Usable Security Evaluation of EasyVote in the Context of Complex Elections

Vom Fachbereich Informatik der

Technischen Universität Darmstadt genehmigte

Dissertation

zur Erlangung des Grades

Doktor-Ingenieur (Dr.-Ing.)

von

M.Sc. & M.Sc. IT-Sec. Jurlind Budurushi

geboren in Tirana, Albanien

Referenten:	Prof. Dr. Melanie Volkamer
	Dr. Karen Renaud
Tag der Einreichung:	08.02.2016
Tag der mündlichen Prüfung:	21.03.2016
Hochschulkennziffer:	D 17

Darmstadt 2016

List of Publications

[1] **Jurlind Budurushi**, Karen Renaud, Melanie Volkamer, and Marcel Woide. An Investigation into the Usability of Electronic Voting Systems for Complex Elections. *Annals of Telecommunications*, pages 1–14. `http://dx.doi.org/10.1007/s12243-016-0510-2`. Springer Paris, 2016. Cited on pages 73 and 99.

[2] Oksana Kulyk, Stephan Neumann, Karola Marky, **Jurlind Budurushi**, and Melanie Volkamer. Coercion-resistant Proxy Voting. In *31st International Conference on ICT Systems Security and Privacy Protection - (IFIP SEC)*, 2016. In Press.

[3] Oksana Kulyk, Stephan Neumann, **Jurlind Budurushi**, Melanie Volkamer, Rolf Haenni, Reto Koenig, and Philemon von Bergen. Efficiency Evaluation of Cryptographic Protocols for Boardroom Voting. In *10th International Conference on Availability, Reliability and Security (ARES)*, pages 224–229. IEEE, 2015.

[4] Montathar Faraon, Georg Stenberg, **Jurlind Budurushi**, and Mauri Kaipainen. Positive but skeptical - A study of attitudes towards Internet voting in Sweden. In Peter Parycek, Michael Sachs, and Marko M. Skoric, editors, *Proceedings of the International Conference for E-Democracy and Open Government (CeDEM Asia)*, pages 191–205. Edition Donau-Universität Krems, 2014.

[5] **Jurlind Budurushi**, Karen Renaud, Melanie Volkamer, and Marcel Woide. Implementation and Evaluation of the EasyVote Tallying Component and Ballot. In Robert Krimmer and Melanie Volkamer, editors, *6th International Conference on Electronic Voting (EVOTE)*, pages 1–8. IEEE, 2014. Cited on page 63.

[6] **Jurlind Budurushi**, Stephan Neumann, Genc Shala, and Melanie Volkamer. Entwicklung eines Common Criteria Schutzprofils für elektronische Wahlgeräte mit Paper Audit Trail. In Erhard Plödereder, Lars Grunske, Eric Schneider, and Dominik Ull, editors, *INF14 - Workshop: Elektronische Wahlen: Unterstützung der Wahlprozesse mittels Technik*, volume 232 of *Lecture Notes in Informatics*, pages 1415–1426. Köllen Druck+Verlag GmbH, Bonn, 2014.

[7] **Jurlind Budurushi**, Simon Stockhardt, Marcel Woide, and Melanie Volkamer. Paper Audit Trails and Voters' Privacy Concerns. In Theo Tryfonas and Ioannis Askoxylakis, editors, *Human Aspects of Information Security, Privacy and Trust*, volume 8533 of *Lecture Notes in Informatics*, pages 400–409. Springer International Publishing Switzerland, 2014. Cited on page 47.

[8] **Jurlind Budurushi** and Melanie Volkamer. Feasibility Analysis of Various Electronic Voting Systems for Complex Elections. In Peter Parycek and Noella Edelmann, editors, *Proceedings of the International Conference for E-Democracy and Open Government (CeDEM)*, pages 141–152. Edition Donau-Universität Krems, 2014.

[9] **Jurlind Budurushi**, Roman Jöris, and Melanie Volkamer. Implementing and evaluating a software-independent voting system for polling station elections. *Journal of Information Security and Applications*, 19(2):1–10, 2014. Cited on page 47.

[10] Maria Henning, **Jurlind Budurushi**, and Melanie Volkamer. Elektronsiche Wahlen durch Stimmzettelbelege? Untersuchung möglicher Umsetzungen des Öffentlichkeitsgrundsatzes bei elektronischen Wahlen. *MultiMedia und Recht (MMR)*, pages 154–158, 2014.

[11] **Jurlind Budurushi**, Marcel Woide, and Melanie Volkamer. Introducing Precautionary Behavior by Temporal Diversion of Voter Attention from Casting to Verifying their Vote. In *Workshop on Usable Security (USEC)*. Internet Society, 2014. Cited on page 73.

[12] Stephan Neumann, **Jurlind Budurushi**, and Melanie Volkamer. Analysis of Security and Cryptographic Approaches to Provide Secret and Verifiable Electronic Voting. In Dimitrios Zissis and Dimitrios Lekkas, editors, *Design, Development, and Use of Secure Electronic Voting Systems*, chapter 2, pages 27–61. IGI Global, 2014.

[13] Kristoffer Braun, **Jurlind Budurushi**, and Melanie Volkamer. Machbarkeitsanalyse der UniWahl4 Software für Wahlen an der TU Darmstadt. In Matthias Horbach, editor, *INF13 - Workshop: Elektronische Wahlen: Ich sehe was, das Du nicht siehst - öffentliche und geheime Wahl*, volume 220 of *Lecture Notes in Informatics*, pages 752–766. Gesellschaft für Informatik, 2013.

[14] **Jurlind Budurushi**, Stephan Neumann, Maina Olembo, and Melanie Volkamer. Pretty Understandable Democracy - A Secure and Understandable Internet Voting Scheme. In *8th International Conference on Availability, Reliability and Security (ARES)*, pages 198–207. IEEE, 2013.

[15] **Jurlind Budurushi**, Maria Henning, and Melanie Volkamer. Vote Casting in Any Preferred Constituency: A New Voting Channel. In James Heather, Steve A. Schneider, and Vanessa Teague, editors, *4th International Conference on e-Voting and Identity (VoteID)*, volume 7985 of *Lecture Notes in Computer Science*, pages 61–75. Springer, 2013.

[16] **Jurlind Budurushi**, Maria Henning, and Melanie Volkamer. Wählen in beliebigen Wahlbezirken: Ein neuer Wahlkanal. In Erich Schweighofer, Franz Kummer, and Walter Hötzendorfer, editors, *Abstraction and Application: Proceedings of the 16th International Legal Informatics Symposium (IRIS)*, pages 249–256. Austrian Computer Society, 2013.

[17] Maria Henning, Melanie Volkamer, and **Jurlind Budurushi**. Elektronische Kandidatenauswahl und automatisierte Stimmermittlung am Beispiel hessischer Kommunalwahlen. *Die Öffentliche Verwaltung (DÖV)*, (20):789–796, 2012. Cited on page 115.

[18] **Jurlind Budurushi**, Stephan Neumann, and Melanie Volkamer. Smart Cards in Electronic Voting - Lessons learned from applications in legally binding elections and approaches proposed in scientific papers. In Manuel J. Kripp, Melanie Volkamer, and Rüdiger Grimm, editors, *5th International Conference on Electronic Voting (EVOTE)*, volume 205 of *Lecture Notes in Informatics*, pages 257–270. Gesellschaft für Informatik, 2012.

[19] Melanie Volkamer, **Jurlind Budurushi**, and Denise Demirel. Vote casting device with VV-SV-PAT for elections with complicated ballot papers. In *International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE)*, pages 1–8. IEEE, 2011.

[20] Richard Frankland, Denise Demirel, **Jurlind Budurushi**, and Melanie Volkamer. Side-channels and eVoting machine security: Identifying vulnerabilities and defining requirements. In *International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE)*, pages 37–46. IEEE, 2011.

List of Figures

List of Tables

Acknowledgements

I praise God for enlightening my life path since the day of my birth by blessing me with two inextinguishable pharos, my parents Afërdita and Llambi Budurushi to whom I dedicate this dissertation.

First and foremost, I want to thank my supervisors Melanie Volkamer and Karen Renaud for their professional and respectful relation with me, especially for reading and providing valuable feedback for this dissertation. I wish to express my deep gratitude to Melanie Volkamer for her commitment, patience, ideas, time, financial support and in particular for believing in me. Her enthusiasm for research and her extraordinary hard-worker genes were contagious and motivational for me, even during tough times in the PhD achievement. She has been a good friend and a great mentor in teaching me how to conduct research. I am very grateful to Karen Renaud for her continuous support, advises and helpful comments on my work. I am also very honoured to have Johannes Buchmann, Marc Fischlin and Joachim Vogt on my PhD committee.

At this point, I wish to express my sincere thanks to my colleagues from SECUSO and CDC, in particular to Stephan Neumann, and my co-authors, especially to Marcel Woide. I want to thank my brothers Gert and Kostandin Budurushi, and their families for their love, respect, kindness, encouragement and support. I also want to thank all the wonderful people who have shared their time, love and knowledge with me. You all have been a source of inspiration to me.

Abstract

Elections differ not only between, but also within, countries. Some elections have very simple voting rules and ballots. For instance, in the parliamentary elections in Estonia or Germany, voters can select *1-out-of-n* candidates. Other elections, like parliamentary elections in Luxembourg and Belgium or local elections in Germany, have very complex voting rules and huge ballots. These elections combine different voting rules, namely select *k-out-of-n*, *weight* and *rank* candidates, and therefore pose a challenge to both voters and electoral officials. Hence, in such elections voters are likely to spoil their vote unintentionally, due to the complex voting rules. In addition, the tallying process is very time intensive and likely to be error prone, because of the combination of complex voting rules and huge ballots.

In order to address such challenges and improve the situation for both voters and electoral officials, in particular with respect to the local elections in Hesse/Germany, the EasyVote electronic voting scheme was proposed. EasyVote focuses on polling station elections and its central idea is to use an electronic voting device that does not store votes, but rather prints out a summary of voter's selections on a DIN-A4 paper ballot (a paper audit trail). The ballot consists of a human- and a machine-readable (a QR-Code) component. Further, electoral officials tally the ballots semi-automatically by scanning the QR-Code of each ballot and verifying that its content matches the human-readable component. However, before EasyVote can be used in legally binding elections, various open research questions need to be addressed.

The goal of this dissertation is to pave the way for the use of EasyVote in legally binding elections. To achieve this goal, this dissertation addresses five open research questions, which are introduced below. While the second and fifth question are EasyVote specific, the remaining ones are relevant to all electronic voting schemes/systems that share similar concepts with EasyVote.

1. Are voters concerned about vote secrecy related to the use of QR-Codes and, if so, how to address such concerns effectively?
2. What is an optimal ballot design that enables voters to understand the impact of their selections and to verify their voting intention easily?
3. What are optimal verification instructions that make voters most likely to verify that their ballot matches their intention?
4. What is an optimal verification setting that makes electoral officials most likely to detect potential discrepancies between the human- and machine-readable ballot components?
5. Are the vote casting and tallying processes usable and, if not, how to improve their usability?

The findings indicate that voters do have secrecy concerns in association with the use of QR-Codes. However, the findings suggest that the threat appraisal approach of the protection motivation theory, is a viable approach to address and significantly allay such concerns. Furthermore, the findings reveal that the ballot design, which highlights the voter's direct selections in orange, represents an optimal design for voters to understand the impact of their selections and to verify their intention easily. In addition, the findings show that *just in time* verification instructions, which are pre-printed on the reverse of the ballot, have a significant effect on voters with respect to verifying their ballot and detecting discrepancies. The findings also indicate a significant increase with respect to detecting discrepancies when electoral officials read voters' direct selections out loud, while verifying that the human-readable ballot component matches the associated QR-Code. Moreover, the findings suggest that the implemented EasyVote prototype has a high perceived usability. In summary, these findings reveal that EasyVote is likely to be recommended and that a malicious or faulty behaviour of an electronic voting device, which might violate the integrity of the election result, would be detected with very high probability.

Zusammenfassung

Wahlen unterscheiden sich nicht nur zwischen, sondern auch innerhalb einzelner Länder. Einige Wahlen haben sehr einfache Abstimmungsregeln und Stimmzettel. Bei Parlamentswahlen in Estland oder in Deutschland können Wähler zum Beispiel *1-aus-n* Kandidaten wählen. Andere Wahlen, wie die Parlamentswahlen in Luxemburg und Belgien oder die Kommunalwahlen in Deutschland, haben sehr komplexe Abstimmungsregeln und große Stimmzettel. Da diese Wahlen verschiedene Abstimmungsregeln kombinieren wie *k-aus-n* Kandidaten wählen (Panaschieren), *Stimmengewichtung* (Kumulieren) und *Vorzugswahl* (den Rang der Kandidaten beeinflussen), stellen diese Wahlen sowohl für Wähler als auch für Wahlhelfer eine Herausforderung dar. Aufgrund der komplexen Abstimmungsregeln ist es wahrscheinlich, dass die Wähler in solchen Wahlen unabsichtlich ungültige Stimmen abgeben. Darüber hinaus ist die Auszählung der abgegebenen Stimmen aufgrund der Kombination von komplexen Abstimmungsregeln und den großen Stimmzetteln überaus zeitintensiv und mit hoher Wahrscheinlichkeit fehleranfällig.

Um solchen Herausforderungen wirksam zu begegnen und die Situation sowohl für Wähler als auch für Wahlhelfer zu verbessern, insbesondere in Bezug auf die Kommunalwahlen in Hessen/Deutschland, wurde EasyVote als Konzept eines hybriden (elektronisch/Papier) Wahlsystems vorgeschlagen. Der Fokus von EasyVote liegt auf Wahlen im Wahlbezirk. Die zentrale Idee von EasyVote besteht in der Anwendung eines elektronischen Abstimmungsgeräts, welches keine elektronischen Stimmen speichert, sondern eine Zusammenfassung der Stimmabgabe auf DIN-A4-Papier (einem sogenannten "Paper Audit Trail") ausdruckt. Der Ausdruck (Stimmzettel) besteht sowohl aus einer menschlich lesbaren als auch einer maschinenlesbaren (QR-Code) Komponente. Innerhalb des Auszählungsprozesses werden die Stimmzettel, d.h. die abgegebenen Stimmen, halbautomatisch gezählt. Dabei scannen Wahlhelfer den QR-Code jedes einzelnen Stimmzettels ein und überprüfen, ob dessen Inhalt mit dem Inhalt der menschlich lesbaren Komponente übereinstimmt. Bevor EasyVote jedoch in rechtsverbindlichen Wahlen verwendet werden kann, müssen diverse Forschungsfragen adressiert werden.

Das Ziel dieser Dissertation ist es, den Weg für den Einsatz von EasyVote in rechtsverbindlichen Wahlen zu ebnen. Um dieses Ziel zu erreichen, befasst sich diese Dissertation mit fünf offenen Forschungsfragen, die im Folgenden vorgestellt werden. Während die zweite und die fünfte Frage EasyVote spezifisch sind, sind die restlichen Fragen für alle Wahlsysteme relevant, welche auf ähnlichen Konzepten wie EasyVote aufbauen.

1. Sind Wähler über ihr Wahlgeheimnis in Zusammenhang mit der Verwendung von QR-Codes besorgt und, wenn ja, wie können solche Sorgen effektiv adressiert werden?

2. Wie sieht ein optimales Stimmzetteldesign aus, das den Wählern die Nachvollziehbarkeit der Auswirkung und eine leichte Überprüfbarkeit ihrer Stimmabgabe ermöglicht?

3. Wie sehen optimale Anweisungen zur Stimmzettelüberprüfung aus, die höchstwahrscheinlich sicherstellen, dass Wähler überprüfen, ob ihr Stimmzettel ihrer Wahlintention entspricht?

4. Welche Methode zur Stimmzettelüberprüfung stellt am besten sicher, dass Wahlhelfer mögliche Diskrepanzen zwischen den menschlich- und maschinenlesbaren Stimmzettelkomponenten feststellen?

5. Sind die Prozesse der Stimmabgabe und Auszählung benutzbar und wenn nicht, wie kann die Benutzbarkeit dieser Prozesse verbessert werden?

Die Ergebnisse zeigen Bedenken der Wähler bezüglich ihres Wahlgeheimnisses in Zusammenhang mit dem Einsatz von QR-Codes. Allerdings zeigen die Ergebnisse auch, dass der Ansatz der Schutzmotivationstheorie zur Einschätzung der Bedrohung ein angemessener Ansatz ist, um solche Bedenken signifikant zu verringern. Darüber hinaus zeigen die Ergebnisse, dass ein optimales Stimmzetteldesign bezüglich der Nachvollziehbarkeit und Überprüfbarkeit der Stimmabgabe erreicht werden kann, indem die direkt vergebenen Stimmen in Orange hervorgehoben werden. Die Ergebnisse zeigen auch, dass Anweisungen zur Stimmzettelüberprüfung, die auf der Rückseite des Stimmzettels vorgedruckt sind und den Wählern zum richtigen Zeitpunkt gegeben werden, einen signifikanten Einfluss darauf haben, ob Wähler ihren Stimmzettel überprüfen und Diskrepanzen zu ihrer Wahlintention feststellen. Zusätzlich zeigen die Ergebnisse eine signifikante Steigerung der erfolgreichen Feststellung von Diskrepanzen zwischen der menschlich lesbaren Stimmzettelkomponente und dem

QR-Code, wenn Wahlhelfer während der Auszählung die direkt vergebenen Stimmen laut vorlesen. Außerdem belegen die Ergebnisse eine hohe wahrgenommene Benutzerfreundlichkeit des implementierten EasyVote Prototypen. Zusammenfassend zeigen diese Ergebnisse, dass der Einsatz von EasyVote zu empfehlen ist, und dass ein böswilliges oder fehlerhaftes Verhalten eines Abstimmungsgeräts, welches die Integrität des Wahlergebnisses verletzen könnte, mit sehr hoher Wahrscheinlichkeit festgestellt wird.

Contents

1 Introduction

The saying *different countries, different customs* also holds true for elections. Elections can be very different between, and even within, countries. Some elections, like parliamentary elections in Estonia or Germany have very simple voting rules and ballots. In such elections voters can select *1-out-of-n* candidates. Other elections, like parliamentary elections in Luxembourg and Belgium or local elections in Germany, have very complex voting rules and huge ballots. These elections combine different voting rules, namely select *k-out-of-n*, *weight* and *rank* candidates, and therefore pose a challenge to both voters and electoral officials. One very important challenge is that voters are likely to spoil their vote unintentionally, due to the complex voting rules. For instance, the number of invalid votes at the last local elections in the city of Darmstadt (Hesse/Germany) in 2011 (5.5%[1]), was almost twice as high compared to the last German federal elections in 2013 (on average 2.8%[2]). Another important challenge is that the tallying process is very time intensive and likely to be error prone, because of the combination of complex voting rules and huge ballots. For instance, the last local elections in Darmstadt in 2011 took place on the 27th of March and results were only published on April 6[3], even though the tallying process is (partially) electronically supported, namely by the PC-Wahl[4] software.

In order to address these challenges and improve the situation for both voters and electoral officials, in particular with respect to the local elections in Hesse, Volkamer *et al.* [VBD11] proposed the EasyVote electronic voting scheme. EasyVote, which is examined in more detail in chapter 5, focuses on polling station elections and can be briefly described as follows: In the vote casting process voters use an electronic voting device to select their preferred candidates/parties. The device supports voters regarding the validity of their selections. When voters confirm their

[1]`http://www.statistik-hessen.de/K2011/EK1.htm`, last accessed February, 7, 2016.
[2]`http://www.bundeswahlleiter.de/en/bundestagswahlen/BTW_BUND_13/ergebnisse/landesergebnisse/l06/`, last accessed February, 7, 2016.
[3]`http://www.statistik-hessen.de/K2011/EG411000.pdf`, last accessed February, 7, 2016.
[4]`http://www.pcwahl.de/`, last accessed February, 7, 2016.

selections, a ballot, or so-called paper audit trail, is printed and no electronic data are retained. The printed ballot contains a summary of voters' selections and consists of a human- and a machine-readable (a QR-Code as proposed in [Int15]) component. Voters are supposed to verify that the human-readable ballot component reflects their intention. Finally, voters exit the voting booth and deposit their ballot into the ballot box. During the tallying process electoral officials tally the ballots semi-automatically by scanning the QR-Codes. Electoral officials scan the QR-Code of each ballot and are supposed to verify that its content matches the human-readable ballot component. When electoral officials confirm that, the scanned ballot is added to the intermediate result. Electoral officials repeat this process for all ballots. The election result is computed after all ballots are tallied.

However, before EasyVote can be used in legally binding elections, various open research questions need to be addressed. The goal of this dissertation is to pave the way for the use of EasyVote in legally binding elections. To achieve this goal, we identify, define and address five open research questions:

1. "Are voters concerned about vote secrecy related to the use of QR-Codes and, if so, how to address such concerns effectively?"
   This research question is motivated by the findings of Gerber *et al.* [GHDD13] and Llewellyn *et al.* [LSX+13]. These findings reveal that voters might abstain from the election [GHDD13] or alter their voting behaviour [LSX+13], if they believe that the electronic voting system endangers their vote secrecy. Further, Llewellyn *et al.* [LSX+13] reports that voters show doubts, i.e. have secrecy concerns, when their ballot contains information additional to their selections. Last, but not least, secrecy concerns regarding barcodes are also mentioned in [NSN06]. We address this research question, which to the best of our knowledge has not been addressed previously, in chapter 7.

2. "What is an optimal ballot design that enables voters to understand the impact of their selections and to verify their voting intention easily?"
   The motivation of this research question is twofold. One the one hand it is driven by the challenge stated in the EasyVote proposal [VBD11], namely how to design the ballot in such a way that it is understandable for the voters, i.e. that voters understand the impact of their selections (how their cast votes are tallied). On the other hand Henning *et al.* [HBV14] states that the mere existence of the option to verify is not sufficient. It is also necessary that the option to verify is made usable, i.e. that voters can verify their cast votes easily. We address this research question, which to the best of our knowledge has been only partially addressed by Jöris [Jör13], in chapter 8.

3. "What are optimal verification instructions that make voters most likely to verify that their ballot matches their intention?"
   Similar to other electronic voting schemes/systems that provide voters with paper audit trails (printed ballots), for instance [BCH+12, BFL+12, Veg12, BBE+13, Boa14, Vot08], EasyVote assumes that voters will verify that their ballot matches their voting intention. However, various research studies, namely [Sel04, Coh05, HNH+05, HNH+06a, mar06, SP06] have investigated this assumption, and report that the number of voters that actually verify their ballot is very low. We address this research question, which is motivated by the results of previous studies, in chapter 9.

4. "What is an optimal verification setting that makes electoral officials most likely to detect potential discrepancies between the human- and machine-readable ballot components?"
   While they tally the election results, electoral officials are required to verify that the human-readable ballot component matches the content stored in and scanned from the QR-Code. Thereby, the accuracy of the tallying process, i.e. election integrity, relies on human (electoral officials) attention. However, studies from other research areas, such as airport baggage screening [WHK05, MM10] or cancer screening [GSR+04], report that human attention is notoriously unreliable. Hence, these results motivate our fourth research question. We address this question, which to the best of our knowledge has not been addressed previously, in chapter 10.

5. "Are the vote casting and tallying processes usable and, if not, how to improve their usability?"
   When a new electronic voting scheme/system is proposed, usually the research focus is its security, for instance vote secrecy (the first research question), and election integrity (the third and fourth research questions). Nevertheless, usability represents another important aspect of electronic voting that we should not ignore. Usability is as important as security, because to ensure election integrity, voters must actually be able to cast their votes as intended. One of the most discussed examples of the impact of poor usability on election integrity, is the so-called *butterfly ballot* in the 2000 election in Florida. This and many other unfortunate experiences of poor usability motivate our last research question. We address this question in chapter 9 for the vote casting process and in chapter 10 for the tallying process. To the best of our knowledge, this question has not been previously addressed in the context of complex elections.

While the second and fifth question are EasyVote specific, the remaining ones are relevant to all electronic voting schemes/systems that share similar concepts with EasyVote, like the Wombat voting system [BFL+12], the Belgian voting system [Veg12], the STAR-Vote voting system [BBE+13], and the Vot.ar voting system [Vot08]. Note that other research questions, like how to improve vote secrecy with respect to side-channel attacks (electromagnetic emissions [VE85], tempest [Fri72] and differential power analysis [KJJ99]), or how EasyVote performs with respect to technical [Vol09, SVB10, WBB+15] and legal [HVB12, SDNK+13, BNSV14] evaluation approaches, are also important and necessary to address. However, they are out of the scope of this dissertation.

2 Related work

This chapter describes related work. We first introduce the methodology applied to identify and determine related research. Afterwards, we describe and discuss related research.

