Lecture Notes in Computer Science 6000

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

David Chaum Markus Jakobsson
Ronald L. Rivest Peter Y.A. Ryan
Josh Benaloh Miroslaw Kutylowski
Ben Adida (Eds.)

Towards Trustworthy Elections

New Directions in Electronic Voting

Springer

Volume Editors

David Chaum
Independent researcher; david@chaum.com

Markus Jakobsson
Palo Alto Research Center, CA, USA; markus.jakobsson@gmail.com

Ronald L. Rivest
Massachusetts Institute of Technology, Cambridge, MA, USA; rivest@mit.edu

Peter Y.A. Ryan
University of Luxembourg, Luxembourg; peter.ryan@uni.lu

Josh Benaloh
Microsoft Research Center, Redmond, WA, USA; benaloh@microsoft.com

Miroslaw Kutylowski
Wroclaw University of Technology, Poland; mirekk@swarog.im.pwr.wroc.pl

Ben Adida
Harvard Center for Research on Computation and Society Boston, MA, USA
ben@adida.net

Administrative Editor

Richard Carback
University of Maryland Baltimore County, Baltimore, MD, USA
carback1@umbc.edu

Library of Congress Control Number: 2010927806

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, J.1, H.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-12979-X Springer Berlin Heidelberg New York
ISBN-13 978-3-642-12979-7 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© IAVOSS/Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Foreword

Cryptography applied to elections holds the promise of being:

- A critical step in a centuries-long and hard-fought struggle for voting rights.
- An end to disputed elections justifying power grabs and the erosion of democracy.
- A stop to a legacy of profit from bungled technology and outmoded analysis.
- A potential reversal of declining voter confidence.
- A breakthrough that for the first time lets voters verify that their own votes are counted.
- A scalable system for secret ballot elections with transparent integrity.
- A technology capable of taking democracy to new levels.

If you are interested in this challenging problem—a problem that even school children can understand but that is made harder than traditional computer security by requirements for public verifiability and ballot secrecy—then this volume is for you. Just as cryptography can keep messages secure for senders no matter the routing to the destination, in principle it can keep votes secure for voters, from vote casting all the way through to inclusion of votes in the final tally. The challenge addressed here is to find practical means suitable for actual elections.

In 2001, Ron Rivest and myself invited all those we could find who had published more than one academic paper on voting security to a "Workshop On Trustworthy Elections." Almost all of them attended. This first workshop on the subject took place in a room built nearly a century earlier to house, fittingly, technology for the first public global radio communication system. A remarkable consensus emerged during the discussion session on the last day, the conclusion that cryptography holds real promise to improve elections and a decision to explore it further.

A series of WOTE workshops ensued, sometimes under names adapted to sponsoring organizations, and ultimately resulting in an annual event sponsored by its own international association—the International Association for Voting Systems Sciences. In addition to this open series of conferences, there was also a week-long invitation-only workshop in 2007.

This volume represents, for each of these meetings, papers selected by a key member of the respective Program Committee serving as an invited editor. The volume aims to be comprehensive as far as the flavor and scope of the field and to bring together important but previously unpublished works. It should prove a valuable resource for those curious about, entering, or seeking a deeper understanding of this extraordinarily important and open-ended new field.

February 2010 David Chaum

Organization

WOTE 2001
Workshop on Trustworthy Elections
August 2001Marconi Conference Center, Tomales Bay, California
Organizers: Ronald L. Rivest, *David Chaum*

DIMACS Workshop on Electronic Voting—Theory and Practice
May 2004 DIMACS Center, Rutgers University
Organizers: *Markus Jakobsson*, Ari Juels

Workshop Frontiers in Electronic Elections
September 2005 University of Milan
Program Committee: Christian Cachin, Jean-Jacques Quisquater, *Ronald L. Rivest*, Peter Y.A. Ryan, Berry Schoenmakers

