynthia J. Alexander, Luciano C. Batista)
  - Multiple Casts in Online Voting: Analyzing Chances (Melanie Volkamer, Rüdiger Grimm)
  - How to create trust in electronic voting over an untrusted platform (Gerhard Skagestein, Are Vegard Haug, Einar Nødtvedt, Judith Rossebø)
  - A generic re-engineering methodology for the organized redesign of the electoral process to an e-electoral process (Alexandros Xenakis, Ann Macintosh)
  - Election Workflow Automation - Canadian Experiences (Goran Obradovic, James Hoover, Nick Ikonomakis John Poulos)
  - A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament (Joao Falcao e Cunha, Mario Jorge Leitao, Joao Pascoal Faria, Miguel Pimenta Monteiro, Maria Antonia Carravilla)
  - Voting in Uncontrolled Environment and the Secrecy of the Vote (Kare Vollan)
  - Coercion-Resistant Electronic Elections with Observer (Jorn Schweisgut)
  - Maintaining Democratic Values in e-Voting with eVACS (Carol Boughton)
  - Transition to electronic voting and citizen participation (Letizia Caporusso, Carlo Buzzi, Giolo Fele, Pierangelo Peri, Francesca Sartori)
  - Security Requirements for Non-political Internet Voting (Rudiger Grimm, Robert Krimmer, Nils Meisner, Kai Reinhard, Melanie Volkamer, Marcel Weinand)
  - Online Voting Project . New Developments in the Voting System and Consequently Implemented Improvement in the Representation of Legal Principles (Klaus Diehl, Sonja Weddeling)
  - The Voting Challenges in e-Cognocracy (Joan Josep Piles, Jose Luis Salazar, Jose Ruiz, Jose Maria Moreno-Jimenez)
  - E-Voting in Slovenia: The view of parliamentary deputies (Tina Juki., Mirko Vintar)

- Prosser & Krimmer (2004): Prosser & Krimmer (Eds., 2004) Electronic Voting in Europe. `http://www.e-voting.at/main.php?ID=88`, `http://static.twoday.net/evoting/files/E-Voting-in-Europe-Proceedin`

- Towards European Standards on Electronic Voting (Michael Remmert)
- E-Democracy in E-Austria (Christian Rupp)
- The Dimensions of Electronic Voting (Alexander Prosser, Robert Krimmer)
- E-Voting: International Developments and Lessons Learnt (Thomas M. Buchsbaum)
- E-Voting: Switzerland's Projects and their Legal Framework (Nadja Braun)
- Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions (Bernard van Acker)
- E-Voting and Biometric Systems (Sonja Hof)
- Security as Belief User's Perceptions on the Security of E-Voting Systems (Anne-Marie Oostveen, Peter van den Besselar)
- Towards Remote E-Voting: Estonian case (Epp Maaten)
- Verifiability and Other Technical Requirements for Online Voting Systems (Niels Meißner, Volker Hartmann, Dieter Richter)
- From Legal Principles to an Internet Voting System (Melanie Volkamer, Dieter Hutter)
- How Security Problems can Compromise Remote Internet Voting Systems (Guido Schryen)
- E-Voting and the Architecture of Virtual Space (Anthoula Maidou, Hariton M. Polatoglou)
- The UK Deployment of the E-Electoral Register (Alexander Xenakis, Ann Macintosh)
- E-Voting in Austria Legal requirements and First Steps (Patricia Heindl)
- Security Assets in E-Voting (Alexander Prosser, Robert Kofler, Robert Krimmer, Martin Karl Unger)

Further sources:

- EVOX (1999-) `http://groups.csail.mit.edu/cis/voting/voting.html`
- Workshop Frontiers in Electronic Elections (FEE 2005) `http://www.win.tue.nl/~berry/fee2005/program.html`
- Improving U.S. Voting Systems. `http://vote.nist.gov/`

- Estonian National Electoral Committee. http://www.vvk.ee/engindex.html

This list is by far *not* complete.

References

AMMAR ALKASAR & MELANIE VOLKAMER (editors) (2007). *VOTE-ID 2007: First Conference on E-Voting and Identity*, number to appear in Lecture Notes in Computer Science. Sirrix AG security technologies, Springer-Verlag, Berlin, Heidelberg. ISBN ??? ISSN 0302-9743 (Print) 1611-3349 (Online). URL http://www.sicherheit2008.de/content/pages/voteid.program.htm.

ROBERT KRIMMER (editor) (2006). *Electronic Voting 2006. 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC*, number P-86 in GI-Edition - Lecture Notes in Informatics. Köllen Druck+Verlag, Bonn. ISBN 978-3-88579-180-5. ISSN 1617-5468. URL http://www.gi-ev.de/service/publikationen/lni/gi-edition-lecture-notes-in-info
For slides and videos(!) of the presentations and proceedings PDFs see http://www.e-voting.cc/topics/conference2006.

ALEXANDER PROSSER & ROBERT KRIMMER (editors) (2004). *Electronic Voting in Europe - Technology, Law, Politics and Society*, number P-47 in GI-Edition - Lecture Notes in Informatics. Köllen Druck+Verlag, Bonn. ISBN 3-88579-376-8. ISSN 1617-5468. URL http://www.gi-ev.de/service/publikationen/gi-edition-lecture-notes-in-informat
For slides see http://www.e-voting.at/main.php?ID=88, for PDF see http://www.e-voting.cc/stories/1275718/.

KRISHNA SAMPIGETHAYA & RADHA POOVENDRAN (2006). A framework and taxonomy for comparison of electronic votingnext term schemes. *Computers & Security* **25**(2), 137–153. ISSN 0167-4048. URL http://dx.doi.org/10.1016/j.cose.2005.11.003.