To identify and determine related research, we conducted a structured literature search based on the approaches proposed by Brocke *et al.* [vBSN+09] and Webster and Watson [WW02]. According to Brocke *et al.* [vBSN+09] a rigorous literature search must be valid and reliable. The validity of our search process is based on the following factors:

- Selected databases, keywords and inclusion and exclusion criteria.
- Covered period.
- Applied forward and backward search.

Further, reliability is based on the fully documented search process.

Databases: We searched through the following databases: ACM, DBLP, IEEEX-Plore, ScienceDirect and SpringerLink.

Key words: We used the following keywords for our search: *usable security*, *evaluation*, *electronic voting*,*e-voting*, *paper audit trails*, *complex elections* and *complicated elections*.

Inclusion criteria: As electronic voting is a relatively young research area we chose to not only focus on high-quality literature, as recommended in [vBSN+09] and [WW02], but we also included journals, conferences and workshops that are not highly rated in international rankings. Furthermore, as electronic voting is also highly applied we included vendors' systems.

Exclusion criteria: We decided to exclude non-academic publications, such as technical reports or white papers. We filtered out publications that were not written in English and those published before the year 2000. Furthermore, we filtered out electronic voting schemes/systems that are not proposed for use in polling station elections. Finally, we filtered out publications, which are included in and considered as contributions of this dissertation.

Forward search: We used Google Scholar[5] citation index service to perform a forward search.

Backward search: In contrast to the forward search, the backward search was conducted manually.

For the search we used key word combinations, which we classify under the following literature categories:

1. Usable security evaluation of electronic voting with paper audit trails in the context of complex elections.
   - *usable security*, *evaluation*, *electronic voting*, *paper audit trails* and *complex elections*
   - *usable security*, *evaluation*, *electronic voting*, *paper audit trails* and *complicated elections*
   - *usable security*, *evaluation*, *e-voting*, *paper audit trails* and *complex elections*
   - *usable security*, *evaluation*, *e-voting*, *paper audit trails* and *complicated elections*
2. Usable security evaluation of electronic voting with paper audit trails.
   - *usable security*, *evaluation*, *electronic voting* and *paper audit trails*
   - *usable security*, *evaluation*, *e-voting* and *paper audit trails*
3. Usable security evaluation of electronic voting.
   - *usable security*, *evaluation* and *electronic voting*
   - *usable security evaluation* and *e-voting*
4. Electronic voting in the context of complex elections.
   - *electronic voting* and *complex elections*
   - *electronic voting* and *complicated elections*

[5] `https://scholar.google.de/`, last accessed February, 7, 2016.

- *e-voting* and *complex elections*
- *e-voting* and *complicated elections*

We conducted a full-text search, and the databases were searched to identify publications that contained at least one of the above combinations. In total, 2839 potentially relevant publications were identified. Afterwards, we applied the defined inclusion and exclusion criteria, by manually screening publications based on title, abstract and, if necessary, by skimming through the full text. Following this process only 11 publications were determined to be relevant. Finally, we performed the forward and backward search. As a result, 58 additional publications were identified as relevant. Table 2.1 shows the number of publications for each journal, conference or workshop that were identified as relevant.

In the following we discuss related research according to the categories defined in the literature search. Note that for a more general overview with respect to usability studies in the context of electronic voting (including Internet voting), we refer the reader to [OV13].

Usable security evaluation of electronic voting with paper audit trails in the context of complex elections

To the best of our knowledge, no previous work has evaluated electronic voting with paper audit trails in the context of complex elections from a usable security perspective.

Usable security evaluation of electronic voting with paper audit trails

For this category we identified the following relevant publications: [Coh05, SP06, GB07, GBG+08, JHG08, BKA15].

Similar to this dissertation, however in the context of simple elections, these publications, namely [Coh05, SP06], investigated whether voters act to verify that their paper audit trail (ballot) matches their voting intention. In the study conducted by Cohen [Coh05] participants were required to follow a voting agenda, i.e. to vote for a pre-defined list of specific candidate(s) and/or a specific party. While instructions regarding the use of the voting system were given in the voting booth, instructions regarding ballot verification were displayed on the final screen of the voting device. The results revealed that only two out of 36 participants actually verified and detected the deliberately, introduced manipulations: (1) Changing a vote to a different candidate; (2) Removing a vote from a candidate; and (3) Removing a complete contest. Furthermore, Selker and Pandolfo [SP06] report that only six out

Table 2.1: Related work: Number of relevant publications per journal, conference and workshop.

	Count
Journal	
Election Technology and Systems	4
Usability Studies	3
Information Forensics and Security	2
Student Journal of Public Policy Research	2
Social Science Computer Review	1
Midwest Political Science Association	1
American Politics Research	1
Electoral Studies	1
Human-Computer Studies	1
Electronic Governance	1
Information Technology & Politics	1
Political Behaviour	1
Interactions	1
Political Science Research and Methods	1
Information Design	1
Information Systems and Social Change	1
Conference	
E-Voting and Identity	5
Electronic Voting	4
Human-Computer Interaction	2
E-Democracy and Open Government	2
Special Interest Group on Computer-Human Interaction	1
Theory and Practice of Electronic Governance	1
Human Factors and Ergonomics Society	1
IEEE Security & Privacy	1
Advances in Cryptology	1
Interfaces and Human Computer Interaction	1
Workshop	
Electronic Voting Technology Workshop	13
Requirements Engineering for Electronic Voting Systems	2
Usability and Security of Electronic Voting System	1
Privacy in Electronic Society	1
e-Voting and e-Government in the UK	1
*Others**	9

* Note that this category includes books, PhD and master theses, and vendors' electronic voting systems.

of 35 participants actually verified and detected the manipulations on their ballot. The manipulations were introduced deliberately and similar to those used by Cohen [Coh05]. In the study, participants were required to cast a vote in 13 contests. While the list of candidates was pre-defined for nine of the contests, participants could chose their preferred candidates in the remaining ones. Further, participants were given verbal instructions with respect to ballot verification and the use of the voting system outside the voting booth.

The rest of the publications focused on other aspects. For instance, Goggin *et al.* [GB07] examined the speed and accuracy of hand recounts of paper audit trails. In addition, Goggin *et al.* [GBG+08] compared the speed and accuracy of hand recounts of paper audit trails with respect to other auditing technologies, e.g. video audit trails. Further, De Jong *et al.* [JHG08] examined voters' perceptions of vote secrecy and user-friendliness regarding paper audit trails. Finally, Belton *et al.* [BKA15] examined the usability of two different ballot box configurations with respect to reducing errors, which result from voters that fail to scan, or place, their ballot into the ballot box.

Usable security evaluation of electronic voting

For this category we identified the following relevant publications: [CLP+06, HNH+06b, SGH+06, Eve07, JHG07, BHMQ+08, EGB+08b, EGB+08a, Gre08, Gog08, HNH+08, AKLM09, CEP09, CB09, CBL+09, OdB09, WBP+09, AKP11, KAC+11, SLC+11, GMR+12, MGO12, AKP13, AILL13, Cam13, GDOS13, LSX+13, AKBW14, HCB15, PLA+14, AKBW15, Lee15].

Similar to this dissertation, however in the context of simple elections and electronic voting without paper audit trails, these publications, namely [Eve07, CB09, GMR+12, AKP13, GDOS13], investigated whether voters act to verify that the review screen matches their voting intention. In the studies conducted by Everett [Eve07] two conditions were used: (1) Participants were required to follow a voting agenda, i.e. to vote for a pre-defined list of specific candidate(s) and/or a specific party; and (2) Participants were required to make their own selections. Further, two different manipulations, one in each study, were used: (1) Adding/removing contests to/from the review screen; and (2) Vote flipping. Last, but not least, fictitious candidates and parties were used. The results revealed that more than 60% of the participants in each study (66 participants in the first, and 101 in the second study), independent of the condition, did not notice (on the review screen) that their selections were altered. All the other studies, namely [CB09, GMR+12, AKP13, GDOS13] are replications of, and motivated by, the studies conducted by Everett [Eve07].

However, Acemyan *et al.* [AKP13] used real candidates/parties and required participant to cast a vote for issues of personal relevance. Furthermore, except Gilbert *et al.* [GDOS13], all studies report similar results to Everett [Eve07], i.e. a very low number of participants who noticed (on the review screen) that their selections were altered. Gilbert *et al.* [GDOS13] report a detection rate of 90%, even without informing participants on the importance of verifying the review screen. Even though the results reported by Gilbert *et al.* [GDOS13] seem very promising, they are not significant with respect to ensuring the integrity of cast votes or election result. A malicious or faulty electronic device, which does not provide an independent verification mechanism for cast votes, e.g. paper audit trails, can alter voters' selections without being detected, while still showing voters their unaltered selections on the review screen.

The rest of the publications focused on other aspects, such as the usability evaluation of different electronic voting technologies [CLP+06, HNH+06b, SGH+06, JHG07, BHMQ+08, Gog08, HNH+08, CEP09, CBL+09, OdB09, WBP+09, KAC+11, SLC+11, MGO12, Cam13, AKBW14, HCB15, AKBW15, Lee15], the comparison between different electronic voting technologies and traditional voting methods (paper-based elections) [EGB+08b, EGB+08a, Gre08], or the implications and effect of voters' trust [AKLM09, AKP11, AILL13, PLA+14] and understanding [LSX+13] on the adoption of electronic voting.

Electronic voting in the context of complex elections

For this category we identified the following relevant publications, namely the Digital Voting Pen [AMBS07], EasyVote [VBD11] and the Belgian voting system [Veg12]. These publications propose electronic voting schemes/systems that are designed for complex elections, similar to the local elections in the city of Darmstadt, see section 4. In the following we outline the differences between these proposals.

For an overview regarding EasyVote [VBD11], we refer the reader to chapter 5. In contrast to EasyVote, when using the Digital Voting Pen [AMBS07], voters cast their vote on a paper ballot by using a pen. Both the pen and the ballot are based on the *Anoto Technology*[6]. After selecting the preferred candidates and/or parties, voters exit the voting booth, and stick their pen into a docking station to register their electronic vote. When the vote is registered, voters deposit their paper ballot into the ballot box. Furthermore, the election results is computed by using the electronic registered votes, while the marked paper ballots can be used for random audits. Note that the main advantage of the Digital Voting Pen is that the vote

[6]http://www.anoto.com/, last accessed February, 7, 2016.

casting process remains almost unchanged as compared to the traditional paper-based elections. However, in the context of complex elections, this is rather the main disadvantage, because voters are not given any feedback with respect to the validity of their cast vote.

In contrast to EasyVote, when using the Belgian voting system [Veg12], voters enable the voting device in the voting booth by using a token (smartcard). Similar to EasyVote, after selecting the preferred candidates and/or parties, the voting device prints a ballot. The printed ballot, as in EasyVote, consists of a human- and a machine-readable (a QR-Code) component. However, as opposed to EasyVote, the QR-Code encodes the encryption of the voters' selections. Afterwards, voters exit the voting booth, scan the QR-Code to register their electronic vote, and deposit their ballot into the ballot box. Furthermore, the election result is computed by using the electronic registered votes, while the printed ballots can be used for random audits. The Belgian voting system and EasyVote are very similar, however the Belgian voting systems has two disadvantages: (1) QR-Codes are unique. This, in contrast to EasyVote, facilitates well-know attacks, like vote buying and voter coercion [JCJ05]; and (2) Tokens are used to enable the voting device. This, as opposed to EasyVote, facilitates well-known attacks, like chain voting [Jon05], or might cause confusion and long queues at the polling stations, in case voters lose their tokens.

Part I.

Fundamentals

3 Usable security

The research questions, which are addressed in this dissertation and listed below, combine human factors (usability) and technical aspects (security) in the context of electronic voting. By following a human-centred security approach, these questions aim to align usability and security. Thus, these questions can be considered as usable security research questions in the context of electronic voting. Therefore, in the first part of this chapter we provide a brief overview of usable security in general. For more detailed information regarding usable security we refer the reader to [Yee04, PE08, Kas14]. In the second part we emphasise the importance of usable security in the context of electronic voting and introduce a standard methodology for assessing usability.

1. Are voters concerned about vote secrecy related to the use of QR-Codes and, if so, how to address such concerns effectively?
2. What is an optimal ballot design that enables voters to understand the impact of their selections and to verify their voting intention easily?
3. What are optimal verification instructions that make voters most likely to verify that their ballot matches their intention?
4. What is an optimal verifiability setting that makes electoral officials most likely to detect potential discrepancies between the human- and machine-readable ballot components?
5. Are the vote casting and tallying processes usable and, if not, how to improve their usability?

3.1. General overview

In 1975, Jerome Saltzer and Michale Schroeder [SS75] were the first to acknowledge the importance and impact of usability regarding the security and acceptance of human-computer interactive systems. Nevertheless, usability has played a limited role in the development of secure systems and security research, because security experts either did not acknowledge its importance or lacked the expertise to consider and address potential usability issues [CG05]. For instance, the famous hacker, Kevin Mitnick, revealed that '...it was easier to dupe people into revealing their password by employing various social engineering techniques, rather than to crack the password.' [SF05]. Usually, such security failures are attributed to users' negligence and lack of education, while the term "stupid user" was often used, typically muttered *sotto voce*, by security experts [VR13].

Fortunately, longer than a decade, the research community has agreed that, for a system to be secure, it must be usable, i.e. we need to design secure systems that people can actually use. Ever since, the usable security community has done a lot to align usability and security, for instance by developing user interfaces for raising security awareness [SMN+13] or for effective anti-phishing software [GHJV94], or implementing Android apps [Bur09] that aim to educate users to spot phishing URLs [CVBB14, CVB+15].

While user authentication is one of the oldest and most researched topics in usable security [Swa12], other researchers have proposed guidelines on how to design secure and usable interactive systems [CG05, HA14], and how to integrate usability into the requirements and design process [FMS07]. Consequently, nowadays usability and security go hand in hand [CB14].

3.2. Usable security in electronic voting

The necessity to align usability and security also holds true for electronic voting. In the context of electronic voting, usability plays a key role with respect to security, namely election integrity. Election integrity can be ensured only if voters are able to cast their vote, and verify that their vote has been cast-as-intended, recorded-as-cast and tallied-as-stored.[7] In particular, in the context of electronic voting with paper audit trails, where voters play a key role in ensuring election integrity, usability becomes even more crucial, because '...security is only as good as it's weakest link, and people are the weakest link in the chain.' [Sch00]. One of the most famous real world examples, which revealed the importance and impact of usability on election integrity, is the so-called *butterfly ballot* in the 2000 election in Florida. The positioning of candidates and arrows caused a significant decrease in usability. This led many voters to make a selection other than their intended one. While the

[7]Refer to [OBV13] for the definition of verifiability in the context of electronic voting.

election in Florida is the most well-known example, there are many cases, refer to Norden *et al.* [NKQC08], where usability issues are likely to have influenced the outcome of an election, i.e. violated election integrity (the security of the system).

In addition, poor usability, i.e. if voters have to wait in long queues or if they are concerned regarding the use of the system [THhP$^+$05], can decrease voter turnout significantly. Hence, when considering electronic voting, usability represents a key aspect that we should not ignore. Therefore in the following, we introduce a standard methodology for assessing usability in the context of electronic voting. Note that we use this methodology throughout the studies reported in this dissertation.

Assessing usability in electronic voting

To assess usability in the context of electronic voting, the National Institute of Standards and Technology (NIST) recommends the use of the ISO 9241-11 standard [Int98]. According to ISO 9241-11, usability comprises the following three components that should be defined with respect to the context of use:

- **Effectiveness** (the ability of users to complete their task).
- **Efficiency** (the extent to which users consume resources to perform their task).
- **Satisfaction** (the level of satisfaction users experience in performing their task).

4 Complex elections: Local elections in Darmstadt

In this dissertation we focus on complex elections, namely the local elections in the city of Darmstadt, Hesse, Germany. The local elections in Darmstadt, similar to parliamentary elections in Luxembourg and Belgium, have very complex voting rules and huge ballots which challenge both voters and electoral officials. In these elections voters are likely to spoil their vote unintentionally. For instance, the number of invalid votes at the last local elections in Darmstadt in 2011 (5.5%[8]), was almost twice as high as at the last German federal elections in 2013 (on average 2.8%[9]). Furthermore, the tallying process is very time intensive and likely to be error prone, because of the combination of complex voting rules and huge ballots. For instance, the last local elections in Darmstadt in 2011 took place on the 27th of March and results were only published on April 6[10], even though the tallying process is (partially) electronically supported, namely by the PC-Wahl[11] software.

In order to improve this situation, Volkamer *et al.* [VBD11] proposed the EasyVote electronic voting scheme. EasyVote aims to address these challenges by supporting voters and electoral officials electronically, and at the same time by maintaining the vote casting and tallying process of the local elections in Darmstadt. Therefore, in this chapter we introduce and describe the steps[12] of these processes, which are adhered to the user studies reported in this dissertation. For that, we use the 2011 elections in Darmstadt as exemplary. Note that the vote casting and tallying

[8] `http://www.statistik-hessen.de/K2011/EK1.htm`, last accessed February, 7, 2016.

[9] `http://www.bundeswahlleiter.de/en/bundestagswahlen/BTW_BUND_13/ergebnisse/landesergebnisse/l06/`, last accessed February, 7, 2016.

[10] `http://www.statistik-hessen.de/K2011/EG411000.pdf`, last accessed February, 7, 2016.

[11] `http://www.pcwahl.de/`, last accessed February, 7, 2016.

[12] The exact steps and their respective rules of action can be found in more detail here, `https://www.darmstadt.de/fileadmin/Bilder-Rubriken/Rathaus/Politik/wahlen/PDF-Dateien/Kommunalwahlen/Leitfaden_fuer_Wahlvorstaende.pdf`, last accessed February, 7, 2016.

process are publicly open. This means that the general public (eligible voters, private individuals, nongovernmental organisations, media etc.) is allowed to observe and thereby verify the correctness of these processes. Nevertheless, to fulfil the principles of free and secret elections, the public observation is restricted, meaning that voters cast their vote secretly in the voting booth.

4.1. Vote casting process

Currently eligible voters receive an election notification. The notification informs them regarding their registration in the electoral register of the assigned polling station, and also serves as proof of identity. Hence, to participate in the election, i.e. to cast their vote, voters visit the polling station they are assigned to. Next, voters identify themselves to the electoral officials. To identify, voters either submit the election notification or use an official identification document, such as driver's license, passport or identity card. Note that according to the Federal Election Code the submission of the election notification or the identification document is not always necessary. For instance in case of personal acquaintance between voters and electoral officials it is not needed. When electoral officials confirm the voters' identity, voters are given a blank ballot and enter the voting booth. To cast their vote, voters use an ordinary pen to select (mark) their preferred candidates/parties. After voters have made their selections, they fold their ballot, exit the voting booth and deposit their ballot into the ballot box. Note that if voters want to change their selections, more specifically to not only correct them, they are required to proceed as follows:

1. Exit the voting booth.
2. Destroy the used ballot in front of the electoral officials, while keeping their selections secret.
3. Get a new blank ballot and reenter the voting booth.

Furthermore, in the vote casting process, voters are restricted by the following voting rules that are also printed on the top of the ballot:

- Voters can cast 71[13] direct votes.
- Voters can assign up to three votes to each candidate (cumulative voting).

[13]This number depends on the number of available seats, which also limits the number of candidates nominated by a party. The number of available seats depends on the size of the district.

- Voters can cast votes to candidates of different parties (vote splitting).
- Voters can select a party (mark a party header).
- Voters can cross out candidates.

If voters select a party, the remaining votes which are not cast directly are assigned to the candidates of the selected party according to the party's list order, automatically. By being able to cross out candidates voters can influence the automatic assignment of votes when a party is selected. Note that practically, the automatic assignment of votes takes place in the tallying process, in which electoral officials evaluate voters' selections. Hence, in the vote casting process voters can not have any certainty of the final allocation.

In addition, depending on the size of the district more than ten parties and more than 450 candidates are nominated for the elections, which results in huge ballots. The ballot of the local elections in Darmstadt, presented in Figure 4.1, consists of two components:

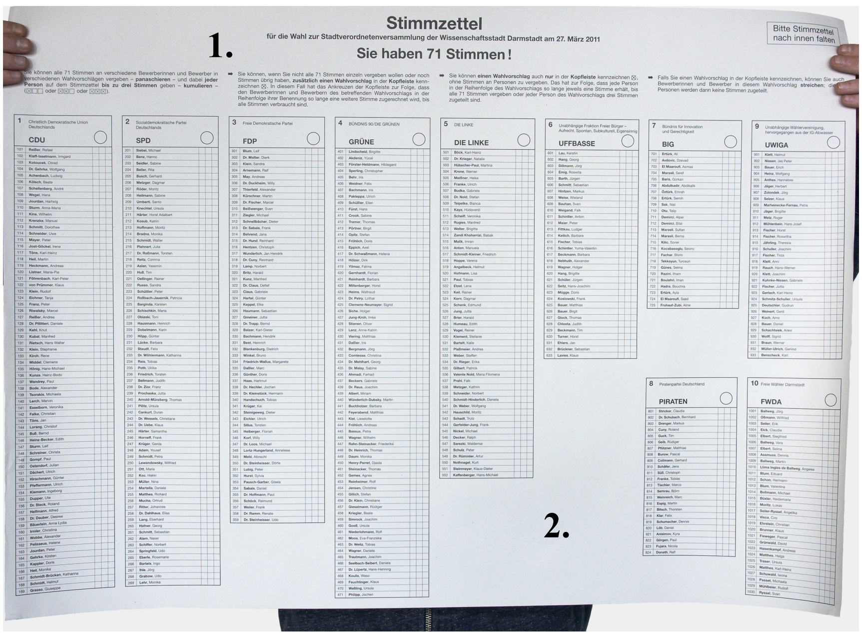

Figure 4.1: Complex elections: The ballot of the local elections in Darmstadt in 2011 (Size: 27" x 35").

1. The component on the top of the ballot. This component contains the description of the election, i.e. the election for which the ballot is cast, and the voting rules.

2. The component, which contains the nominated candidates and parties for the respective election. While the order of candidates is determined by the party, the order of parties is determined according to the results of the last election. Thus, in the last election the CDU party got the most votes, and therefore is listed on the first place.

Since the combination of complex voting rules and huge ballots undoubtedly leads to errors, so-called *healing rules* are applied during the tallying process:

- If a voter casts more than 3 direct votes to a candidate, only three votes are tallied.
- If a voter casts more than 71 direct votes for the candidates of one party, only 71 votes are tallied.
- If a voter selects more than one party and casts fewer than, or equal to, 71 direct votes, only the direct votes are tallied.

These healing rules aim to validate a ballot which might be interpreted as invalid according to the strict letter of the voting rules.

4.2. Tallying process

The tallying process consists of two phases carried out by the electoral officials. The first phase of the tallying process, which starts at the end of the election day and is monitored by an electoral officer, takes place in the respective polling stations. The electoral officials (approximately 9 volunteers) are required to perform the following sequential steps:

1. Open the ballot boxes and ensure that the number of cast ballots matches the number of voters marked off in the electoral register. If there is no match, electoral officials have to try to clarify the difference. This might require to repeat the entire count. If the error (mismatch) can not be determined, this is to be explained in the respective transcript record.

2. Classify ballots into four categories:

(1) Only a party is selected.

(2) Candidates are directly selected (and a party is selected).

(3) Invalid.

(4) Cannot be obviously assigned to any of the other categories.

3. Verify that ballots are correctly classified.
4. Manually tally the ballots of category **(1)** according to the selected party.
5. Review ballots of category **(4)** and assign them to the respective category **(1, 2 or 3)**.
6. Compute the intermediate result manually, by considering only the ballots of category **(1 and 3)**, including those from the fifth step.
7. Communicate by phone the intermediate result to the corresponding electoral registration office.
8. Fill in and sign the election transcript record.

The second phase, which starts the day after the election, takes place in publicly accessible offices of the respective municipality. In this phase, during which the ballots of category **(2)** are tallied, electoral officials are electronically supported by a tallying software, namely the PC-Wahl[14]. Figure 4.2 shows the PC-Wahl interface for entering the ballots (votes). Nevertheless, before this phase starts the electoral officer enters the intermediate result from the first phase into the PC-Wahl. Note that in practice the correctness of this step could be, but it is not, verified because the electoral officer is considered trustworthy.

In the second phase electoral officials (three municipality employees) have to perform the following sequential steps:

1. Enter the votes (voter's selections) of the first five ballots into PC-Wahl.
2. Manually tally the first five ballots.
3. Verify that the outcome of the 2nd and 3rd steps match.[15]
4. Enter the votes from the remaining ballots into PC-Wahl.

[14] `http://www.pcwahl.de/`, last accessed February, 7, 2016.

[15] The PC-Wahl software is assumed to be trustworthy. Thus, this step serves as a self-control for the electoral officials.

