

Robert Krimmer · Melanie Volkamer
Nadja Braun Binder · Norbert Kersting
Olivier Pereira · Carsten Schürmann (Eds.)

Electronic Voting

Second International Joint Conference, E-Vote-ID 2017
Bregenz, Austria, October 24–27, 2017
Proceedings

Editors

Robert Krimmer 
Tallinn University of Technology
Tallinn
Estonia

Melanie Volkamer 
Technische Universität Darmstadt
Darmstadt
Germany

Nadja Braun Binder 
German Research Institute for Public
Administration
Speyer
Germany

Norbert Kersting
University of Münster
Münster
Germany

Olivier Pereira
Université Catholique de Louvain
Louvain
Belgium

Carsten Schürmann 
IT University of Copenhagen
Copenhagen
Denmark

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-68686-8

ISBN 978-3-319-68687-5 (eBook)

DOI 10.1007/978-3-319-68687-5

Library of Congress Control Number: 2017955783

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Election Security and Economics: It's All About Eve	1
<i>David Basin, Hans Gersbach, Akaki Mamageishvili, Lara Schmid, and Oriol Tejada</i>	
Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations	21
<i>Ralf Küsters and Johannes Müller</i>	
Voting in E-Participation: A Set of Requirements to Support Accountability and Trust by Electoral Committees	42
<i>Peter Parycek, Michael Sachs, Shefali Virkar, and Robert Krimmer</i>	
The Weakness of Cumulative Voting.	57
<i>Josh Benaloh</i>	
No More Excuses: Automated Synthesis of Practical and Verifiable Vote-Counting Programs for Complex Voting Schemes	66
<i>Lyria Bennett Moses, Rajeev Goré, Ron Levy, Dirk Pattinson, and Mukesh Tiwari</i>	
Public Evidence from Secret Ballots	84
<i>Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y.A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach</i>	
Towards a Mechanized Proof of Selene Receipt-Freeness and Vote-Privacy . . .	110
<i>Alessandro Bruni, Eva Drewsen, and Carsten Schürmann</i>	
Trust Implications of DDoS Protection in Online Elections.	127
<i>Chris Culnane, Mark Eldridge, Aleksander Essex, and Vanessa Teague</i>	
Updated European Standards for E-voting: The Council of Europe Recommendation Rec(2017)5 on Standards for E-voting	146
<i>Ardita Driza Maurer</i>	
A Formally Verified Single Transferable Voting Scheme with Fractional Values.	163
<i>Milad K. Ghale, Rajeev Goré, and Dirk Pattinson</i>	
Reverse Bayesian Poisoning: How to Use Spam Filters to Manipulate Online Elections	183
<i>Hugo Jonker, Sjouke Mauw, and Tom Schmitz</i>	

Return Code Schemes for Electronic Voting Systems	198
<i>Shahram Khazaei and Douglas Wikström</i>	
Eos a Universal Verifiable and Coercion Resistant Voting Protocol	210
<i>Ştefan Patachi and Carsten Schürmann</i>	
Clash Attacks and the STAR-Vote System	228
<i>Olivier Pereira and Dan S. Wallach</i>	
Verifiability Experiences in Government Online Voting Systems.	248
<i>Jordi Puiggalí, Jordi Cucurull, Sandra Guasch, and Robert Krimmer</i>	
Cast-as-Intended Mechanism with Return Codes Based on PETs.	264
<i>Achim Brelle and Tomasz Truderung</i>	
How Could Snowden Attack an Election?	280
<i>Douglas Wikström, Jordi Barrat, Sven Heiberg, Robert Krimmer, and Carsten Schürmann</i>	
Bits or Paper: Which Should Get to Carry Your Vote?	292
<i>Jan Willemson</i>	
Estonian Voting Verification Mechanism Revisited Again	306
<i>Ivo Kubjas, Tiit Pikma, and Jan Willemson</i>	
Author Index	319