WOTE 2006
June 2006 Cambridge University
General Chair: *Peter Y.A. Ryan*

WOTE 2007
June 2007 University of Ottawa
Program/General Chair: *Josh Benaloh*

Frontiers of Electronic Voting
June/July 2007 Schloss Dagstuhl
Organizers: David Chaum, *Miroslaw Kutylowski*, Ronald L. Rivest, Peter Y.A. Ryan

WOTE 2008
July 2008 Katholieke Universiteit Leuven, Belgium
Chairs: *Ben Adida*, Olivier Pereira

The names of editors of this volume appear in italics above. Financial and other support for these six events was provided, respectively, in part by:

(1) CalTech/MIT Voting Technology Project and the organizers
(2) Center for Discrete Mathematics and Theoretical Computer Science, Rutgers and Princeton Universities
(3) European Network of Excellence in Cryptology in association with the 10th European Symposium on Research in Computer Security
(4) IAVOSS in association with the Privacy Enhancing Technologies Symposium 2006
(5) IAVOSS in association with the Privacy Enhancing Technologies Symposium 2007
(6) Schloss Dagstuhl, Leibniz Center for Informatics
(7) Katholieke Universiteit Leuven

Table of Contents

The Witness -Voting System 1
Ed Gerck

Coercion-Resistant Electronic Elections 37
Ari Juels, Dario Catalano, and Markus Jakobsson

Receipt-Free K-out-of-L Voting Based on ElGamal Encryption 64
Martin Hirt

A Secure Architecture for Voting Electronically (SAVE) 83
Jonathan A. Goler and Edwin J. Selker

A Modular Voting Architecture ("Frog Voting") 97
Shuki Bruck, David Jefferson, and Ronald L. Rivest

Unconditionally Secure Electronic Voting 107
Akira Otsuka and Hideki Imai

Electronic Elections: A Balancing Act 124
Pedro A.D. Rezende

An Implementation of a Mix-Net Based Network Voting Scheme and Its Use in a Private Organization 141
Jun Furukawa, Kengo Mori, and Kazue Sako

The Vector-Ballot Approach for Online Voting Procedures 155
Aggelos Kiayias and Moti Yung

On Optical Mark-Sense Scanning 175
Douglas W. Jones

On Some Incompatible Properties of Voting Schemes 191
Benoît Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern, and Jacques Traoré

A Threat Analysis of Prêt à Voter 200
Peter Y.A. Ryan and Thea Peacock

Anonymity in Voting Revisited 216
Hugo Jonker and Wolter Pieters

Anonymous One-Time Broadcast Using Non-interactive Dining Cryptographer Nets with Applications to Voting 231
Jeroen van de Graaf

An Introduction to PunchScan 242
Stefan Popoveniuc and Ben Hosp

Component Based Electronic Voting Systems 260
David Lundin

A Verifiable Voting Protocol Based on Farnel (Extended Abstract) 274
Roberto Araújo, Ricardo Felipe Custódio, and Jeroen van de Graaf

Verifying Privacy-Type Properties of Electronic Voting Protocols: A Taster 289
Stéphanie Delaune, Steve Kremer, and Mark Ryan

Improving Remote Voting Security with CodeVoting 310
Rui Joaquim, Carlos Ribeiro, and Paulo Ferreira

A Practical and Secure Coercion-Resistant Scheme for Internet Voting (Extended Abstract) 330
Roberto Araújo, Sébastien Foulle, and Jacques Traoré

Scratch, Click & Vote: E2E Voting over the Internet 343
Mirosław Kutyłowski and Filip Zagórski

Securing Optical-Scan Voting 357
Stefan Popoveniuc, Jeremy Clark, Richard Carback, Aleks Essex, and David Chaum

Attacking Paper-Based E2E Voting Systems 370
John Kelsey, Andrew Regenscheid, Tal Moran, and David Chaum

Aperio: High Integrity Elections for Developing Countries 388
Aleks Essex, Jeremy Clark, and Carlisle Adams

Author Index 403