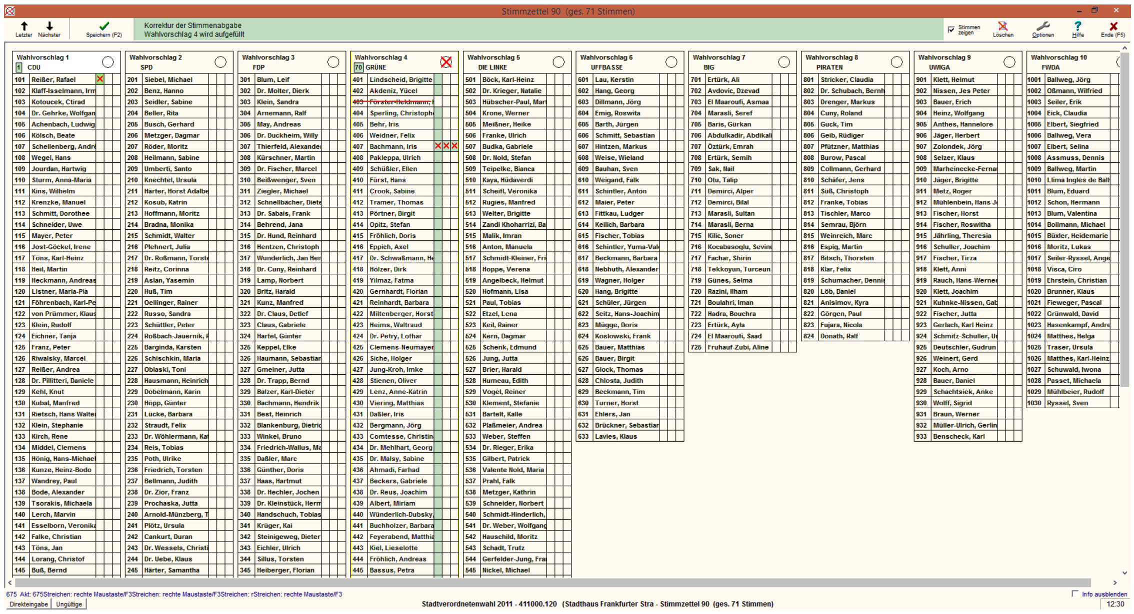

Figure 4.2: Complex elections: The interface of the PC-Wahl software for entering the votes.

5. Compute, with PC-Wahl, the final election result.

6. Sign the printed disposition.

The process of entering the votes into PC-Wahl is performed by three electoral officials. The first electoral official narrates the voter's selections on the ballot, the second enters them into the PC-Wahl, and the third observes and thereby verifies the correctness of this process. Note that for auditing purposes, electoral officials label (mark with an ordinary pen) ballots consecutively with the respective number of their digital representation (PC-Wahl entry).

Electoral officials who participate in the second phase are employees of the corresponding municipality and therefore are considered to be technically skilled. They participate in an introductory workshop regarding the PC-Wahl software. During the workshop, which usually lasts about 30 minutes, the electoral officials have the opportunity to try out the PC-Wahl software.

5 EasyVote

In this chapter we introduce EasyVote [VBD11], an hybrid (electronic/paper) voting scheme. In the first part of this chapter we outline the main goal and the general concept, focusing on the vote casting and tallying process, of EasyVote. In the second part we present the EasyVote prototype, which is used and incrementally improved in the user studies reported in this dissertation. Thereby, we focus on the ballot design and the interfaces for the vote casting and tallying process.

5.1. General concept

Complex elections, i.e. elections with complex voting rules and huge ballots, challenge both voters and electoral officials. Among many challenges, there are two very important ones:

- Voters are likely to spoil their vote unintentionally.
- The tallying process is very time intensive and likely to be error prone.

The main goal of EasyVote, which focuses on the complex local elections in Darmstadt, is to address the above challenges by supporting voters and electoral officials electronically. Thereby, however, by preserving the rough, publicly open, processes (vote casting and tallying) of the traditional paper-based elections. Hence, the central idea of EasyVote is to use an electronic voting device, which supports voters with interactive feedback while selecting their preferred candidates/parties and prints the summary of their selections on a DIN-A4 [Int07] piece of paper. The printed ballot or so-called paper audit trail, which contains the summary of voter's selections, consists of a human- and a machine-readable (a QR-Code as proposed in [Int15]) component. Voters are supposed to verify that the human-readable ballot component reflects their voting intention and then to deposit their ballot into the ballot box. Similarly, electoral officials are supported by an electronic tallying device, which enables them to tally the ballots semi-automatically by scanning the QR-Codes. Thus, to compute the election result, electoral officials scan the QR-Code of each ballot and supposedly verify that its content matches the human-readable ballot component.

The advantages of EasyVote, in comparison to the traditional paper-based elections, can be summarised as follows:

- Voters do not spoil their vote (ballot) unintentionally . Note that EasyVote does not (fully) restrict voters in their selections. For instance, voters are able to invalidate their ballot intentionally, either directly (e.g. selecting the button *spoil ballot*) or indirectly (e.g. printing a blank ballot). Nevertheless, there are two restrictions regarding the act of voting: (1) Voters can not cast more than three direct votes to a candidate; (2) An indirectly invalidated ballot, for instance when a voter casts more than 71 votes among candidates of different parties, does not contain all selections due to the restricted ballot size, but rather a textual explanation regarding the invalidity of the ballot.

- Voters do better and directly understand the impact of their selections, because the so-called healing rules are applied immediately, i.e. not in the tallying phase.

- Visually impaired voters are able to cast their vote without assistance.

- Electoral officials might make fewer errors, as voter's selections are automatically, rather than manually, transferred into the tallying device.

- Electoral officials and the general public are able to verify intermediate results.

- Electoral officials might compute the election results faster, i.e. on the election day, due to smaller ballot sizes. The smaller size of the ballots might also improve the accuracy of the process.

- Fewer personnel are necessary, because EasyVote suggest that only two electoral officials are required to perform the tallying process.

Next to the above advantages, EasyVote introduces a number of new challenges that need to be considered and addressed. Some of these challenges, for instance the development of effective verification instructions that make voters most likely to verify that their ballot matches their intention, are addressed within this dissertation. However, others, for instance how to ensure vote secrecy against side-channel attacks, are out of the scope of this dissertation.

While Figures 5.1 and 5.2 present the EasyVote components, in the following we describe the EasyVote steps of the vote casting and tallying process. Note that for the sake of simplicity, we assume that there is only one electronic voting device in the polling station. Nevertheless, in practice, depending on the size of the district, polling stations might be equipped with many electronic voting devices, including backups. Furthermore, for procedures that are out of the scope of this dissertation, like filling printouts, changing cartridges or dealing with complaints, we refer the reader to [BJV14].

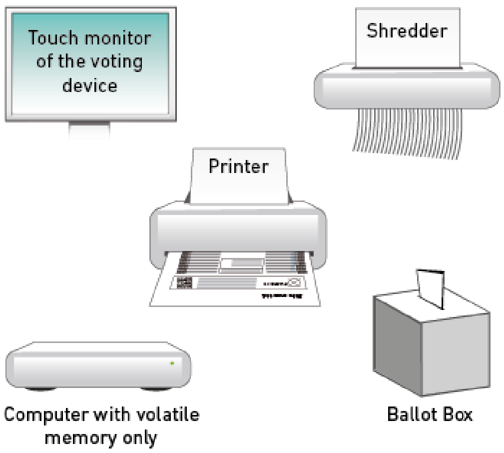

Figure 5.1: EasyVote: The components used in the vote casting process.

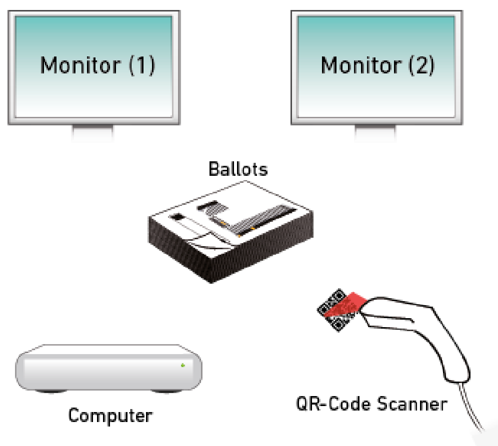

Figure 5.2: EasyVote: The components used in the tallying process.

5.1.1. Vote casting process

As EasyVote aims to maintain the processes of the traditional paper-based elections, voters proceed similar to the local elections in Darmstadt regarding identification, see section 4.1.

After electoral officials confirm the voter's identity, they enable the electronic voting device by using a remote wired controller. Next, the voter enters the voting booth. In the voting booth, the voter prepares the ballot by selecting the preferred candidates/parties on the voting device. The voting device supports the voter by giving feedback about the current state of the ballot, specifically whether it is valid or not. When the voter confirms her selections, which are shown on the review screen, the voting device prints the ballot. After printing, the voting device is disabled automatically and no electronic data are retained. The printed ballot contains the voter's selections, as shown before on the review screen, in a human- and a machine-readable (a QR-Code) format. The voter is supposed to verify that the human-readable ballot component reflects her voting intention. Finally, the voter folds the printed ballot, exits the voting booth and deposits the ballot into the ballot box. In case the voter wants to cast a different ballot, i.e. not the one already printed, she is required to proceed as follows:

1. Exit the voting booth.
2. Destroy the printed ballot in front of the electoral officials, while keeping her selections secret.
3. Wait until electoral officials re-enable the voting device, and then reenter the voting booth.

5.1.2. Tallying process

The EasyVote tallying process, similarly to the vote casting process, is based on the tallying process of the local elections in Darmstadt, see section 4.2. In the following we describe only the second phase, because the first phase and the respective preparatory steps, for instance entering intermediate results, are completely maintained from the traditional paper-based elections.

Similar to the process with PC-Wahl, electoral officials tally ballots individually. Thereby, electoral officials scan the QR-Code and are supposed to ensure that its content, as shown on the first monitor, matches the human-readable ballot component. In case there is a mismatch, electoral officials are supposed to undertake respective corrections, such that the digital representation of the ballot (EasyVote entry) matches the printed one. The corrected, printed ballots are placed on a separate batch for later auditing. After electoral officials have verified (when necessary corrected) the content, and confirmed its correctness, the scanned ballot is added to the intermediate result, shown on the second monitor. Further, electoral officials are supposed to verify that the scanned ballot is added to the intermediate result correctly. Afterwards, for auditing purposes, electoral officials label (mark with an ordinary pen) ballots consecutively with the respective number of their digital representation (EasyVote entry). When all ballots are tallied/scanned, electoral officials compute the final election result by printing and signing the disposition.

5.2. Prototype

This section introduces the EasyVote prototype. This prototype, which is used and incrementally improved throughout this dissertation, is the result of the master thesis by Jöris [Jör13]. The goal of this prototype is to enable researchers to explore research questions regarding electronic voting in the context of complex elections. Thus, even though this prototype is based on well-known software design patterns (model-view-controller, observable, singleton, composite etc.) [GHJV94] and it does not store ballots electronically, we do not recommend the use of this prototype in legally binding elections. This prototype should be considered a tool to conduct research rather than a system to conduct (legally binding) elections. However, we encourage other researchers who are interested in electronic voting and complex elections to use and further improve the EasyVote prototype.

In the following we introduce and describe the different components of the EasyVote ballot. Further, we present and describe the different components of the interfaces for the vote casting and tallying process.

5.2.1. Ballot design

In this section we introduce and describe the components of the EasyVote ballot design, which is proposed in [Jör13] and presented in Figure 5.3. The ballot consists of three main components:

1. The component on the top of the ballot. This component contains the description of the election, i.e. the election for which the ballot is cast.
2. The middle component which consists of the following three sub-components:
   a) The left sub-component, which contains the name or abbreviation of the selected party.
   b) The middle sub-component or so-called status bar. This component contains a textual explanation regarding the ballot composition, i.e. how the voter has cast her votes. This explanation shall enable voters and electoral officials to comprehend the consequences of the voter's actions (selections), and thereby prevent the role of the electronic voting device as a decision maker. For instance, due to the many possibilities to invalidate a ballot and the ballot's size restriction, all invalid ballots share the same look. Thus, the left sub-component contains the word *invalid*, and the middle sub-component explains in text, why the electronic device has

interpreted a voter's selections as invalid. This enables both voters and electoral officials to comprehend the consequences of the voter's actions (selections).

c) The right sub-component contains the QR-Code. The QR-Code, which encodes the same information as the human-readable ballot component, serves to tally the ballots semi-automatically. Note that the QR-Code encodes the information in plaintext. This means that the encoded information can be read and interpreted with any QR-Code reader.

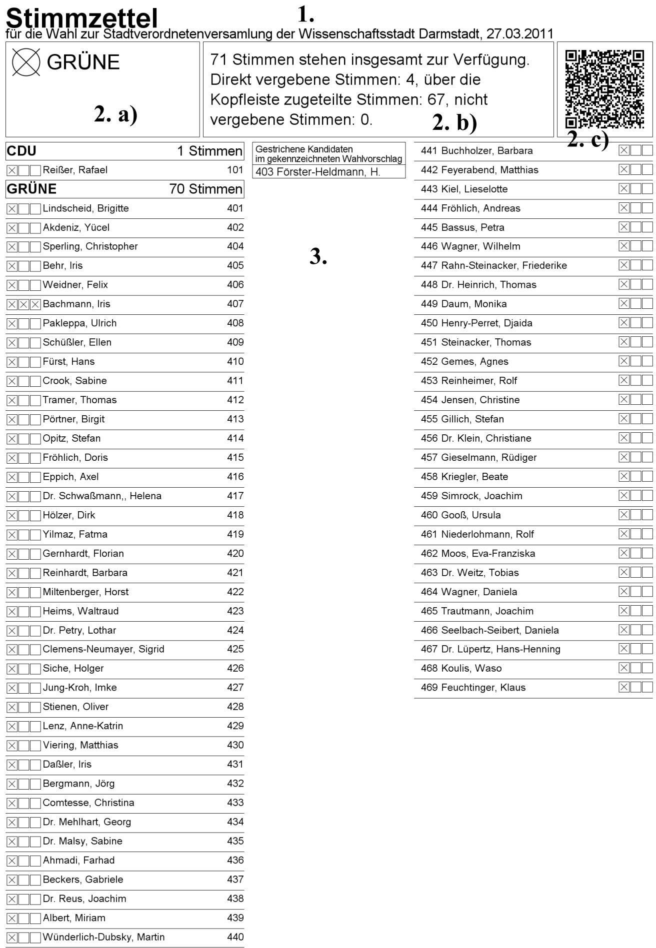

Figure 5.3: EasyVote: The ballot design and components.

3. The bottom component which consists of three columns. While the middle column contains the crossed out candidates, the left and right columns contain

the selected candidates, i.e. candidates that are assigned votes, either directly or automatically by selecting a party. Note that due to size restrictions the middle column contains only the crossed out candidates of the selected party.

Note that in contrast to the interfaces, which are presented in the next section, no usability methods have been applied to evaluate the proposal, shown in Figure 5.3.

5.2.2. Interfaces

In this section we introduce and describe the components of the interfaces for the vote casting and tallying process. The interfaces of the vote casting and tallying process have been designed based on *The Low Error Voting Interface* [SHGS05] and the following interface design recommendations by Tidwell [Tid10]:

1. The interfaces provide *clear entry points*, i.e. the interfaces determine a clear starting point and accompany the user (voter and/or electoral official) in the subsequent steps by providing all information necessary to proceed.

2. The interfaces are *safe to explore*, i.e. users are able to undo every single step and also start from the beginning[16], without worrying about the consequences of their previous action(s).

3. The interfaces facilitate *recognition*, because all interfaces share the same font, font size, colour, and positioning of buttons and information panels. Note that these attributes are different between the vote casting and tallying process interfaces.

4. The interfaces follow the *few hues, many values* design pattern. This means that the interfaces consist of one basic colour which is used in various colour shades and supplemented only by signal colours, namely red, green and orange. Note that the basic colours, namely blue for the vote casting and gray for tallying process interfaces, are selected based on the system neutrality requirement [Ric12]. This requirement states that any content-related influence of voters by the voting system should be excluded, for instance colours that are socially associated with nominated parties.

Furthermore, the interfaces have been iteratively improved by applying a usability method, namely the cognitive walkthrough method proposed by Stone *et*

[16]This is possible as long as voters do not start the printing process.

al. [SJWM06]. Thereby, information security, cryptography, electronic voting, usability, human computer interaction, legal, election administration and design experts inspected the interfaces by going through various fictitious voting scenarios. The goal of applying the cognitive walkthrough was to analyse and improve the functionality and information provided to voters and electoral officials in each step. This is so that they can make an informed decision regarding which functionality to use, and understand the corresponding next step.

Interfaces for the vote casting process

The interfaces for the vote casting process, presented in Figure 5.4, consist of four main components:

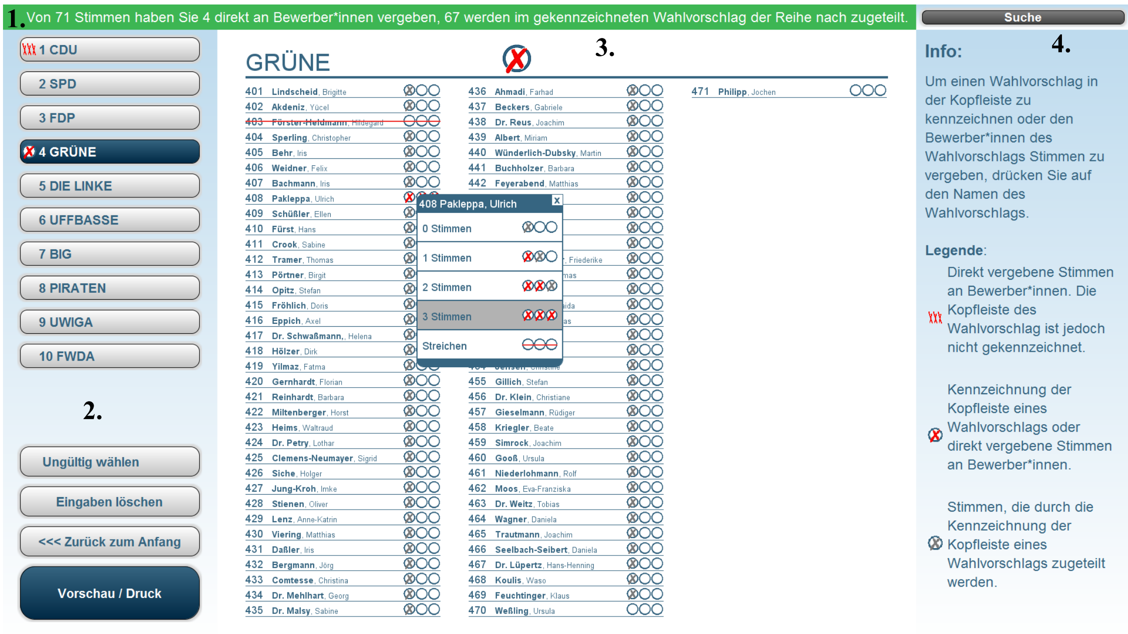

Figure 5.4: EasyVote: Components of the vote casting process interfaces.

1. The component on the top of the interface which has two functionalities:
    a) It informs voters regarding the number of already cast votes and the remaining ones. Further, the presented information distinguishes between votes that are cast directly and votes that are assigned automatically, if the voter has selected a party.
    b) It informs voters regarding the current state of their selections, specifically whether the ballot is valid or not. This information is supported by

using different colours: (1) Blue for neutral (vote casting not started); (2) Green for valid; (3) Red for invalid; and (4) Orange when a healing rule is applied. Note that the information regarding the applied healing rule, or why the ballot is invalid, is also printed on the status bar (middle sub-component) of the ballot, refer to section 5.2.1.

2. The left column component which consists of two parts. While the upper part contains the list of nominated parties (as buttons), the bottom part contains the control and navigation buttons.

3. The middle component, which displays the candidates of the clicked party. In this component the voter can cast direct votes, cross-out candidates or select the clicked party.

4. The right column component which consists of two parts. While the upper part contains the search function and general information on how to proceed, the bottom part contains the legend regarding the different symbols.

Note that these components are shared among all interfaces for the vote casting process. The different interfaces for the vote casting process are presented in section A in appendix.

Interfaces for the tallying process

The interfaces for the tallying process build upon the recommendations in [VBD11] (the original EasyVote publication), namely to use two different interfaces that are displayed on two different monitors simultaneously. The first interface, presented in Figure 5.5, consists of the following components:

1. The left column component which contains the control and navigation buttons.

2. The middle component which is a blank space. On this component electoral officials shall hold the currently scanned ballot and compare whether its content matches the displayed data.

3. The left and right columns, next to the middle component. This component, which displays the data scanned from the QR-Code, enables electoral officials to perform a column-wise comparison with the printed ballot. In addition, the left column displays the selected party and the sequential number (ID) of the currently scanned ballot. Further, the right column displays whether the ballot is valid (green) or invalid (red).

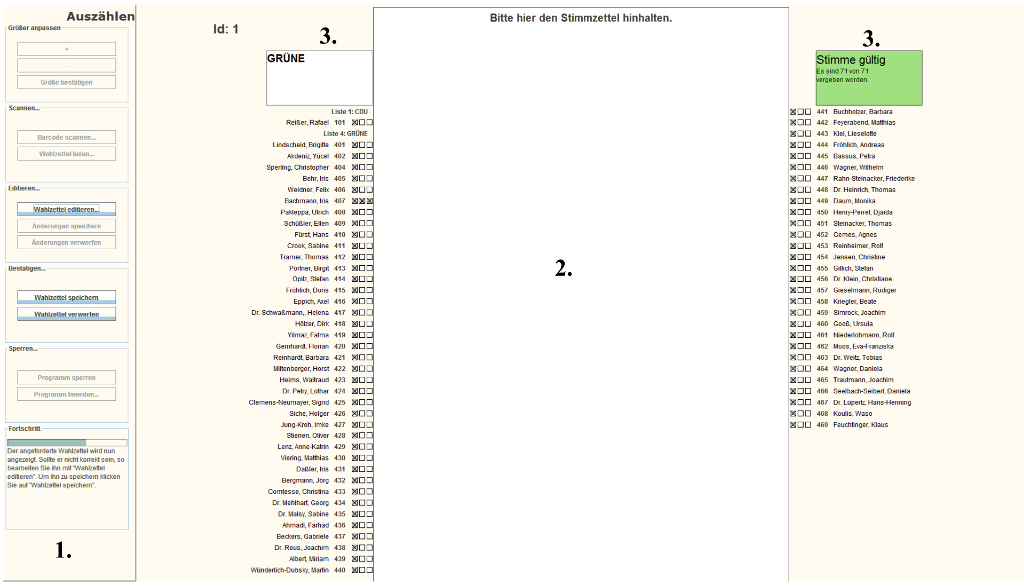

Figure 5.5: EasyVote: Scanning and verifying the content of the current ballot.

The second interface, presented in Figure 5.6, consist of the following components:

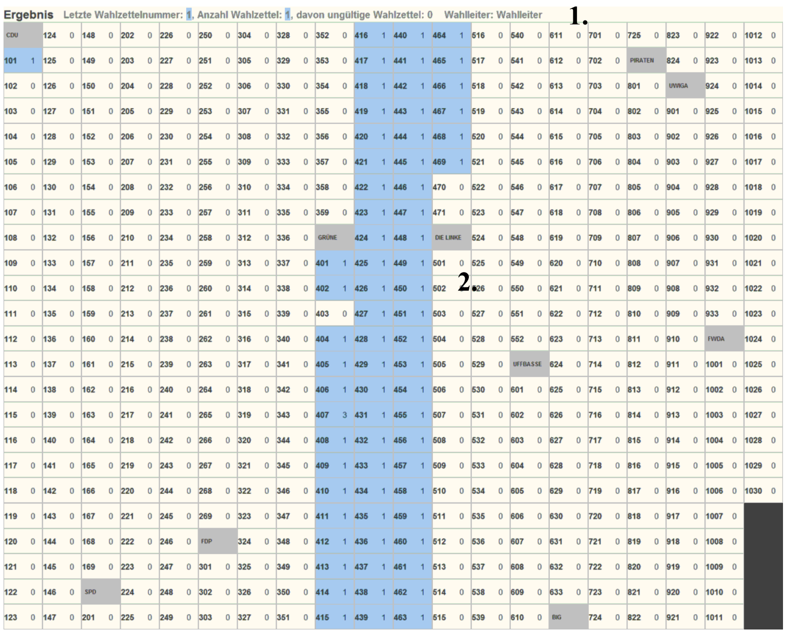

Figure 5.6: EasyVote: Verifying the correctness of the intermediate result.

1. The component on the top of the interface. This component contains the sequential number (ID) of the currently scanned ballot, the number of all

scanned ballots, the number of valid and invalid ballots and the name of the electoral officer.

2. The bottom component which contains the current intermediate result, i.e. the total number of votes per candidate. The candidates are ordered according to the paper-based elections, i.e. according to their party list order and to the order of parties on the paper ballot. Furthermore, in order to support the verification of intermediate results, the candidates that are assigned votes after scanning the current ballot are highlighted. Note that due to size restrictions, i.e. size of the monitor, the candidates are listed/represented only by their election specific number.

Part II.

User studies

6 Background

In this chapter we introduce background information with respect to the user studies reported in this dissertation. The first part provides a short overview regarding the used research methods. In the second part we introduce some additional considerations that are shared among the reported studies.

6.1. Research methods

In this section we introduce the different types of behavioural research and discuss how to determine the design structure of an experiment. Further, we outline the various types of experimental design and statistical tests.

Types of behavioural research

A variety of research method are available for conducting research in the area of human-computer interaction (HCI), which includes the area of usable security. The most frequently used are observations, field studies, surveys, usability studies, interviews, focus groups, and controlled experiments. All of these methods are kinds of behavioural research (empirical investigations) and can be categorised into three groups: descriptive, relational and experimental. Descriptive investigations, for instance observations and surveys, aim to construct an accurate description of a situation or a set of events. However, this method does not enable the researcher to identify a relationship between observed events, nor to provide an explanation. In contrast, relational investigations allow the establishment of relations between multiple factors, for instance the value of factor X changes as the value of factor Y changes. However, in contrast to experimental investigations, this method can rarely determine the casual relationship between factors. Hence, experimental research enables the identification of causal relationships. Table 6.1 summarises the differences between these types of behavioural research. For more detailed information regarding research methods in HCI, we refer the reader to [LFH10].

Table 6.1: Research methods: Differences between descriptive, relational and experimental research [LFH10].

Types of research	**Focus**	**General claims**	**Typical methods**
Descriptive	Describe a situation or a set of events	X is happening	Observation, field studies, focus groups, interviews
Relational	Identify relations between multiple variables	X is related to Y	Observation, field studies, interviews
Experimental	Describe a situation or a set of events	X is responsible for Y	Controlled experiments

Note that most of the studies reported in this dissertation aim to identify casual relationships, so the experimental research method was usually applied.

Determining the design structure of experiments

According to Lazar *et al.* [LFH10], the basic structure of a controlled experiment can be determined by answering the following questions:

1. How many independent variables do we aim to explore in the experiment?
2. How many different values does each independent variable have?

The answers to these questions can be derived from the research hypotheses of the respective experiment. Therefore, research hypotheses should clearly state the independent and dependent variables of the experiment. In general, independent variables are factors that the researcher controls and dependent variables are the effects that the researcher measures. More specifically, in an experiment the researcher aims to find out whether and how changes in the independent variables imply changes in the dependent variables. Furthermore, the decision to adopt the appropriate design, namely between-group, within-group or split-plot design, should be based on the following attributes:

1. The number of conditions in the experiment, i.e. the number of values of each independent variable.

2. The nature of application.
3. The participants (size, characteristics etc.).
4. The task to be examined.

Figure 6.1 presents the procedure to determine the structure of experiments. For more detailed information regarding the determination of the design structure, we refer the reader to [LFH10].

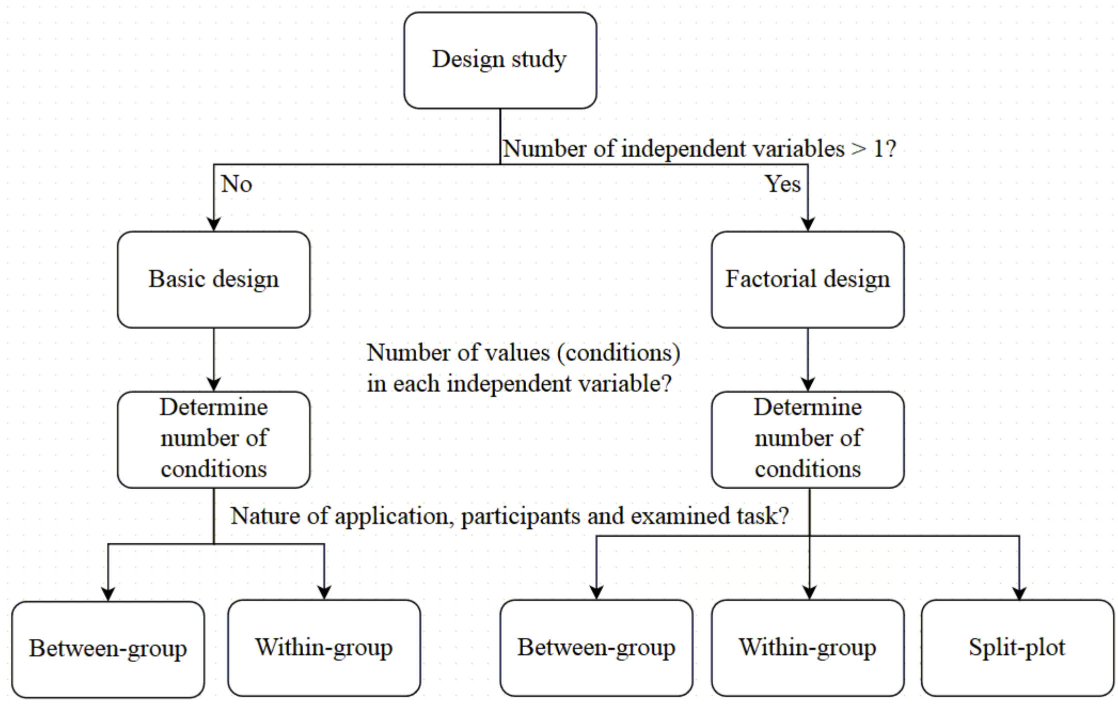

Figure 6.1: Research methods: Procedure to determine the structure of an experiment.

Types of experimental design

Lazar *et al.* [LFH10] distinguishes between three types of experimental designs, namely between-group, within-group and split-plot design. In a between-group experiment design, presented in Figure 6.2, each participant is exposed to only one experiment condition. Thus, the number of groups in the experiment directly corresponds to the number of conditions. In contrast, in a within-group experiment design, presented in Figure 6.3, each participant is exposed to all conditions in the experiment. Thus, only one group of participants is necessary. Furthermore, a split-plot design, which is used when more than one independent variable is investigated, is a combination of the between-group and within-group experimental designs. This means that one or more independent variables are investigated through a between-group design, while the others are investigated through a within-group design.

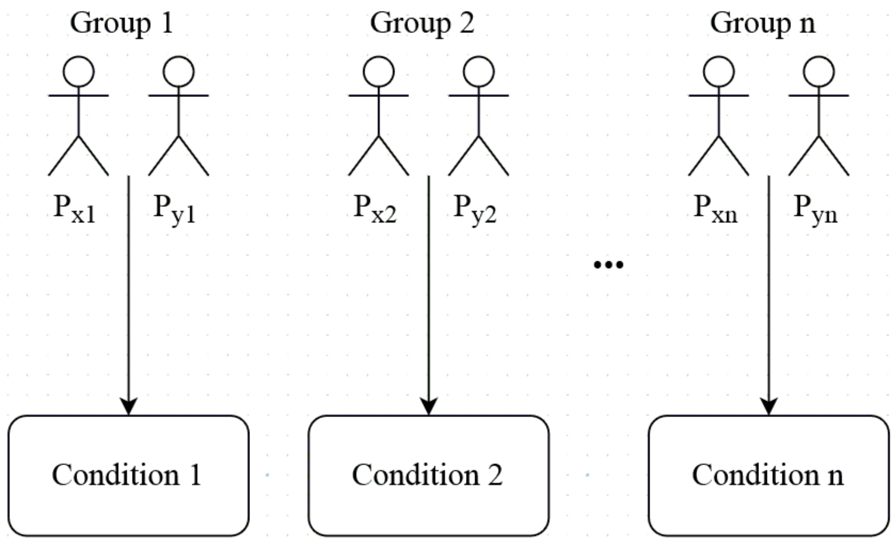

Figure 6.2: Research methods: Between-group design.

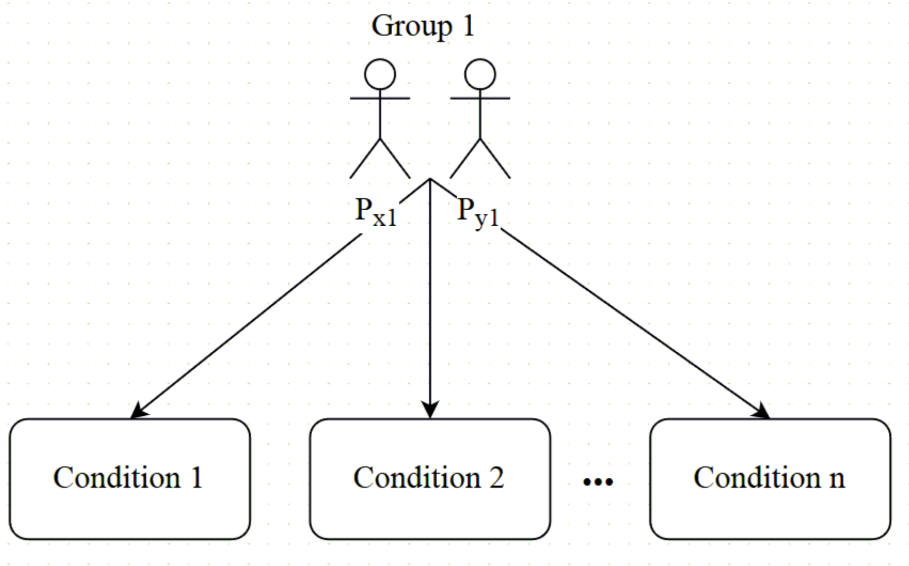

Figure 6.3: Research methods: Within-group design.

Table 6.2 summarises the advantages and disadvantages of the fundamental experimental designs, namely between-group and within-group. For more detailed information regarding the different types of experimental design, we refer the reader to [LFH10].

Table 6.2: Research methods: Advantages and disadvantages of the fundamental experimental design types [LFH10].

	Fundamental types of experimental design	
	Between-group design	**Within-group design**
Advantages	Cleaner, Avoids learning effect, Better control of confounding factors such as fatigue	Smaller sample size, Effective isolation of individual differences, More powerful tests
Disadvantages	Larger sample size, Large impact of individual differences, Harder to get statistically significant results	Hard to control learning effect, Large impact of fatigue

Types of statistical tests

When investigating a certain phenomenon within a large population, such as eligible voters, there is no way to collect data from every individual in the population. Therefore, a smaller group (a sample) from the larger population is selected to represent the entire population. In order to determine the confidence with respect to the generalisation of the observed phenomenon to the entire population, statistical tests are used to process the data collected from the sample.

In general statistical tests can be classified into parametric and non-parametric tests. Parametric tests, such as t tests, rely on several general assumptions:

1. The sample has an approximately normal distribution.

2. The variables should be at least scaled by intervals.

3. The variance in the data collected from different groups should be approximately equal.

When the above assumptions are not met, non-parametric tests are used. It is important to emphasise that non-parametric tests, even though they are called "assumption free", also rely on assumptions. Nevertheless, the assumptions of non-parametric tests are specific to the test. For instance, one of the most commonly used non-parametric tests, namely Chi-square, has a specific assumption on the sample size and independence of the data points.

Note that the selection of the appropriate statistical test and the accurate interpretation of the results are essential for justifying the validity of the reported findings. Beside the nature of the collected data, the study design is also important when selecting the statistical test. For more information with respect to the context of use and assumptions of different (parametric and non-parametric) statistical tests, please refer to [LFH10].

6.2. Additional considerations

In this section we introduce some additional considerations that are shared among the reported studies, namely the platform for conducting online experiments, participants' experience with electronic voting, ethical considerations and control of systematic errors. Note that participants' experience with electronic voting and ethical considerations are not explicitly mentioned in the reported studies.

Platform for online experiments

In order to create and conduct online experiments we used the SoSci Survey[17] online platform. SoSci Survey is specifically developed for scientific online surveys and/or experiments. It provides a usable interface and very high flexibility with respect to the design of online surveys and/or experiments. This enables the creation of sophisticated online questionnaires and complex experimental designs.

Participants' experience with electronic voting

In 2009, the German Federal Constitutional Court introduced the principle of *public nature of elections* [Fed09]. This principle states that it must be possible for any citizen/voter to verify the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge, i.e. each election step must be transparent to the voter.

Since the introduction of the principle of public nature of elections, all electronic voting systems that were in use, for instance Nedap voting systems, were banned and judged unconstitutional, because they do not to comply with this principle. Hence, as all studies reported in this dissertation focus on local elections in Germany

[17] https://www.soscisurvey.de/, last accessed February, 7, 2016.

(Darmstadt, Hesse), and are conducted in Germany, participants who were younger than 18 years old in 2005 are not familiar with electronic voting.

Nevertheless to support this dissertation, it is important to emphasise that EasyVote has been analysed and shown, refer to [HVB12] for the legal analysis, to comply with the German legal requirements for local elections in Hesse, in particular with the principle of the public nature of elections. As the legal analysis is in German, we summarise the most important conclusions:

- Voters can verify their vote without any specialist knowledge.
- Voters are not required to blindly trust the underlying integrity of EasyVote.
- EasyVote enables an automatic tally of single votes (ballots), and also a full manual tally of votes, similar to traditional paper-based elections.
- The human-readable ballot component is the deciding factor regarding the tallying process.
- EasyVote strengthens the principle of public nature of elections, since, on the one hand, voters can better understand the impact of their selections (how their cast votes are tallied), and on the other hand the tallying process might be faster and more accurate than in the traditional paper-based elections.

Ethical considerations

An ethics commission at the *Technische Universität Darmstadt* lays down ethical requirements for research involving humans[18]. These requirements are considered in all reported studies. Hence, participants in the respective study are required to read and sign[19] a declaration of consent. Furthermore, when necessary, participants are debriefed regarding the actual research goal at the end of the study. Last, but not least, participants can interrupt and leave the study at any time without needing to provide a reason.

Control of systematic errors

One of the main challenges in the area of usable security is to avoid potential social desirability biases [KPW06], also referred as systematic errors. Otherwise participants may act in a manner perceived to be socially desirable rather than acting as

[18] `http://www.intern.tu-darmstadt.de/gremien/ethikkommisson/index.en.jsp`, last accessed February, 7, 2016.

[19] For the online studies, participants clicked on a “I agree to the terms” checkbox.

they actually would in a real world situation [SHB10]. In order to offset social desirability, when necessary, a fictitious instead of the actual research goal is presented to participants. Nevertheless, in accordance to the ethical considerations introduced above, participants are debriefed regarding the actual research goal at the end of the study.

7 Investigating and addressing secrecy concerns regarding QR-Codes

The goal of this chapter is to investigate whether voters have secrecy concerns with respect to the use of QR-Codes and, if so, to address such concerns effectively.

To achieve this goal, we conducted a survey to determine whether voters have secrecy concerns with respect to the use of QR-Codes. We analysed and summarised voters' stated concerns about QR-Codes. Building upon the results of the survey, we discussed different alternatives on how to address such concerns, and identified the most appropriate one. Finally, we conducted an online experiment to evaluate the effectiveness of the identified alternative regarding the allay of such concerns. In the experiment we used the protection motivation theory [Rog75], as the underlying theoretical foundation. Note that, to the best of our knowledge, this is the first work to investigate and address voters' secrecy concerns regarding QR-Codes.

The content of this chapter has been published at the *Journal of Information Security and Applications* [9] and the *16th International Conference on Human-Computer Interaction* [7].

7.1. Risks and benefits of using QR-Codes

Independent of whether voters have secrecy concerns regarding QR-Codes, it is of crucial importance first to analyse and contemplate the risks and benefits of using QR-Codes. Hence, with respect to the risks of using QR-Codes, the question is whether QR-Codes introduce a new attack vector, i.e. whether they constitute an additional risk regarding vote secrecy. Note that this question relates not only to EasyVote, but also to other electronic voting schemes/systems that share similar concepts, for instance [BCH$^+$12, BFL$^+$12, Veg12, BBE$^+$13, Vot08]. The answer to this question is no, because by removing QR-Codes the risk that additional information, for instance the time of vote casting, can be subliminally introduced into the printed ballot can not be prevented, refer to [BCT10, Mac10, vBSB13]. Therefore, the use of QR-Codes does not represent an additional risk regarding vote secrecy.

Furthermore, regarding the benefits of using QR-Codes, they offer several advantages, listed below, in comparison to Optical Character Recognition (OCR) scanners, which would be the obvious alternative if QR-Codes were removed.

- QR-Code scanners are less expensive than OCR scanners, or even for free.
- Because of inbuilt (in QR-Codes) redundancy, refer to [Int15], QR-Code scanners provide a higher error correction level and therefore are more accurate than OCR scanners.
- QR-Code scanners can be used for all types of ballots (universal encoding), while OCR scanners need to be configured and maintained for each type of ballot.

7.2. Investigating secrecy concerns regarding QR-Codes

When confronted with electronic voting, most voters focus on non-technical aspects, such as “Can I use it?”, “Is my vote choice secret?” and “Will my vote count?” [OdB04], [OdB09], [AKLM09]. However, if voters believe a technical aspect endangers their vote secrecy, they might abstain from voting [GHDD13] or alter their voting behaviour [LSX$^+$13]. Further, Llewellyn *et al.* [LSX$^+$13] reports that voters show doubts, i.e. have secrecy concerns, when their ballot contains information additional to their selections. Last, but not least, secrecy concerns regarding barcodes are also mentioned in a technical analysis of various vote verification technologies for the Maryland State Board of Elections [NSN06]. This issue is thus a real concern with respect to the acceptability of electronic voting schemes/systems such as EasyVote. Hence, as the EasyVote ballot contains additional information, namely the QR-Code, which is a technical aspect that serves to tally ballots semi-automatically, we postulate that the use of QR-Codes raises secrecy concerns among voters. Therefore, the goal of this section is to determine whether voters have secrecy concerns about the use of QR-Codes and, if so, to analyse and summarise their concerns. In order to achieve this goal, we conducted a user study. In the following we describe our study and report the results.

7.2.1. Overview

In this section we describe the design, setting and evaluation methodology of the user study.

Design

The main purpose of the study was to determine whether participants (voters) have secrecy concerns with respect to the use of QR-Codes and to analyse and summarise their concerns. To achieve this goal we conducted a trail election with EasyVote in combination with an online exit survey.

The trial election took place alongside the university elections at Technische Universität Darmstadt in June 2013. In this trial election participants cast a vote to express their satisfaction regarding their supervisor, namely the orientation phase tutor and mentor (for freshers), bachelor thesis supervisor (for undergraduates), master thesis supervisor (for graduated students), PhD thesis supervisor (for PhD students), line manager (for employees), and the president (for professors). Participants could express their satisfaction by selecting one of the following options:

1. Always satisfied.
2. Mostly satisfied.
3. Sometimes yes sometimes no.
4. Rarely satisfied.
5. Never satisfied.

After casting their vote in the trial election, participants filled in the exit survey. The exit survey consisted of a number of questions and statements regarding the implemented prototype (EasyVote) and electronic voting in general. In particular, in alignment with our goal, the survey required participants to indicate their agreement with and comment on the following statement:

Statement regarding QR-Codes: I think that vote secrecy might be violated by the use of the QR-Code.

Thus, while the survey directly served our actual research goal, the goal of the trial elections was twofold:

1. Hide the actual goal of the study to avoid potential social desirability bias, see section 6.2. Therefore, in the study participants were given the following fictitious goals:
   a) Evaluation of the EasyVote prototype from a technical and practical perspective.
   b) Evaluation of electronic voting in general.
2. Induce a personal relevance to the ballot regarding secrecy, in order to create a realistic voting scenario.

Note that in the time of this study, the EasyVote prototype for complex elections was not implemented yet. Therefore, for the purpose of the study, we implemented and deployed a simplified prototype.

Setting

Figure 7.1 provides a general overview of the setting used in our study. The polling station, which was placed in the cafeteria next to the university election polling stations, consisted of these areas:

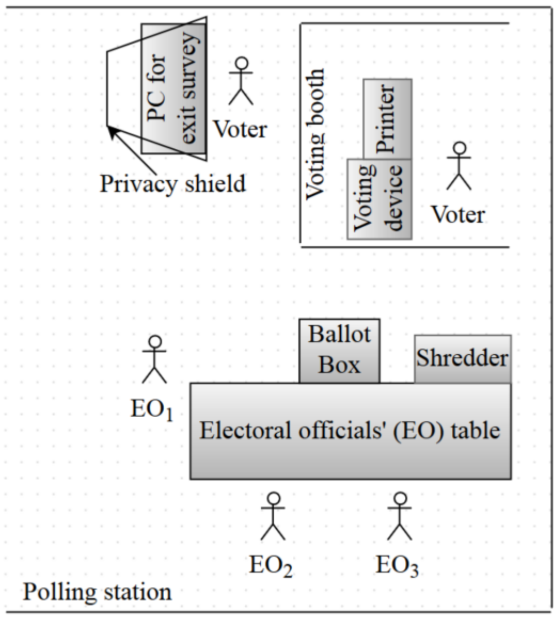

Figure 7.1: Trial elections: General overview of the user study setting.

- The electoral officials' area, presented in Figure 7.2.

- The exit survey area, presented in Figure 7.3.
- The voting booth area, presented in Figures 7.4 and 7.5.

Figure 7.2: Trial elections: The electoral officials' area.

Figure 7.3: Trial elections: The exit survey area.

Figure 7.4: Trial elections: The inside of the voting booth.

Figure 7.5: Trial elections: The outside of the voting booth.

Further, Figures 7.6, 7.7, 7.8 and 7.9 present the interfaces of the implemented EasyVote prototype. Finally, for the exit survey we used the SoSci Survey online platform, refer to section 6.2.

Evaluation methodology

To determine whether participants have secrecy concerns regarding the use of QR-Codes, we evaluated their responses, on a five-point Likert scale anchored in "strongly

Figure 7.6: Trial elections: Welcome screen.

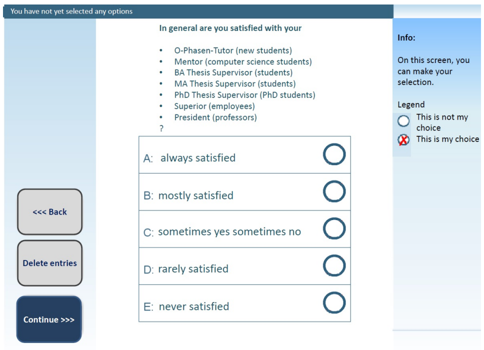

Figure 7.7: Trial elections: Options screen.

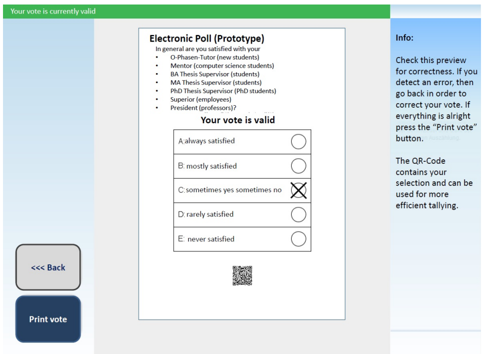

Figure 7.8: Trial elections: Preview screen.

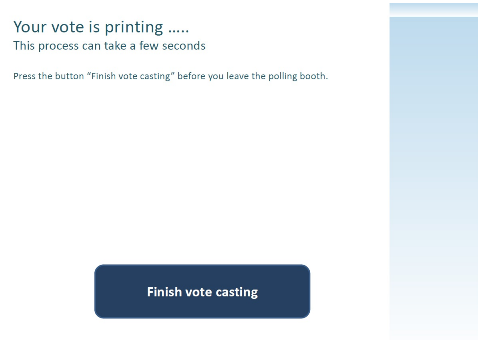

Figure 7.9: Trial elections: Finish screen.

disagree" and "strongly agree", with respect to the statement:

Statement regarding QR-Codes: I think that vote secrecy might be violated by the use of the QR-Code.

Furthermore, to analyse and summarise participants' concerns, we conducted a qualitative analysis of their comments. The qualitative analysis was carried out by using the Grounded Theory Method [SC90]. In order to identify codes, the author and another member of the author's research group independently analysed participants' comments by using spread sheets. Each single code was considered, even when several codes were mentioned by a single participant. The identified codes were discussed and agreed upon by both reviewers. Note that participants' comments were translated into English for reporting.

7.2.2. Procedure

The study consisted of the following sequential steps:

1. Participants read and signed the declaration of consent for participating in the study.
2. Participants were verbally presented with the goals and the procedure of the entire study (trial election plus exit survey).
3. Participant were verbally introduced to the vote casting process with EasyVote, focusing on the voting rules.
4. Participants registered in the electoral register.
5. Participants entered the voting booth, made their selection and deposited their ballot into the ballot box.
6. Participants filled in the exit survey, either next to our polling stations or from any other location. The survey also collected demographic data (age range, gender and education).

7.2.3. Participants: Recruitment, incentives and sample

The participants were recruited verbally, directly after having cast their vote for the university elections. One of the three electoral officials stood in front of the electoral officials' area and asked people to participate in the study. No incentives were provided, thus participation was purely voluntary.

In total 421 participants cast a vote in the trial election. However, only 198 of them (135 male, 63 female), see Figure 7.10 for the participants' age ranges, filled in the online exit survey. Thus, in the results we consider only 198 participants. The sample consisted of students from different departments (e.g. sociology, psychology, mathematics) and employees (e.g. secretaries, care takers, administrative technical staff) of the Technische Universität Darmstadt.

7.2.4. Results

According to the findings from our exit survey, 79 out of 198 participants were concerned regarding their vote secrecy in association with QR-Codes. Figure 7.11 presents the distribution of participants' agreement with the presented statement, namely "I think that vote secrecy might be violated by the use of the QR-Code.".

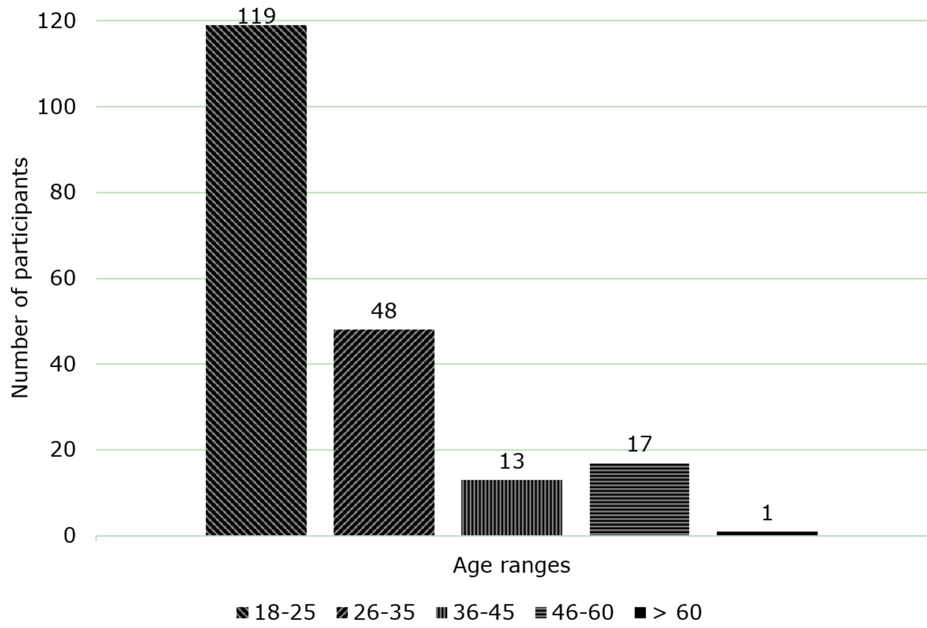

Figure 7.10: Trial elections: Participants' age range.

These findings confirm the results reported by Llewellyn *et al.* [LSX+13] and also our assumption, that the use of QR-Codes in the EasyVote ballot raises secrecy concerns among voters.

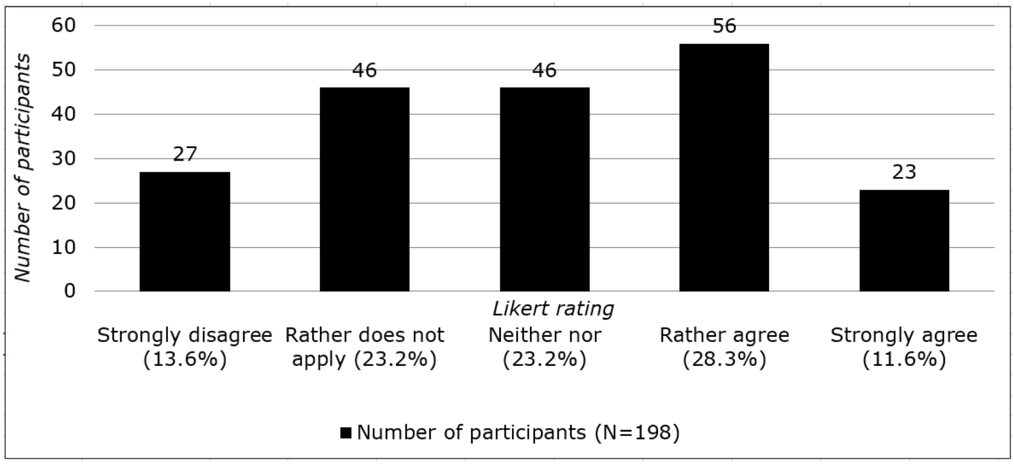

Figure 7.11: Trial election: Participants' agreement regarding secrecy concerns with QR-Codes.

In addition, based on our qualitative analysis we identified two codes. For each code we also provide two sample comments given by the participants.

1. Transparency:
    a) It is not apparent which information is stored.
    b) The QR-Code stores information that is not readable by the human eye. One cannot see which information is stored, the QR-Code could therefore store personal data.
2. Technical equipment to verify not available:
    a) A QR code is (naturally) a representation of information that is not written in "natural language". Therefore, its' content cannot be verified without necessary technical equipment.
    b) The QR code is readable only with appropriate technical equipment. The QR-Code may include additional information, like the voting booth and time of vote casting, and this cannot be verified without necessary technical equipment.

Finally, from the participants' comments, we developed a summarised description of participants' concerns:

Description of secrecy concerns: Voters can not verify what information is stored in the QR-Code reliably. Hence, a malicious voting device could store information additional to voters' selections, for instance the time of vote casting or the sequential number of cast votes. Such additional information could unambiguously link voters to their ballots (cast votes). Thus, vote secrecy would be violated.

Note that in the analysis we considered only the comments of the 79 participants, who agreed or strongly agreed with the presented statement.

7.2.5. Discussion and limitations

The study confirmed that the use of QR-Codes in the EasyVote ballot had the potential to raise secrecy concerns among voters. These findings are in alignment with the findings of previous studies, namely that voters show doubts, i.e. have secrecy concerns, when their ballot contains information additional to their selections [LSX+13]. However, it is possible that the number of participants having secrecy concerns might be slightly different in a real world situation. The number might be higher in legally binding elections, where vote secrecy might have greater importance to voters in comparison to our trial election. The number might also be lower, because of the potential bias caused through our study design, i.e. by confronting participants with the statement regarding secrecy concerns in association with QR-Codes.

Both these perspectives, namely that in reality the number might be slightly higher or lower, reveal two limitations of our study. Nevertheless, the findings of our study reveal the potential for doubts and concerns to be caused by QR-Codes. A more accurate reflection could only be obtained, if voters' concerns are evaluated in legally binding elections. Moreover, to the best of our knowledge no such baseline data exist, even though we are aware of legally binding elections with electronic voting systems, whose ballots contain information additional to the voters' selections, for instance in Argentina [PLA$^+$14] and Ecuador [Poz14]. Therefore, we encourage researchers and election administrators who are involved in future elections, which are conducted with such voting systems, to address this issue. Furthermore, the potential overestimation of the reported results seems plausible for the following reasons: First, the slightly greater importance of vote secrecy in legally binding elections and the potential overestimation might cancel each other out in reality. Second, evaluating voters' concerns not in combination with a voting scenario, for instance through an interview or a survey, would be even less representative, because the ballot (cast vote) has no personal relevance to the voters. Third, evaluating voters' concerns indirectly, i.e. without directly asking their opinion regarding secrecy concerns in association with QR-Codes, would produce unreliable results. In reality, in particular in Germany where the well-known Chaos Computer Club[20] is very active regarding electronic voting, such technical aspects would be sufficiently discussed and challenged in beforehand, in public. Last, but not least, another limitation is that most of the participants in our study were university members, and therefore not representative of the larger voting population.

7.3. Addressing secrecy concerns regarding QR-Codes

The main goal of this section is to address secrecy concerns regarding QR-Codes effectively. While QR-Codes do not represent an additional risk regarding vote secrecy, refer to section 7.1, they can still be misused. Such concerns should be addressed by using risk communication techniques, which helps voters realistically to assess the likelihood of such a misuse. Hence, to achieve our goal, i.e. to address such concerns effectively, we use the threat appraisal approach of the protection

[20]The Chaos Computer Club is the Europe's largest hacker Association, refer to `https://www.ccc.de/`, last accessed February, 7, 2016.

motivation theory [Rog75]. Furthermore, we define the following hypothesis:

Hypothesis: The threat appraisal approach significantly allays voters' secrecy concerns regarding QR-Codes.

The independent variable is the threat appraisal approach, and the dependent variable is represented by voters' secrecy concerns regarding QR-Codes.

7.3.1. Overview

In this section we describe the design, setting and evaluation methodology of the user study.

Design

The main purpose of the study was to test the defined hypothesis. To achieve this goal we conducted an online experiment.

In the experiment participants were first introduced to the research goal. To avoid potential social desirability bias, see section 6.2, participants were given a (partially) fictitious research goal. Hence, participants were told that the goal of the experiment is to actively feed into the EasyVote voting scheme, in particular with respect to the ballot design, by following the human-centred design principles for interactive systems [Int10]. Next, participants were introduced to the EasyVote voting scheme, more specifically to the vote casting process. Afterwards, participants were presented with the description of secrecy concerns regarding QR-Codes, introduced below. Participants were told that these concerns were raised by participants of a previous survey. Subsequently, participants were required to indicate their agreement with the presented concerns. In the next step, participants were confronted with the threat appraisal approach. Finally, participants were required to reassess their opinion towards the presented concerns.

Description of secrecy concerns: Voters can not verify what information is stored in the QR-Code reliably. Hence, a malicious voting device could store information additional to voters' selections, for instance the time of vote casting or the sequential number of cast votes. Such additional information could unambiguously link voters to their ballots (cast votes). Thus, vote secrecy would be violated.

Note that based on our hypothesis and participants' task, which involves substantial human cognitive and perceptual capabilities (reading and comprehension), we adopted a basic within-groups design to diminish individual differences effectively.

Setting

To create the online experiment we used the SoSci Survey online platform, refer to section 6.2.

Evaluation methodology

To measure the effectiveness of the threat appraisal approach regarding the allay of secrecy concerns in association with QR-Codes, we compared participants' agreement, on a five-point Likert scale anchored in "strongly disagree" and "strongly agree", with respect to the presented secrecy concerns, before and after the threat appraisal approach. Finally, to determine the confidence of our measurements we ran a respective significance test.

7.3.2. Procedure

The online experiment consisted of the following sequential steps:

1. Participants read and confirmed (clicked on the checkbox) the declaration of consent for participating in the experiment.
2. Participants became familiar with the EasyVote vote casting process, in particular with the components of the EasyVote ballot.
3. Participants read the description of the secrecy raised by previous participants.
4. Participants indicated their agreement with respect to the presented concerns.
5. Participants were confronted with the threat appraisal approach, which is introduced in more detail below.
6. Participants reassessed their agreement with respect to the presented concerns.
7. Participants provided their demographics (age range, gender and education).

As recommended in the protection motivation theory [Rog75], the threat appraisal approach focused on the source of the threat by describing a sample attack of violating vote secrecy by misusing QR-Codes. The description consisted of the adversary's sequential steps, which are introduced below:

1. The adversary needs to gain access to and manipulate the electronic voting device, such that additional information, like timestamps, would be encoded in QR-Codes.

2. The adversary must be physically present in the polling station to record the name and time voters cast a vote.

3. The adversary needs to have access to the QR-Codes (ballots) in order to violate vote secrecy. This can only be done after the public tallying phase, either during transport or by accessing the storage room in the respective municipality.

7.3.3. Participants: Recruitment, incentives and sample

Participants were recruited via E-Mail and online social networks. No incentives were provided, thus participation was purely voluntary.

94 subjects (33 female, 61 male) participated, see Figure 7.12 for the participants' age ranges. Participants had the following education levels: 8 participants had a secondary school certificate, 11 had an advanced technical certificate, 38 had a general qualification for university entrance, 18 had a bachelors degree, 12 had a masters degree or equivalent like diploma, 4 had a Ph.D. and 3 had an alternative educational degree.

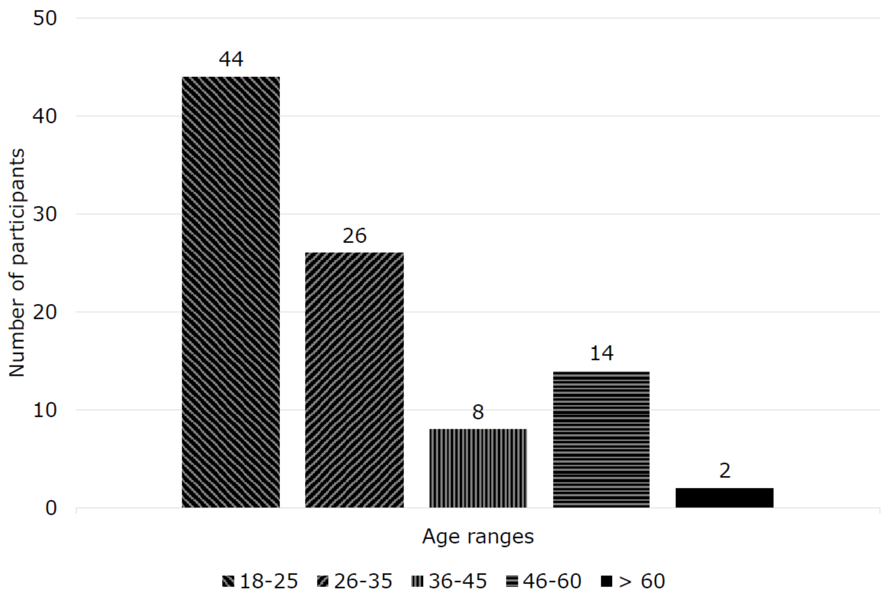

Figure 7.12: Threat appraisal approach: Participants' age range.

7.3.4. Results

The findings of the experiment are presented in Figure 7.13 and 7.14. While Figure 7.13 presents participants' agreement regarding the secrecy concerns stated in the previous study, before the threat appraisal approach, Figure 7.14 presents those after. Note that nine participants were negatively influenced by the threat appraisal approach, i.e. they rather agreed with the secrecy concerns stated in the previous study. While 38 participants did not change their opinion, 47 participant were positively influenced by the threat appraisal approach, i.e. they rather disagreed with the secrecy concerns stated in the previous study.

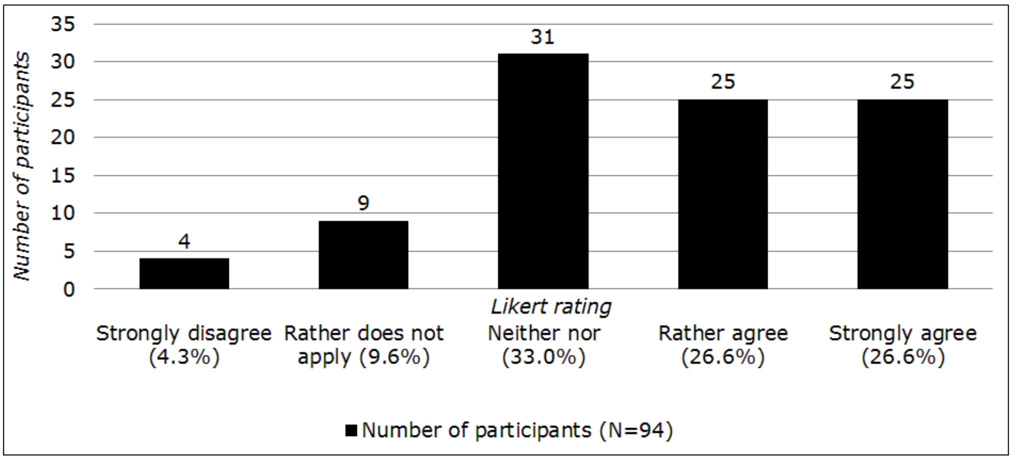

Figure 7.13: Threat appraisal approach: Participants' agreement regarding secrecy concerns about QR-Codes (before).

In order to measure the effect of the threat appraisal approach with respect to the presented concerns, we used the Wilcoxon signed-rank test. Note that we selected a non-parametric statistical test, because the data was collected by using an ordinal scale, namely a Likert scale, refer to section 6.1. The test suggested that the threat appraisal approach significantly allayed participants' concerns regarding QR-Codes ($Z = -4.245, p < .001$).

7.3.5. Summary, outlook and limitations

The findings of our study revealed that the threat appraisal approach has a significant effect regarding the allay of secrecy concerns in association with QR-Codes. These findings suggest that the threat appraisal approach of the protection motivation theory is a promising approach to address secrecy concerns in the context of electronic voting, in particular regarding QR-Codes. Based on these findings and the

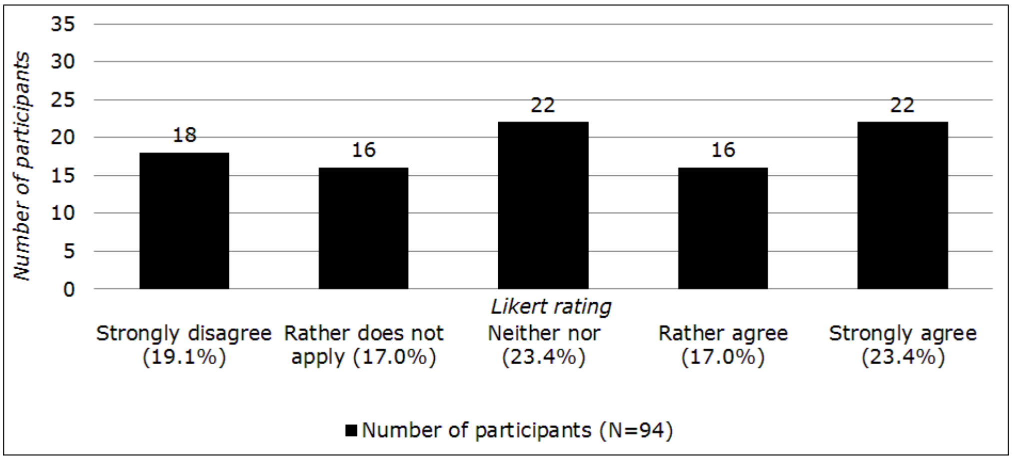

Figure 7.14: Threat appraisal approach: Participants' agreement regarding secrecy concerns about QR-Codes (after).

fact that QR-Codes do not represent an additional risk regarding vote secrecy, we recommend the use of QR-Codes to enable a semi-automatic tallying of the ballots.

It is important to note that most of the participants in our experiment were relatively young, and therefore may not be representative of the larger voting population. Furthermore, due to the adopted study design (within-group), fatigue might have also slightly influenced our findings. However, we addressed this issue carefully, by requiring participants to complete only a single task, while the entire experiment could be completed in less than 30 minutes. Last, but not least, as the presented concerns were rather external than participants' own thoughts, this might have slightly influenced our findings regarding the impact of the threat appraisal approach on participants' secrecy concerns.

While our findings provide important baseline data and novel directions on addressing and allaying voters' secrecy concerns in the context of electronic voting, future work should address the limitations of the reported study. In particular, more research is needed to better understand voters' mental models with respect to new voting technologies in relation to trust, secrecy and integrity concerns. Furthermore, future work should also investigate whether secrecy concerns' regarding QR-Codes correlate with voters' readiness to use EasyVote in legally binding elections.

8 Improving and evaluating the EasyVote ballot design

The goal of this chapter is to identify an EasyVote ballot design, which enables voters to understand the impact of their selections and to verify their voting intention easily.

To achieve this goal, we proposed three alternative EasyVote ballot designs, which build upon the design proposed by Jöris [Jör13], refer to section 5.2.1. Further, we conducted an online experiment to evaluate the three alternative designs with respect to *understandability*, i.e. whether voters understand the impact of their selections (how their cast votes are tallied), and *verifiability*, i.e. whether voters can verify their cast vote easily.

The content of this chapter has been published at the *6th International Conference on Electronic Voting* [5].

8.1. Improving the EasyVote ballot design

As stated by the National Institute of Standards and Technology, the design of ballots (paper and/or electronic) is a complicated challenge [LAC+04]. This challenge becomes even more complicated in the context of complex elections, i.e. elections with complex voting rules and huge ballots. The main challenge in such a context is to develop an optimal ballot design that enables voters to understand the impact of their selections [VBD11], and to verify their voting intention easily [HBV14].

To the best of our knowledge, there is a single work [Jör13] which proposes a ballot design for complex elections. The main advantage of this proposal, presented in Figure 5.3 in section 5.2.1, is that it complies with the most well-known recommendations for ballot designs. For instance, language clarity [RL09], ballot (paper audit trail) usability [ELE15], design consistency [NKQC08] and font type (size, alignment and style) [Ame16]. Nevertheless, this proposal makes it difficult for voters to verify their voting intention, because it does not explicitly distinguish between votes that are directly cast, and votes that are assigned to candidates automatically, due to the selection of a party. Furthermore, as the QR-Code encodes the entire information contained on the human-readable ballot component, i.e. it does also not distinguish between votes that are directly cast and votes that are assigned automatically, this ballot design reflects the voter's intention ambiguously. Figures 8.1 and 8.2 present two ballots, which are identical with respect to the human-readable voter's selections (denoted with **(1)**) and the information encoded in the QR-Code (denoted with **(2)**), except for the composition of the cast votes (denoted with **(3)** and **(3')**).

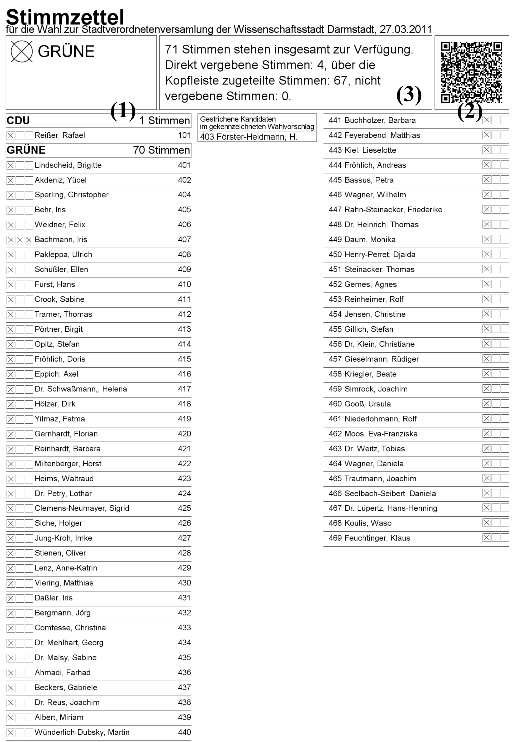

Figure 8.1: EasyVote ballot: First composition.

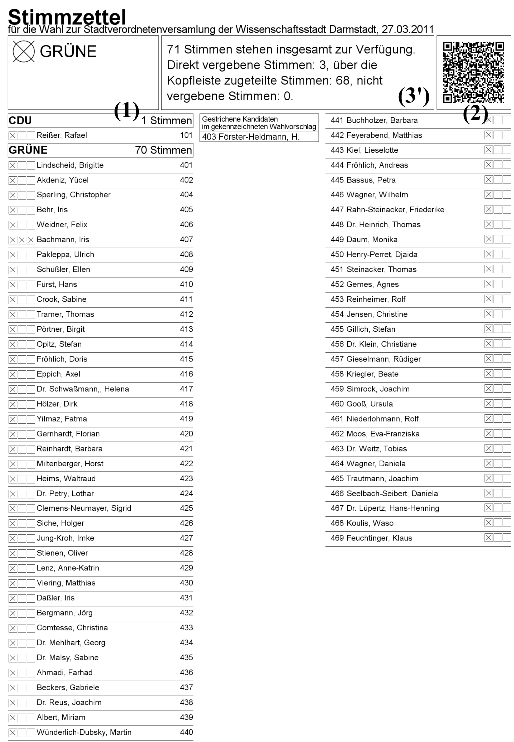

Figure 8.2: EasyVote ballot: Second composition.

To improve the situation we propose three alternative ballot designs, shown in Figures 8.3, 8.4 and 8.5.

In order to solve the problem of ambiguity, we propose that, in general, QR-Codes encode only voters' direct selections, including the crossed out candidates. This modification requires an adaptation of the EasyVote vote casting and tallying prototypes. Furthermore, the tallying prototype should implement the algorithm to distribute votes in dependence of voters' direct selections automatically, rather than

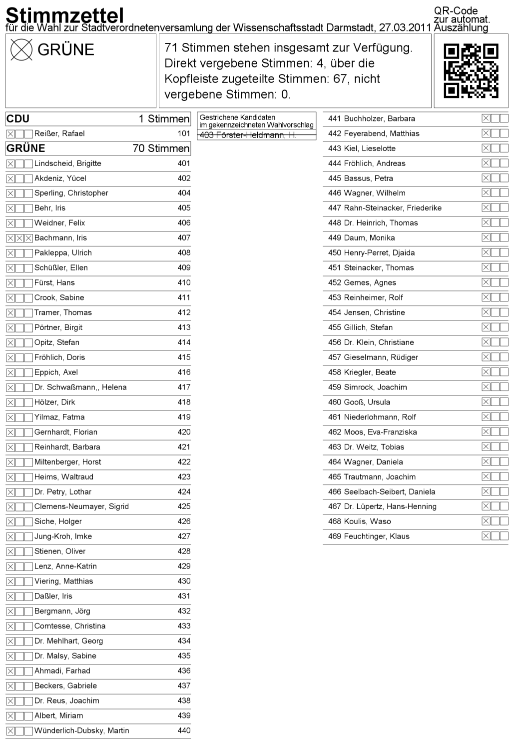

Figure 8.3: EasyVote ballot: Black-and-white.

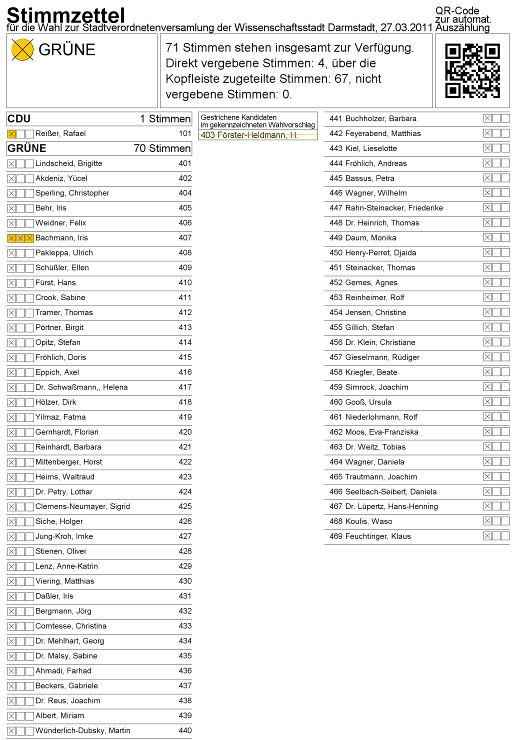

Figure 8.4: EasyVote ballot: Hybrid orange.

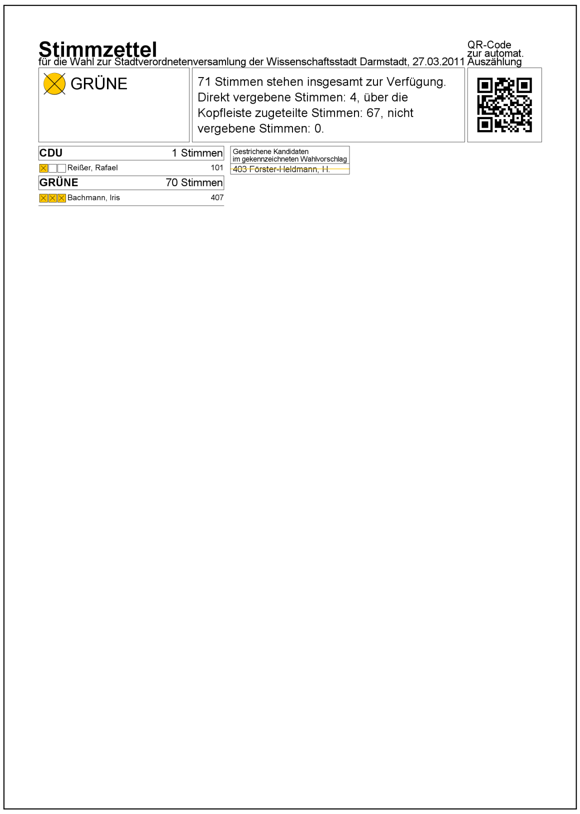

Figure 8.5: EasyVote ballot: Compact orange.

only relying on the data stored in the QR-Codes. It is important to emphasise that this modification improves the overall security of the EasyVote scheme by enforcing the principle of separation of duty regarding the vote casting and tallying device. In addition, for the sake of clarification we added a short text description on top of the QR-Code and a strikethrough on the crossed out candidates. Note that with the exception of these improvements, the first alternative, the *Black-and-white* ballot design, is similar to the ballot design introduced in section 5.2.1.

Furthermore, to improve the ease of verification the second (*Hybrid orange*) and third (*Compact orange*) alternative designs use colour. According to Braun and Silver [BS95], the colour red conveys the highest level of perceived hazard followed by orange, black, green and blue. In addition, Young and Wogalter [YW90] found that with respect to memory times print highlighted with orange was better remembered than non-highlighted text. Moreover, since red is problematic for a significant percentage of the male population due to colour blindness, orange seems the best choice. Therefore, both alternatives highlight voters' direct selections in orange, and imply that voters verify only the highlighted selections. Last, but not least, the *Compact orange* ballot design simplifies things even further, because it contains only voters' direct selections. It is important to note that this design contains the same amount of information as the ballot in the paper-based election. Therefore, it might be inferior compared to the *Black-and-white* and *Hybrid orange* ballot designs with respect to understandability. Note that by introducing colour the vote casting and tallying prototypes need to be adapted. While the vote casting prototype should highlight (on the review screen) and print voters' direct selections in orange, the tallying prototype should also highlight voters' direct selections in orange. Finally, a colour printer is necessary.

While the next section evaluates the proposed alternative ballot designs regarding *understandability* and *verifiability* of the cast vote, Table 8.1 presents a hypothetical comparison thereof. This comparison is based on the above arguments, namely that the *Hybrid orange* and *Compact orange* ballot designs improve the ease of verification and that the *Compact orange* lowers understandability.

8.2. Evaluating different EasyVote ballot designs

In this section we evaluate the EasyVote ballot designs, proposed in the previous section, with respect to *understandability*, i.e. whether voters understand the impact of their selections (how their cast votes are tallied), and *verifiability*, i.e. whether voters can verify their cast vote easily. Furthermore, based on the hypothetical

Table 8.1: EasyVote ballot: Comparison of the different EasyVote ballot designs.

	Understandability	Verifiability
Black-and-white vs. Hybrid orange	$=$	$<$
Black-and-white vs. Compact orange	$>$	$<$
Hybrid orange vs. Black-and-white	$=$	$>$
Hybrid orange vs. Compact orange	$>$	$=$
Compact orange vs. Black-and-white	$<$	$>$
Compact orange vs. Hybrid orange	$<$	$=$

Note that $A = B$ means that ballots A and B are equal regarding the respective criterion. Further, while $C < D$ means that ballot D is better than ballot C, $E > F$ means that ballot E is better than ballot F regarding the respective criterion.

comparison in Table 8.1 we define the following hypotheses:

Hypothesis U_1: There is no significant difference between the *Black-and-white* and *Hybrid orange* ballot designs with respect to understandability.

Hypothesis U_2: The *Black-and-white* and *Hybrid orange* ballot designs are significantly better than the *Compact orange* design with respect to understandability.

Hypothesis V_1: There is no significant difference between the *Hybrid orange* and *Compact orange* ballot designs with respect to verifiability.

Hypothesis V_2: The *Hybrid orange* and *Compact orange* ballot designs are significantly better than the *Black-and-white* design with respect to verifiability.

While hypothesis (U_1) is derived from the first and third row (left column), hypothesis (U_2) is derived from the fifth and sixth row (left column) of Table 8.1. Further, while hypothesis (V_1) is derived from the fourth and sixth row (right column), hypothesis (V_2) is derived from the first and second row (right column) of Table 8.1. Note that in all defined hypotheses the independent variable is the type of ballot design, and the dependent variables are *understandability* and *verifiability* of the cast vote.

8.2.1. Overview

In this section we describe the design, setting and evaluation methodology of the user study.

Design

The main purpose of the study was to test the defined hypotheses. To achieve this goal we conducted an online experiment.

In the experiment participants were first introduced to the actual research goal, namely to actively feed into the EasyVote voting scheme, in particular with respect to the ballot design, by following the human-centred design principles for interactive systems [Int10]. Next, participants were introduced to the EasyVote voting scheme, more specifically to the vote casting process. Further, to assess participants' understanding regarding the vote casting process, we required them to negate or approve the following statements:

1. The vote is cast by manually marking candidates on the paper ballot.
2. The vote is cast purely electronically.
3. A ballot is printed at the end of vote casting. However, this ballot serves only for own verification.
4. A ballot is printed at the end of vote casting. The ballot represents the cast vote.

Note that these statements served to filter out those participants, that did not take the necessary time to become familiar with the vote casting process. Afterwards, participants were presented with a textual description of a cast vote, which is introduced below. At this step, participants were also presented with the three ballot designs simultaneously. Finally, participants were required to rank the three ballots with respect to *understandability* and *verifiability* of the cast vote.

Textual description of the cast vote: Imagine you go to the next local elections and use the EasyVote voting system to cast your vote. After you identify yourself to the electoral officials, you enter the voting booth. Next, you start casting your vote **by selecting the SPD party**. You are good friends with **Sabine Seidler and Rita Beller of the SPD** party and therefore assign both of them **three direct votes**. **You cross out Dagmar Metzger from the SPD** party, as you can not stand her. You support your neighbours **Brigitte Lindscheid und Christopher Sperling from the GRÜNE** party and assign each of them **three direct votes**. You agree with the ballot shown on the review screen and click on finish. Finally, EasyVote prints your ballot.

Note that in the description we used short sentences for better reading comprehension [FP96], and set keywords in bold to improve information cognition [Mar13]. Finally, based on our hypotheses and participants' task, which is less susceptible to the learning effect and involves substantial human cognitive and perceptual capabilities (information retrieval), we adopted a basic within-groups design to diminish individual differences effectively.

Setting

To create the online experiment we used the SoSci Survey online platform, refer to section 6.2.

Evaluation methodology

To measure the dependent variables, namely *understandability* and *verifiability*, we compared the participants' rankings of the different ballot designs. Finally, to determine the confidence of our measurements we ran a respective significance test.

8.2.2. Procedure

The experiment consisted of the following sequential steps:

1. Participants read and confirmed (clicked on the checkbox) the declaration of consent for participating in the experiment.

2. Participants read the goal of the experiment.

3. Participants became familiar with the EasyVote vote casting process.

4. Participants indicated their opinion on four general statements regarding the vote casting process.

5. Participants read the textual description of a sample cast vote.

6. Participants ranked the three ballot designs with respect to *understandability* and *verifiability* of the cast vote.

7. Participants provided their demographics (age range, gender and education).

8.2.3. Participants: Recruitment, incentives and sample

The participants were recruited via e-mail, advertising in social networks, flyers and by personal contact. No incentives were provided, thus participation was purely voluntary.

In total 87 subjects participated (35 female, 48 male, 4 others) between the ages of 19-75 years, with an average age of 36.15 years ($s = 14.4$) and a median age of 40. We removed 14 participants (3 female, 9 male, 2 others), because they did not answer the statements with respect to the EasyVote vote casting process correctly. The remaining 73 subjects (32 female, 39 male, 2 others) aged 19-65, with an average age of 35.37 years ($s = 13.79$) and a median age of 30, comprised one participant with apprenticeship, four with a Ph.D. degree, five with middle school qualification, seven with a B.Sc. degree, seven with a technical college qualification, eight with a vocational education, 15 with a Diploma/M.Sc. degree and 26 with a high school qualification.

8.2.4. Results

Figures 8.6 and 8.7 summarise the results of our experiment.

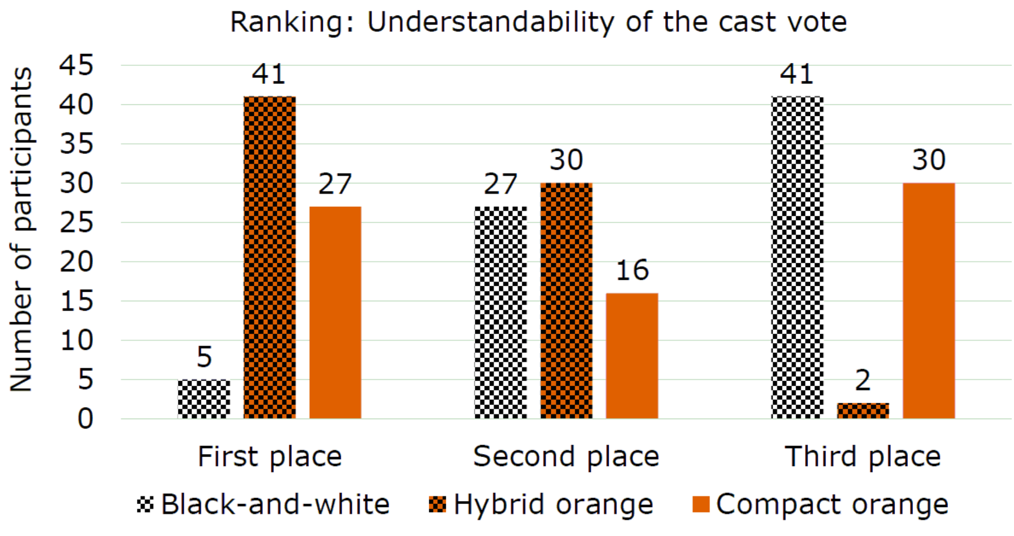

Figure 8.6: Participants' ranking regarding understandability of the cast vote.

In order to measure the significance of our findings, presented in Figure 8.6 and 8.7, we used the Wilcoxon signed-rank test. Note that we selected a non-parametric statistical test, because the data was collected by using an ordinal scale, refer to section 6.1.

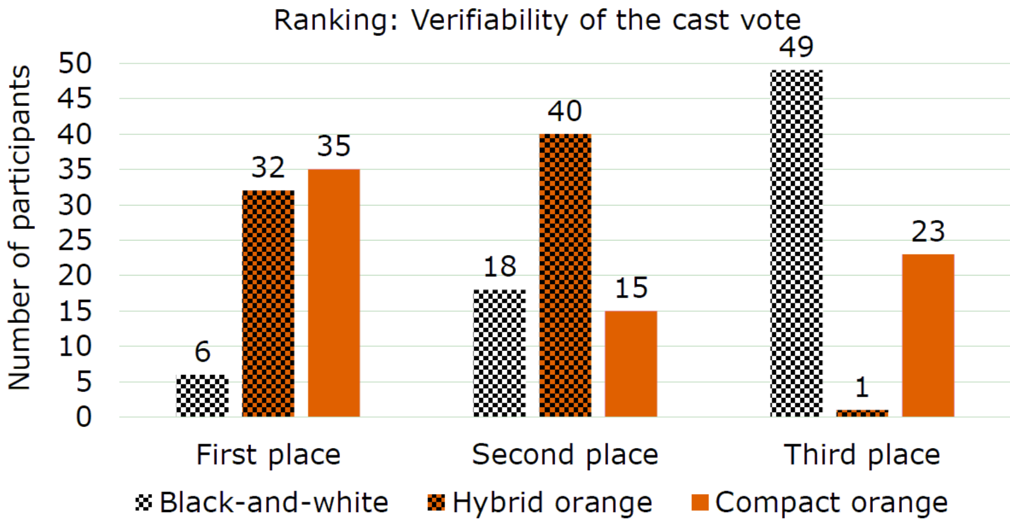

Figure 8.7: Participants' ranking regarding verifiability of the cast vote.

The test revealed that the *Hybrid orange* ballot design is significantly better than the *Black-and-white* design regarding both understandability ($Z = -6.722$; $p < .001$), and verifiability of the cast vote ($Z = -6.722$; $p < .001$). Similar, the test suggested that the *Compact orange* ballot design is significantly better than the *Black-and-white* design regarding both understandability ($Z = -2.891$; $p < .004$), and verifiability of the cast vote ($Z = -4.205$; $p < .001$). Further, the test revealed a significant difference between the *Hybrid orange* and the *Compact orange* ballot designs regarding understandability of the cast vote ($Z = -3.673$; $p < .001$) with a higher rank sum for the *Hybrid orange* design (1993.50). However, no significant difference was found between these designs regarding verifiability of the cast vote ($Z = -1.945$; $p < .052$).

8.2.5. Discussion and limitations

The study only partially confirmed our defined hypotheses. The findings did not confirm hypothesis (U_1), because the *Hybrid orange* ballot design is significantly better than the *Black-and-white* with respect to understandability. Further, the findings partially confirmed hypothesis (U_2), because only the *Hybrid orange* ballot design is significantly better than the *Compact orange* design regarding understandability. It is important to emphasise that these findings indicate that the use of colour (orange) also improves understandability. In addition, the findings confirmed hypothesis (V_1), because there is no significant difference between *Hybrid orange* and *Compact orange* ballot designs with respect to verifiability. Last, but not least, our findings validated hypothesis (V_2), revealing that the *Hybrid orange* and *Compact orange* ballot designs are significantly better than *Black-and-white* design regarding verifiability. In summary, the findings of our study indicate that the *Hybrid orange* ballot design represents an optimal design with respect to understandability and verifiability of the cast vote. Consequently, we recommend the use of this ballot design for EasyVote.

It is important to mention that these findings do not only induce design (interfaces) modifications, but also concept modifications that might improve the efficiency and accuracy (security) of EasyVote. For instance, voters that are familiar with the voting rules, i.e. those that would not necessarily need support with respect to understanding the impact of their selections, could only verify their direct selections (highlighted in orange). Furthermore, in the tallying process, electoral officials could also verify only voters' direct selections. Nevertheless, even though the algorithm for distributing votes automatically is implemented by both the vote casting and tallying device, and is also publicly known, we recommend that electoral officials perform random audits. This means that for a random set of ballots, electoral officials should verify the correctness of the algorithm for distributing votes automatically and also that scanned ballots are added correctly to the intermediate result. This significant reduction of the number of comparisons for both voters and electoral officials might also improve accuracy, as potential discrepancies may be easier to detect. In the following chapters, in particular with respect to the tallying process, we explore the impact of these improvements regarding efficiency and accuracy.

Note that our findings might be slightly susceptible towards a sample selection bias, because our sample may not be representative of the larger voting population. Furthermore, due to the adopted study design (within-group), fatigue might have also slightly influenced our findings. Nevertheless, in our opinion we addressed the issue of fatigue carefully, by requiring participants to complete only a single task. Last, but not least, the entire experiment could be completed in less than 7 minutes.

9 Developing & evaluating verification instructions and usability: Voters' perspective

The main goal of this chapter is to develop verification instructions that make voters most likely to verify that their ballot matches their intention. In addition, this chapter aims to evaluate the usability of the implemented EasyVote prototype.

To achieve this goal, we developed verification instructions by considering the context constraints, the medium of delivery, the position, the time and the design of such instructions. Further, we identified the most appropriate approach for evaluating the effectiveness of verification instructions with respect to ballot verification. Finally, we conducted a laboratory experiment to evaluate the developed instructions and the usability of the implemented EasyVote prototype from the voters' perspective, i.e. the usability of the vote casting process.

The content of this chapter has been published at the *Workshop on Usable Security* [11] and the *Journal of Annals of Telecommunications* [1].

9.1. Developing verification instructions

To ensure the integrity of cast votes, EasyVote, similar to all electronic voting schemes/systems that provide voters with paper audit trails (printed ballots), for instance [SMA16, Ben06, Ben07, Cha04, WV08, BCH+12, BFL+12, Veg12, BBE+13, Boa14, Vot08], assumes that voters act to verify that their ballot matches their intention. Nevertheless, previous studies, namely [Sel04, Coh05, HNH+05, mar06, SP06], reveal that this assumption does not hold true, even though such study participants often consider paper audit trails to be important [MSG+11]. Therefore, the goal of this section is to improve the situation by developing verification instructions that make voters most likely to verify their ballot, i.e. to detect potential discrepancies.

In order to achieve this goal, we first define the constraints for providing voters with verification instructions, in particular by considering the context addressed in this dissertation. Next, we discuss the medium for delivering such instructions, and identify the most appropriate one. Further, we investigate and determine the appropriate time and position for providing voters with such instructions. Finally, we also improve the design of the verification instructions.

9.1.1. Context constraints

In contrast to paper-based elections, where voters manually mark their preferred candidates/parties on a paper ballot, in electronic voting voters perform an additional step to ensure the integrity of cast votes, namely they verify that their vote has been cast-as-intended. To inform or rather make voters to verify, so-called verification instructions are used. Hence, the aim of such instructions is to ensure the integrity of cast votes. Therefore, the integrity of verification instructions should be ensured without relying on the trustworthiness of the electronic voting device. Displaying the verification instructions on the screen of the voting device is inappropriate. A malicious or faulty device might not only alter the printed ballot, but could also display incorrect verification instructions, for instance "Thank you for voting. Deposit the ballot into the ballot box." Similar problems might occur when verification instructions are printed on the ballot together with the voters' selections. Last, but not least, to ensure election integrity, i.e. the integrity of all cast votes, verification instructions should be provided to all voters. Based on these arguments we define the following constraints:

1. Verification instructions should not only be displayed on the screen of the electronic voting device.
2. Verification instructions should not be printed together with the voter's selections.
3. Verification instructions should be provided to all voters.

Note that such constraints are context-dependent. For instance, the above list may not be sufficient when considering visually impaired voters.

9.1.2. Medium of delivery

There are many different tools (media) which can be considered for informing voters about the use of the electronic voting scheme/system, in particular about the verification step (instructions). In the following we list the most popular:

- Television news.
- Radio news.
- Internet news.
- Social networks.
- Newspapers.
- Academic research papers/journals.
- Public debates.
- Blogs/Forums.
- Non-governmental organisations.
- Governmental institutions.
- Election guidelines.
- Election notification.
- Polling stations.

Nevertheless, when delivering important information to voters, such as the verification instructions, the standard guidelines by Help America Vote Act (HAVA) [ELE15] recommend that:

1. The verification instructions are publicly available.
2. The verification instructions are accessible to all voters.
3. The verification instructions are standardised with respect to their content.

In order to meet the first recommendation, the verification instructions should be provided in the respective polling station. Further, to meet the second recommendation, the verification instructions should be included in the election notification. Note that in Germany the election notification is very often used to identify and authorise voters. Therefore, we assume that all voters have access to the verification instructions. Finally, to meet the third recommendation, the verification instructions should be provided in written form, because there already exist standard guidelines for written instructions, refer to [RL09, Ame16].

9.1.3. Time, position and design

According to Nielsen [Nie94], "...instructions should be visible or easily retrievable whenever appropriate." This indicates that verification instructions should be provided in the voting booth (*position*). Further, in the context of electronic voting, Redish *et al.* [RL09] recommend that "...instructions must come "just in time" – when voters need them." This indicates that the verification instructions should be provided in the vote casting process (*time*).

In order to identify the appropriate *position* and *time* we conducted a number of pre-tests with the following different approaches:

1. Posters on the screen.
2. Posters on the printer.
3. Front of the ballot.
4. Reverse of the ballot.

In the pre-tests we observed whether participants verified the printed ballot, i.e. whether they detected the deliberately introduced manipulation. We carried out some informal interviews afterwards. Based on these pre-tests, the most appropriate approach was number four. Hence, participants seeing first the verification instructions, and then turning the ballot to verify its content. It is important to emphasise that to ensure the integrity of the verification instructions, the instructions were pre-printed.

Furthermore, through the pre-tests and with the aid of a designer[21] we improved the design of the verification instructions should. This led to a design consisting of two pictures, shown in Figures 9.1 and 9.2, accompanied by two main sentences and one auxiliary sentence:

First main sentence: **Verify** the correctness of the **orange marked** **selections** on the rear.

Auxiliary sentence: In case of mistakes please contact the electoral officials.

Second main sentence: **Fold** the printed ballot **twice**.

[21] The designer works as a student assistant at the author's research group, and studies at the University of Applied Sciences Darmstadt in the Faculty of Design, Industrial Design & Communication Design.

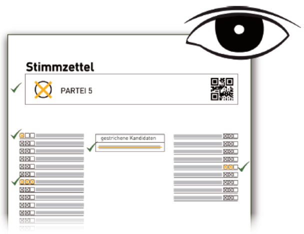

Figure 9.1: Voters' perspective: The picture associated the first main sentence.

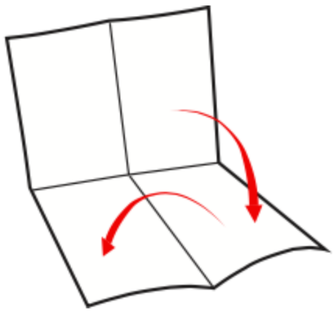

Figure 9.2: Voters' perspective: The picture associated the second main sentence.

The design of the verification instructions is based on established research results. Pictures and short sentences are used for better reading comprehension [FP96], and keywords are underlined and set in bold to improve information cognition [Mar13]. Furthermore, instructions are set in a logical order and written in plain language, as recommended in the respective standard guidelines, namely [LR06], [RL09] and [Ame16]. No words are emphasised in the auxiliary sentence, in order not to weaken the effect of the two main sentences. Note that even though our focus is on integrity of cast votes, we included the second main sentence to avoid that voters forget to fold their ballots and thereby violate vote secrecy accidentally.

As the verification instructions presented in the appropriate time and position should make (stimulate) voters more likely to verify their ballot, in the following we refer to the verification instructions developed in this section (time, position and design), as the *stimulus*.

9.2. Evaluation approaches

In previous studies [Sel04, Coh05, HNH$^+$05, mar06] and [SP06], which investigated whether voters act to verify that their ballot matches their intention, two different approaches were used:

1. Ballot manipulation [Coh05, SP06].
2. Time observation [HNH^{+}05, mar06, Sel04].

Furthermore, another approach that can be used to investigate whether voters act to verify that their ballot matches their intention, is the approach used by Olembo *et al.* [ORBV14], namely participants' self-reports. Even though this approach was used in a different setting (Internet voting) and with a different goal, namely to explore the effects of motivating messages on voters' intention to verify their vote by using a smartphone app, it can also be applied in the context of this dissertation.

In the following we describe and report the results of the previous studies, which are related to the electronic voting context considered in this dissertation. Afterwards, we compare the advantages and disadvantages of the three different approaches, namely ballot manipulation, time observation and participants' self-reports, to identify the most appropriate one.

9.2.1. Ballot manipulation

One of the goals in the study conducted by Cohen [Coh05] was to evaluate the effectiveness, specifically whether participants were able to detect manipulations on the paper audit trail, of the Low Error Voting Interface [SHGS05]. In the study, participants were required to cast a vote in four elections by following a voting agenda, i.e. voting for a pre-defined list of candidates and/or parties. In three of the four elections, the paper audit trail was altered and one of the following manipulations was randomly introduced:

1. Change a vote to a different candidate.
2. Remove a vote from a candidate.
3. Remove a complete contest.

While instructions regarding the use were provided in the voting booth and also by the voting device, instructions regarding ballot verification were displayed on the final voting screen. Finally, the results revealed that only two out of 36 participants, recruited from the MIT community, actually verified their paper audit trail and detected the introduced manipulation.

Similar to Cohen [Coh05], one of the goals in the study conducted by Selker and Pandolfo [SP06] was to check whether participants verified and detected manipulations on the paper audit trail of the MIT voting prototype. In the study participants were required to cast a vote by following a voting agenda with 13 contests. While the list of candidates was determined for nine of the contests, participants could chose their preferred candidates in the remaining ones. The paper audit trail was altered and the following two manipulations were deliberately introduced:

1. Change a vote to a different candidate.
2. Remove a vote from a candidate.

Participants were given verbal instructions regarding ballot verification and the use of the prototype outside the voting booth. Finally, the results revealed that only six out of 35 participants, all eligible voters of Arlington town in Massachusetts, actually verified their paper audit trail and detected the introduced manipulations.

9.2.2. Time observation

One of the goals in the study conducted by Herrnson *et al.* [HNH+05] was to evaluate the usability of a voting device with paper audit trails, namely the Avante Vote-Trakker. In the study participants were required to vote by following a voting agenda. While instructions regarding the use of the system were given verbally outside the voting booth, participants were also explicitly required to pay attention to the paper audit trail. Furthermore, verification instructions were displayed on the final screen of the voting device. Finally, the results revealed that most of the 1536 participants, recruited from university student bodies, maintenance staff, community centres, etc., ignored the paper audit trails, i.e. they did not take the time to verify their content.

Similar to Herrnson *et al.* [HNH+05], one of the goals in the study conducted by The Center for American Politics and Citizenship (CAPC) [mar06] was to evaluate the usability of the Diebold AccuVote-TSx with AccuView Printer Module voting system, which provides voters with paper audit trails. In the study participants were required to vote by following a voting agenda. While instructions regarding the use of the system were given verbally outside the voting booth, participants were also explicitly required to pay attention to the paper audit trail. No verification instructions were provided by the voting device. Finally, the results revealed that most of the 804 participants, recruited from shopping malls, office buildings, college campuses, etc., did not take the time to verify their paper audit trail.

Last, but not least, Selker [Sel04] reports that during the legally binding elections in Reno, Nevada September 7th, 2004, many voters did not take the time to verify their ballot. Note that only in one out of the 36 observed polling stations, voters were provided instructions regarding the use of the voting system. However, no differences with respect to voters' behaviour regarding ballot verification are reported.

9.2.3. Comparison of the different approaches

The main advantage of the ballot manipulation approach is that it allows to unambiguously determine whether participants (voters) verify their ballot and detect potential discrepancies (manipulations). In contrast, relying on the observation of the time that participants spend in the voting booth after the ballot is printed, does not allow to unambiguously determine whether participants verify their ballot and detect potential discrepancies. Participants' self-reports might produce similar, unreliable results to the time observation approach. However, some researchers have found evidence that intention and behaviour are related [VEOS13], and that behavioural intention is antecedent to actual behaviour [LUB+13].

Based on these arguments, we suggest the use two evaluation approaches simultaneously, namely the ballot manipulation and participants' self-reports approaches.

9.3. Evaluating the verification instructions and usability

The main goal of this section is to evaluate the effectiveness of the developed *stimulus* (time, position and design of the verification instructions) with respect to making voters to verify their ballot, i.e. to detect potential discrepancies. We focus on the local elections in Darmstadt, and define the following hypothesis:

Hypothesis: The *stimulus* has a significant effect with respect to making voters to verify their ballot and thus detect potential discrepancies.

The independent variable is the *stimulus*, and the dependent variable is the ratio of detected discrepancies. Note that even though our main focus is on integrity of cast votes, we also measure the effect of the *stimulus* regarding vote secrecy, more specifically whether voters fold their ballot or not. Further, we compare the used evaluation approaches (ballot manipulation and participants' self-reports) regarding the reliability of their results. Thus, we compare whether the participants' self-reports approach is as reliable as the ballot manipulation approach with respect to unambiguously determine whether voters verify their ballot and detect potential discrepancies. In addition, poor usability is shown to "violate" election integrity, for instance by influencing the election outcome [NKQC08] or by significantly decreasing voter turnout [THhP+05]. Therefore, in this section we also evaluate the usability of the EasyVote (the implemented prototype) vote casting process according to the ISO 9241-11 standard [Int98]. Last, but not least, motivated by the research directions proposed in section 7.3.5, in particular regarding voters' mental models with respect to integrity concerns, we explore participants' perceptions towards ballot verification. Note that to the best of our knowledge, this is the first work to address these issues regarding electronic voting in the context of complex elections.

9.3.1. Overview

In this section we describe the design, methodology to introduce manipulations, setting, questionnaires and evaluation methodology of the user study.

Design

The main purpose of the study was to test the defined hypothesis. To achieve this goal we conducted a laboratory experiment.

In the experiment participants were required to cast a vote with EasyVote in an election forecast of the forthcoming local election in Darmstadt. Thereby, we intentionally and randomly manipulated each participant's ballot. Further, to simulate a realistic voting scenario, i.e. to induce a personal relevance to the ballot, in contrast to previous, related studies [Sel04, Coh05, HNH+05, mar06, SP06], participants were free to select their preferred candidates and/or parties.

In addition, to avoid potential social desirability bias, see section 6.2, participants were given a fictitious research goal. Thus, participants were told that they are taking part in a research experiment, which emerged from a collaboration between the computer science and political science departments at the *Technische Universität Darmstadt*. The stated research focus was said to be twofold:

1. The political science department is interested in the development of democracy in Germany. Hence, the research experiment aims to compare citizens' interest and motivation to actively participate in politics. The experiment claims to conduct a comparison between citizens involved in the 1960s protest movements and the citizens of today. To achieve this goal participants are asked to cast a vote in an election forecast of the forthcoming local elections in Darmstadt. Furthermore, to strengthen the credibility of this research focus, we used real candidates and parties.

2. The computer science department is interested in evaluating the usability of the implemented EasyVote prototype.

Further, based on our hypothesis and participants' task, which is highly susceptible to the learning effect, we adopted a basic between-groups design. Hence, the experiment consisted of two groups:

1. The treatment group.
2. The control group.

While the treatment group got the *stimulus*, the control group got the verification instructions as part of the experiment guidelines, simulating voters that get the verification instructions as part of the election notification. Finally, to exclude the turning of the printout (printed ballot) as the cause to verify its content, participants in the control group were confronted with the blank side of the printout.

Introducing manipulations: Altering the printed ballot

In the experiment we manipulated the ballot of each participant intentionally. We used the following manipulations:

1. Exchange a party, including its candidates.
2. Exchange a crossed out candidate.
3. Exchange a directly selected candidate.
4. Exchange votes between directly selected candidates.

The second and fourth manipulation changed only the distribution of cast votes. The first and third manipulation introduced new content into the printed ballot, for instance a new party and/or a new candidate. Note that these manipulations were also used in similar, previous studies [Coh05, SP06, Eve07].

Furthermore, we introduced the manipulations in a pseudo-random fashion, rather than truly random. This means that we always introduced a single manipulation from the above list in dependency of the participants' direct selections. If manipulations are introduced truly at random, they might be very easy to detect. For instance, if the participant selects only a party, the introduced manipulation cannot be the second, third or fourth, otherwise the manipulation is very obvious. Such a manipulation methodology, i.e. introducing manipulations truly at random, wouldn't simulate the behaviour of a real world adversary, whore aim is to manipulate the election outcome without being detected. Otherwise, this would bias our findings and lead us to false conclusions. Based on the above argument, we did not simply remove or introduce candidates and/or parties, but rather pseudo-randomly exchanged (altered) participants' selections, such that we preserved a similar distribution of directly cast votes, i.e. of orange marked selections. For instance, if the participant selected party X out of 10 parties, we randomly altered participant's selection to party Y from the 9 remaining parties, excluding party X. Note that as all invalid ballots share the same look, refer to section 5.2.1, we refrained to alter such ballots.

Table 9.1 provides on overview of our methodology to introduce manipulations, while considering all possible combinations to fill in a ballot.

The column **Voting options** describes the available options to fill in a ballot according to the strict letter of the voting rules. Note that we do not distinguish between one, two or three directly cast votes, because practically this does not make any difference, if we shall preserve a similar distribution of orange marked selections. For instance, if the participant selects only one candidate and assigns to that candidate either one, two or three direct votes, the selected candidate would be exchanged by preserving the same number of votes assigned by the participant. It is important to emphasise that the voting options, namely select one, several (same votes), several (different votes), are mutually exclusive.

The column **Possible combinations** describes all possible combinations to fill in a ballot according to the strict letter of the voting rules. Thereby, "X" denotes the participant's selection, "(X)" denotes the participant's optional selection, and "–" denotes no selection with respect to the available option.

The bottom column **Manipulations** describes the category of manipulations randomly introduced, depending on the participants' selections. Note that the category of the introduced manipulation is restricted with respect to the ease of detection. For instance, in all combinations where the participant might have selected a party, denoted by "(X)", we refrained from introducing the first manipulation, namely *Exchange a party, including its candidates*.

In the following we describe Table 9.1 in more detail.

1. The participant selects only a party, implying that only the manipulation *Exchange a party, including its candidates* can be introduced.

2. The participant selects only a party and crosses out at least one candidate, implying that only the manipulation *Exchange a crossed out candidate* is randomly introduced.

3. The participant selects only one direct candidate (in combination with selecting a party), implying that only the manipulation *Exchange a directly selected*

Table 9.1: Voters' perspective: Introducing manipulations in a pseudo-random fashion.

Voting options		**Possible combinations**							
		1	2	3	4	5	6	7	8
Select a party		X	X	(X)	X	(X)	X	(X)	X
Select direct candidates	One	–	–	X	X	–	–	–	–
	Several (same votes)	–	–	–	–	X	X	–	–
	Several (diff. votes)	–	–	–	–	–	–	X	X
Cross out candidates		–	X	–	X	–	X	–	X
		1	2	3	2, 3	3	2, 3	3, 4	2-4
		Manipulations							

candidate is randomly introduced.

4. The participant selects one direct candidate, a party and crosses out at least one candidate of the selected party, implying that either *Exchange a crossed out candidate* or *Exchange a directly selected candidate* is randomly introduced.

5. The participant selects direct candidates and assigns them the same number of votes (in combination with selecting a party), implying that only the manipulation *Exchange a directly selected candidate* is randomly introduced.

6. The participant selects direct candidates, assigns them the same number of votes, and selects a party and crosses out at least one candidate of the selected party, implying that either *Exchange a crossed out candidate* or *Exchange a directly selected candidate* is randomly introduced.

7. The participant selects direct candidates and assigns them a different number of votes (in combination with selecting a party), implying that either *Exchange a directly selected candidate* or *Exchange votes between directly selected candidates* is randomly introduced.

8. The participant selects direct candidates, assigns them a different number of votes, and selects a party and crosses out at least one candidate of the selected party, implying that either *Exchange a crossed out candidate* or *Exchange a directly selected candidate* or *Exchange votes between directly selected candidates*

is randomly introduced.

Finally, to identify which manipulation category was introduced in the ballot of each participant, we encoded the respective category in the QR-Code.

Setting

Figure 9.3 provides a general overview of the setting used in the experiment. The experiment took place in our laboratory. It is important to note that we used two ballot boxes, in order to distinguish between participants that detected and those that did not detect the manipulation. One of the ballot boxes was hidden behind the experimenter table.

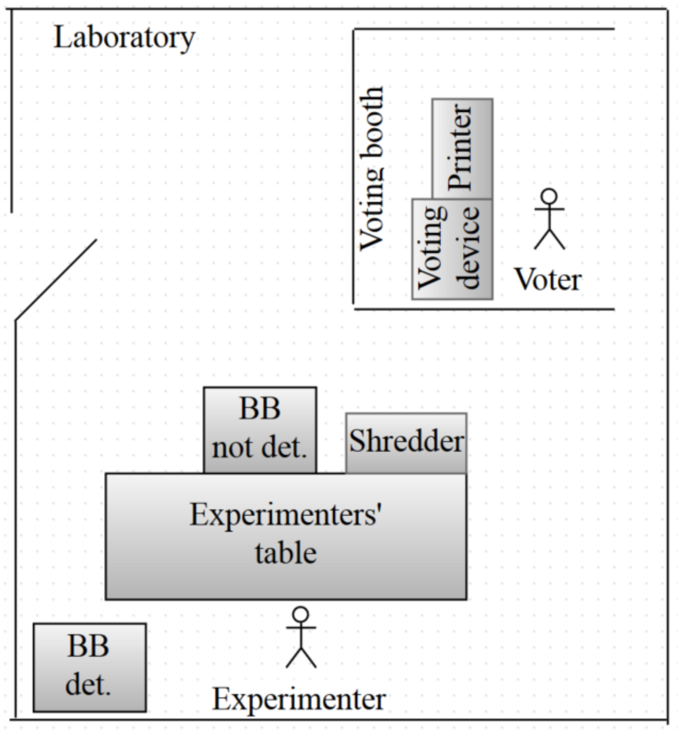

Figure 9.3: Voters' perspective: General overview of the experiment setting.

While Figure 9.4 presents the voting booth from the outside, Figure 9.5 presents the voting booth from the inside.

Further, in the experiment we used an adapted implementation of the EasyVote prototype, introduced in chapter 5. We adapted the prototype with respect to the ballot design, according to the findings in chapter 8. Figure 9.6 presents a sample ballot and the pre-printed verification instructions on the reverse of the ballot. Note

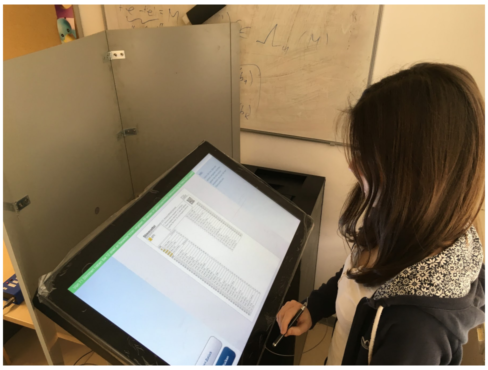

Figure 9.4: Voters' perspective: The inside of the voting booth.

Figure 9.5: Voters' perspective: The outside of the voting booth.

that for the sake of the experiment we exchanged the word "electoral officials" with "experimenter", and adapted the description of the election on top of the ballot.

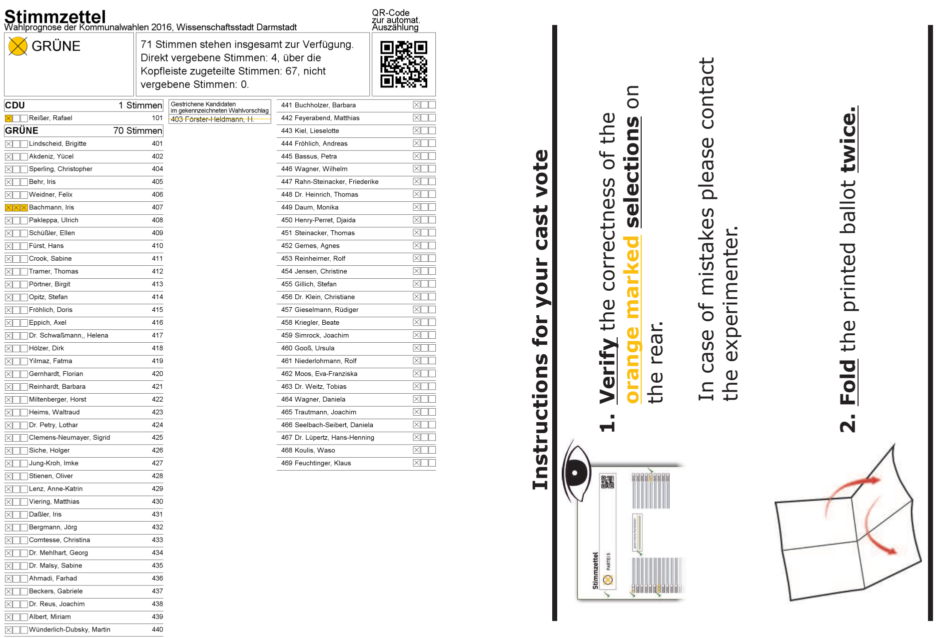

Figure 9.6: Voters' perspective: A sample ballot with the pre-printed verification instructions. (English translation)

In addition, to fulfil the Help America Vote Act (HAVA) standard usability requirements for electronic voting [ELE15], in particular regarding the public availability and standardisation of vote casting instructions, we developed a poster, see Figure 9 in section B in the appendix. To ensure that the instructions were (publicly) available to all participants, i.e. that all participants noticed the instructions and took the time to become familiar with the vote casting process, we hung the poster on the outside, instead on the inside, of the voting booth. This also enabled us to better control the effect of the *stimulus* with respect to ballot verification (detecting manipulations). Last, but not least, to provide participants with standard instructions, the poster was based on the developed verification instructions, refer to section 9.1. In summary, the purpose of the poster was twofold:

1. Instruct participants how to cast a vote with EasyVote.
2. Provide participants with standardised vote casting instructions, to avoid potential social desirability bias that may arise when giving verbal instructions.

Questionnaires

Demographics. This questionnaire served to collect participants' demographic data (gender, age, and education).

Pre-questionnaire. This questionnaire served to measure participants' general interest in politics, and also to conceal our actual research goal.

Post-questionnaire. This questionnaire served to compare the used evaluation approaches, namely participants' self-reports and ballot manipulation. Consequently, the questionnaire contained the following statement:

- I have verified the correctness of the orange marked selections on the ballot.

Furthermore, to assess participants' perceptions towards ballot verification, we added the following statements to the questionnaire:

- I perceived the verification of the printed ballot to be a demanding task.
- I perceived the verification of the printed ballot to be an error prone task.

SUS. This questionnaire served to measure participants' satisfaction with respect to the EasyVote vote casting process.

Evaluation methodology

In the experiment, and therefore also in our evaluation, we distinguish between the following evaluation categories:

1. *Stimulus*: Integrity of cast votes and vote secrecy.

2. Evaluation approach: Ballot manipulation versus participants' self-reports.
3. Usability of EasyVote: Effectiveness, efficiency and satisfaction of the vote casting process.
4. Mental models: Participants' perceptions towards ballot verification.

In the following we introduce the evaluation methodology for each of the above categories.

Stimulus In order to measure the effectiveness of the *stimulus* with respect to integrity of cast votes, i.e to test the defined hypothesis, we manipulated the ballot of each participant, and observed whether she detected the introduced manipulation. Further, to determine the confidence of our measurements we ran a respective significance test. In addition, to measure the impact of the *stimulus* regarding vote secrecy, we took note whether participants folded their ballot after leaving the voting booth.

Evaluation approach In order to compare the evaluation approaches, namely participants' self-reports and ballot manipulation approach, we compared participants' actual behaviour, i.e. whether they detected the manipulation, and their answers on the following statement of the post-questionnaire:

- I have verified the correctness of the orange marked selections on the ballot.

Usability of EasyVote To evaluate the usability of the vote casting process, we defined effectiveness, efficiency and satisfaction according to our context as follows:

Effectiveness: *The ability of participants to cast their vote.* We further specified the task of casting a vote by the following sub-tasks:

1. Participant starts the vote casting process.
2. Participant makes her selections.
3. Participant prints the ballot.
4. Participant verifies that the ballot matches her intention.
5. Participant folds the ballot.
6. Participant deposits the ballot into the ballot box.

We measured effectiveness by observing the vote casting process and filling in a check-list that consisted of these sub-tasks. In case of queries by participants with respect to any of the defined sub-tasks, we denoted that sub-task as not accomplished. Note that the fifth sub-task corresponds to the main goal of our experiment.

Efficiency: *The time participants spent casting their vote.* We further specified the time of vote casting by the following time intervals:

1. Time spent to read the voting rules.
2. Time spent to make selections.
3. Time spent to verify the printed ballot.

To measure the first time interval we used a stopwatch and observed the enabling device. More specifically we measured the time between two events:

1. Participant enters the voting booth.
2. The red LED light of the enabling device turns on.

Further, the EasyVote prototype measured the second time interval, i.e. the time passing between the start of the vote casting process and the start of the printing process. In order to measure the third time interval, we first measured the total time that a participant spent in the voting booth and the average time that the prototype took to print the ballot. Afterwards, we subtracted the time elapsed during the first and second time intervals, and the average printing time from the total time spent in the voting booth.

Satisfaction: *The level of satisfaction participants experienced while casting their vote.* In order to measure satisfaction we used a German translation [LS13] of the original SUS questionnaire [Bro96].

Mental models In order to measure participants' perceptions towards ballot verification, we measured participants' responses, on a five-point Likert scale anchored in "strongly disagree" and "strongly agree", with respect to the following statements of the post-questionnaire:

- I perceived the verification of the printed ballot to be a demanding task.
- I perceived the verification of the printed ballot to be an error prone task.

9.3.2. Procedure

The experiment was carried out in our laboratory. The participants were randomly assigned to the two groups (control and treatment). In the experiment each participant had to perform the following sequential steps:

1. Read and sign the declaration of consent for participating in the experiment.
2. Read the experiment guidelines, which also contained the goal of the experiment.
3. Provide the demographics.
4. Fill in the pre-questionnaire regarding the political interest.
5. Read the poster describing the vote casting process, in order to become familiar with it.[22]
6. Cast a vote and deposit the ballot into the ballot box.
7. Fill in the post-questionnaire.
8. Fill in the SUS questionnaire.
9. Debrief: Reveal the actual research goal.

If a participant detected the manipulation, debriefing took place before filling in the post-questionnaire. Furthermore, in order to ensure vote secrecy, the experimenter instructed participants that did not fold the ballot to fold it before depositing it into the ballot box.

9.3.3. Participants: Recruitment, incentives and sample

Participants were recruited via flyers and by personal contact. In order to encourage participation we provided €10 per participant.

44 subjects participated (14 female, 30 male), ranging in age from 20-75, with an average age of 31.45 years ($s = 13.44$) and a median age of 25. Further, participants had the following educational levels: One participant had completed an apprenticeship; 20 participants had a high school degree or less; and the rest of the participants had a bachelor's degree or equivalent.

[22] Note that if participants had questions regarding the vote casting process while reading the poster, they could ask the experimenter.

9.3.4. Results

We report the findings of our experiment according to the categories defined in the evaluation methodology:

1. *Stimulus*: Integrity of cast votes and vote secrecy.
2. Evaluation approach: Ballot manipulation versus participants' self-reports.
3. Usability of EasyVote: Effectiveness, efficiency and satisfaction of the vote casting process.
4. Mental models: Participants' perceptions towards ballot verification.

Stimulus

The participants in the treatment group detected the randomly introduced manipulations more frequently with 81.81% (18 out of 22) compared to 36.36% (8 out of 22) of participants in the control group. In order to determine if there is a relationship between the categorical variables *stimulus* and manipulation detection among both groups, we ran a Chi-square test. The Chi-square test suggested that there is a significant difference in detecting the manipulation between the treatment and the control group ($\chi^2 = (1, N = 44) = 9.402$, $p < 0.002$).

Furthermore, except for those participants that detected the introduced manipulations, all other participants folded their ballot. To ensure vote secrecy, the experimenter instructed participants that detected the manipulations, to fold and deposit their ballot into the respective ballot box.

Last, but not least, Figure 9.7 provides an overview of the frequency of occurrence for each manipulation category and whether it was detected or not. The manipulation categories, which were considered in the present experiment, are introduced below.

1. Exchange a party, including its candidates.
2. Exchange a crossed out candidate.
3. Exchange a directly selected candidate.
4. Exchange votes between directly selected candidates.

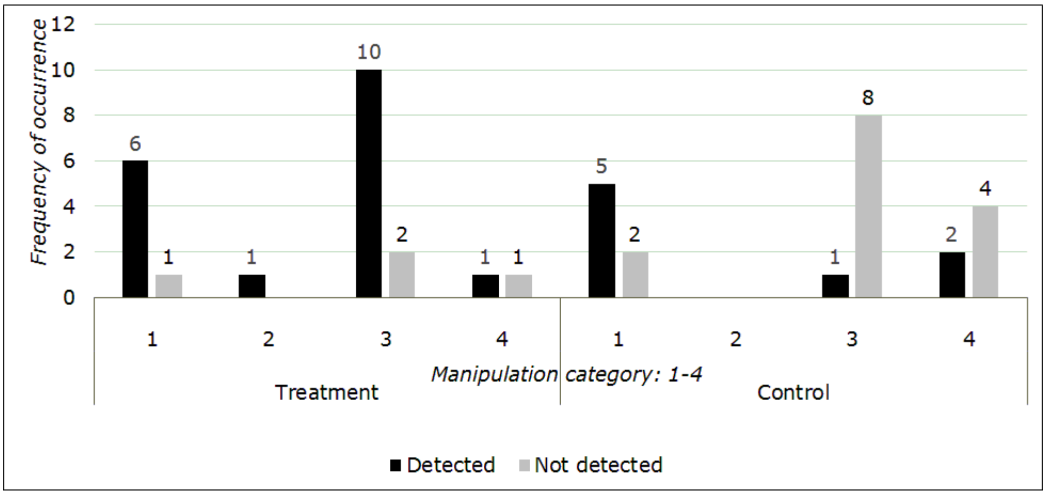

Figure 9.7: Voters' perspective: Frequency of occurrence and detection of each manipulation category.

Evaluation approach

In total 26 (18 from the treatment and 8 from the control group) out of 44 participants detected the introduced manipulations and also noted in the post-questionnaire to have verified the correctness of their ballot. Further, 16 (3 from the treatment and 13 from the control group) out of 18 participants, who did not detect the introduced manipulations, claimed in the post-questionnaire to have verified the correctness of their ballot.

Usability

For the sake of completeness, we report the findings of our usability evaluation for both groups (control and treatment). Nevertheless, in the next section we discuss only the results from the treatment group, because this group used the state of the art EasyVote.

Effectiveness: Figure 9.8 presents the percentage of participants that were able to cast their vote successfully, according to the sub-tasks defined in section 9.3.1. Except for the sub-tasks that were affected by the introduced manipulations, namely verify and fold the ballot, all other sub-tasks were successfully accomplished by all participants.

Last, but not least, it is important to emphasise that none of the participants cast an invalid ballot, and that no questions were asked regarding the vote casting process while reading the poster.

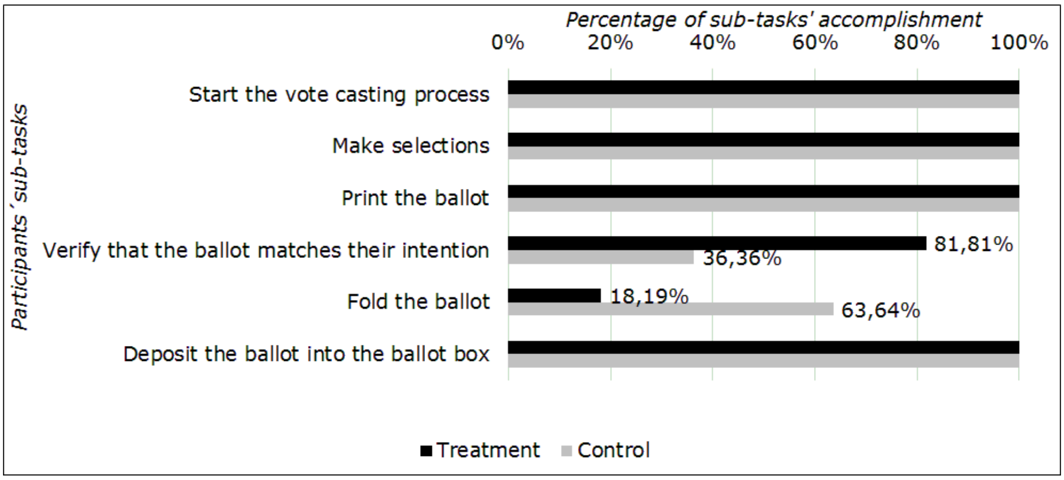

Figure 9.8: Voters' perspective: The percentage of participants that cast their vote successfully.

Efficiency: Figure 9.9 presents the average time that participants spent to cast their vote, according to the time intervals defined in section 9.3.1.

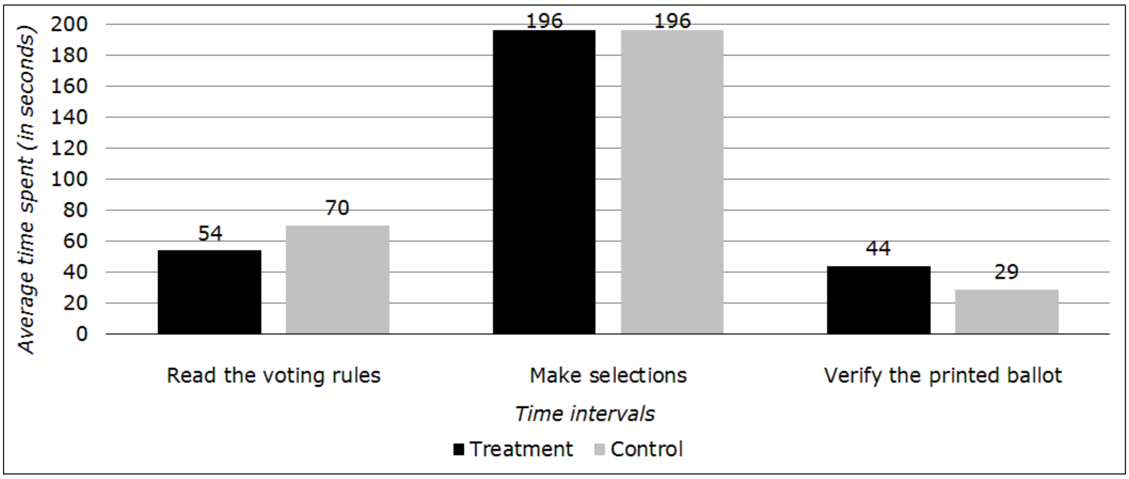

Figure 9.9: Voters' perspective: The average time (in seconds) that participants spent to cast their vote.

Satisfaction: For the SUS questionnaire we distinguish between the following categories:

1. Treatment group.

2. Control group.

3. Manipulation detected.

4. Manipulation not detected.

For the first category the SUS questionnaires resulted in an average value of 79.29 ($\sigma = 13.80$). Further, in the second category, the SUS questionnaires resulted in an average value of 80 ($\sigma = 13.11$). While the scoring of the SUS questionnaires from the third category resulted in an average value of 80 ($\sigma = 14.78$), the scoring of those from the fourth category resulted in an average value of 79.86 ($\sigma = 13.07$).

Mental models

Figures 9.10 and 9.11 present the distribution of participants' perceptions towards ballot verification, namely whether participants perceived ballot verification as demanding and error prone.

9.3.5. Summary and limitations

The findings of our study revealed that the *stimulus* has a significant effect with respect to ballot verification. Significantly more manipulations were detected when the *stimulus* was present. Our findings, not only validate our hypothesis, but reveal a significant improvement in comparison with previous, related studies. Furthermore, with the exception of the participants that detected the manipulations, all other participants folded their ballot. This indicates that the *stimulus* seems to not prevent voters from folding their ballot. In summary, these findings show that the *stimulus* has a positive impact on the security, more specifically on ensuring the integrity of cast votes, of EasyVote and all similar voting schemes/systems.

In total 18 participants did not detect the manipulation, and 16 thereof reported to have verified their ballot. This reveals that self-reported statements are not reliable. Thus, similar studies should use the ballot manipulation approach, otherwise it is not possible to unambiguously determine whether voters verify their ballot or not.

The usability evaluation revealed that EasyVote is significantly better than other similar schemes/systems, represented by EasyVote without the *stimulus*, regarding effectiveness, i.e. the ability of participants to cast a vote successfully. Further, EasyVote seems to be as efficient as other similar schemes/systems, for instance VoteBox [EGB+08b] representing DREs or EasyVote without the *stimulus* representing DREs with paper audit trails. Nevertheless, it is important to note that efficiency might be slightly better, when considering simple elections. Last, but not least, the SUS questionnaires resulted in an average value of 79.29 ($\sigma = 13.80$) which

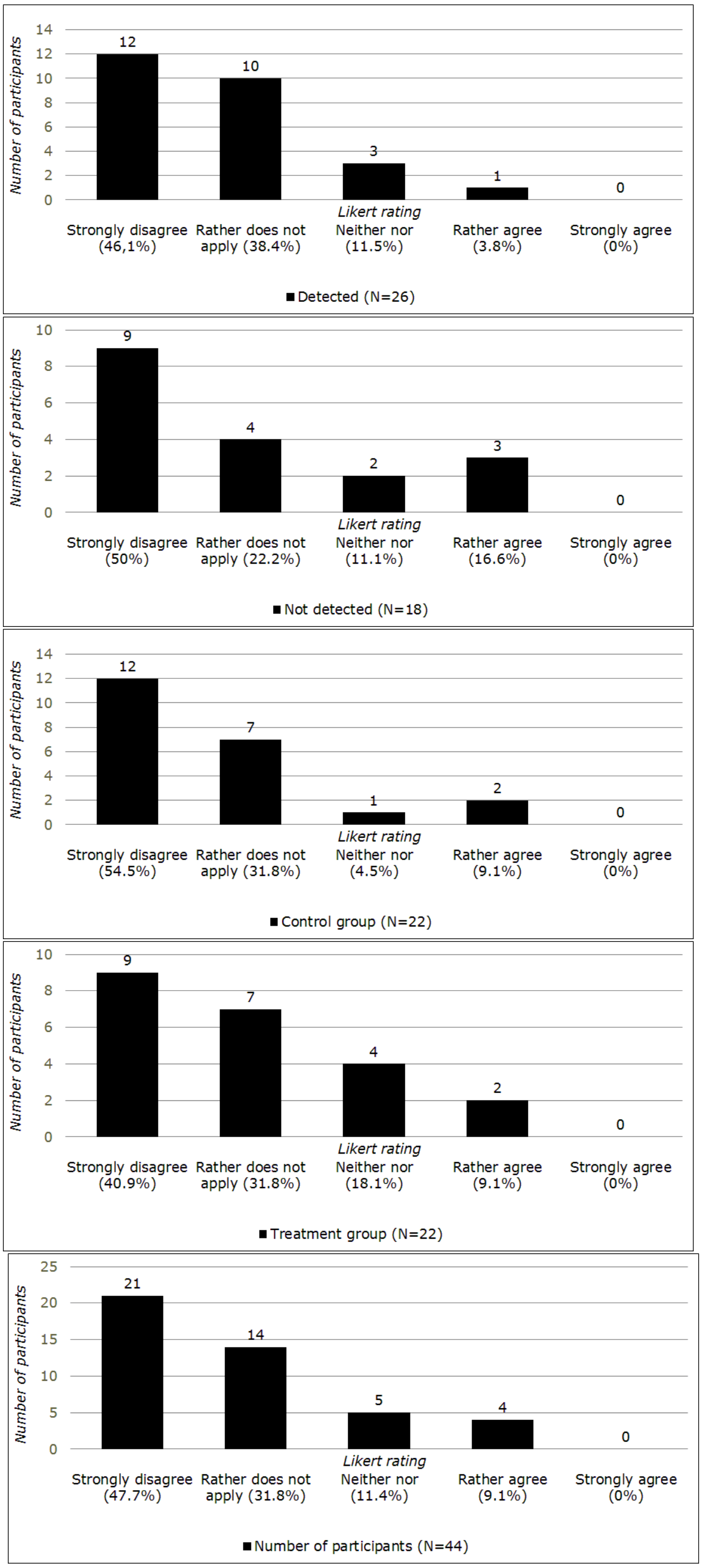

Figure 9.10: Voters' perspective: I perceived the verification of the printed ballot to be a demanding task.

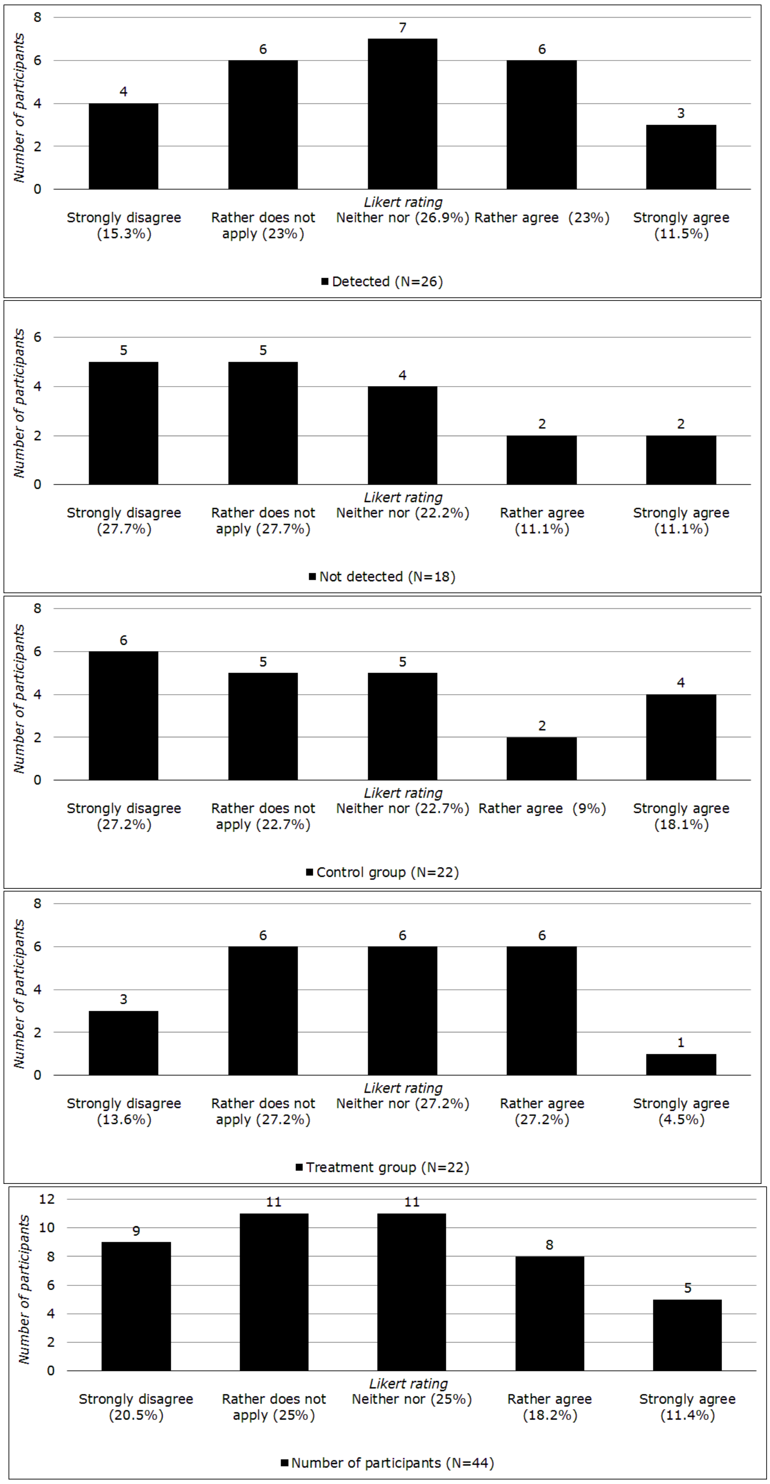

Figure 9.11: Voters' perspective: I perceived the verification of the printed ballot to be an error prone task.

according to Sauro's normalisation method [Sau11] can be interpreted as a grade of B. Consequently, EasyVote (the implemented prototype) has a high perceived usability.

In addition, 79.5% of the participants, namely 35 out of 44 participants, perceived ballot verification as an easy task. Further, 29.6% of the participants, namely 13 out of 44 participants, perceived ballot verification as an error prone task. It is important to emphasise that the majority of the participants who perceived ballot verification as an error prone task, namely 69.2% (9 out of 13 participants), also detected the introduced manipulation. Hence, manipulation detection seems to have lead participants to perceive ballot verification as an error prone task. Furthermore, the treatment and the control group did not differ with respect to their perceptions regarding ballot verification. Even though the majority of the participants perceive the act of verification as easy, it is important to determine, and allay the factors which make participants to perceive ballot verification as error prone.

While the above findings are very promising and represent the first contribution of this chapter, it should be emphasised that this chapter has a second important contribution. Hence, this chapter introduces a new research design for testing hypotheses related to ballot verification by voters. In the following we provide a list of recommendations for such research studies:

- Participants should select their own preferred candidates and/or parties.
- Participants should be deceived.
- Participants should cast a vote for an election that has relevance to them.
- Necessary measures should be taken to prevent any unintentional violation of vote secrecy.
- Real candidates and parties should be used.
- The ballot manipulation approach should be used.

The limitation of the present study is that participants in this sample might be more interested in politics, being self-selecting, than the general voting population. Therefore, these individuals might be more likely to verify their ballot and detect manipulations in comparison to the average voter. As such, the prevalence of verification of the ballot and detection of the manipulations might be relatively biased to the general voting population. Moreover, we made the manipulation reporting very simple, while in genuine elections this may require strict organisational protocols, perhaps a signed form. Furthermore, in legally binding elections the results regarding the verification and detection of manipulations might be slightly different than in a non-legally binding election forecast. Finally, the number of voters that verify their ballot and detect manipulations might be different, depending whether the participation in the election is compulsory or voluntary.

10 Improving & evaluating the verification setting and usability: Electoral officials' perspective

The main goal of this chapter is to identify an effective verification setting that makes electoral officials most likely to detect potential discrepancies between the human- and machine-readable (QR-Code) ballot components. Furthermore, this chapter aims to evaluate the usability of the implemented EasyVote prototype.

To achieve this goal, we proposed an alternative verification setting, which builds upon findings other research areas such as psychology. Further, we conducted a laboratory experiment to evaluate the effectiveness of the proposed verification setting with respect to detecting discrepancies between the human-readable ballot component and the associated QR-Code. Thereby, we also evaluated the usability of the implemented EasyVote prototype from the electoral officials' perspective, i.e. the usability of the tallying process.

The content of this chapter has been published at the *Journal of Annals of Telecommunications* [1].

10.1. Improving the verification setting

Similar to voters, whose primary task is to cast their vote rather than verify, electoral officials' primary task is to tally the election result rather than verify that the human-readable ballot component matches the content stored in and scanned from the associated QR-Code. In addition, electoral officials have to scan a relatively large number of individual ballots, one after the other, and thereby accuracy of the tallying process relies on human (electoral officials) attention.

Previous studies, even though from other research areas, such as airport baggage screening [WHK05, MM10] or cancer screening [GSR+04], report that human attention is notoriously unreliable. This is especially the case when the prevalence of the target to be noticed is low [RKW+08, WHW+07], when the searcher has to look for multiple different targets at the same time [MCD09] and when the size of the area to be searched is large [ZF97]. As all these characteristics hold true for EasyVote (ballot and tallying process), it is important to address this human limitation. Furthermore, the results of our first experiment (EasyVote verification setting) confirm this limitation. Therefore, to improve the situation, we propose that electoral officials read voters' direct selections out loud, while they tally the election result (the individual ballots). Because *reading out loud* is shown to increase and require more attention than "reading" silently [Swa72, Lev79, Kra95, ORSB08].

Note that in the local elections in Darmstadt, electoral officials also read voters' direct selections out loud, while they tally the election result. However, this serves to transfer the votes, from the ballots into the PC-Wahl, rather than to ensure the accuracy of the process.

10.2. Evaluating different verification settings and usability

The main goal of this section is to evaluate the effectiveness of the proposed verification setting with respect to making electoral officials to detect discrepancies between the human-readable ballot component and the associated QR-Code. We focus on the local elections in Darmstadt, and define the following hypothesis:

Hypothesis: Reading the voter's direct selections out loud has a significant impact on detecting potential discrepancies between the human-readable ballot component and the associated QR-Code.

The independent variable is *reading out loud* and the dependent variable is the ratio of detected discrepancies. Furthermore, poor usability is shown to "violate" election integrity, in particular by influencing the election outcome [NKQC08]. Therefore, we also evaluate the usability of the EasyVote (the implemented prototype) tallying process according to the ISO 9241-11 standard [Int98]. To the best of our knowledge, this is the first work to address these issues regarding electronic voting in the context of complex elections.

10.2.1. Overview

In this section we describe the design, materials, methodology to introduce manipulations, setting, and evaluation methodology of the user study.

Design

The main purpose of the study was to test the defined hypothesis. To achieve this goal we conducted a laboratory experiment. Note that due to the experiment's goal we only focus on the second phase of the tallying process.

In the experiment participants (groups of two individuals as suggested in section 5.1) were required to perform the tallying process with EasyVote. Thereby, participants were first trained to use the prototype, similar to the local elections in Darmstadt. Afterwards, participants tallied the ballots that belonged to one polling station of the 2011 local elections in Darmstadt. In the experiment we intentionally manipulated the QR-Codes of a small set of the ballots to be tallied. It is important to emphasise that participants were confronted with a different random order of the same set of manipulations.

In addition, to avoid potential social desirability bias, see section 6.2, participants were given a fictitious research goal. Thus, participants were told that the goal was to evaluate the usability [Int98] of, and actively feed into, the implemented EasyVote prototype by following the human-centred design principles for interactive systems [Int10].

Note that this experiment (EasyVote + reading voter's direct selections out loud) is a replication of the first experiment (EasyVote verification setting), which, for the sake of completeness, we also report in the following of this chapter. The difference between the first experiment and the replication was the verification setting. In contrast to the first experiment, where participants verified that the human-readable ballot component matches the associated QR-Code silently (refer to section 5), in the replication participants read voters' direct selections out loud. Further, in both experiments only the orange marked selections were verified. Last, but not least, based on our hypothesis and participants' task, we adopted a basic within-groups design.

Materials

In the following we list the materials used in the experiment:

- The EasyVote tallying prototype.
- The training workshop presentation.
- 89 ballots, which were created from the ballots of the 2011 local elections in Darmstadt. The ballots contained directly selected candidates and/or a party, as well as crossed out candidates.

- Five training ballots for the training workshop: Three ballots with candidates and a party selected, and two ballots that also contained crossed out candidates. Two of the five ballots required corresponding corrections by the participants.

Introducing manipulations: Altering the QR-Code

In the experiment we intentionally manipulated the QR-Codes of a random set of the ballots to be tallied. We used the following manipulations:

1. Remove votes from a candidate and assign them to another candidate.
2. Remove votes from a candidate and do not re-assign them.
3. Remove a candidate and insert another candidate instead.
4. Remove a candidate.
5. Remove a party, including its candidates.

We decided to manipulate only five out of the 89 ballots to be tallied. This enabled us to cover all manipulation types and to minimise the probability of guessing the actual research goal. Finally, to randomly select the type of manipulation, the ballots to be manipulated, and the positions to introduce the manipulated ballots into the set of all ballots, we used the service provided by RANDOM.ORG[23].

Setting

The experiment took place in a seminar room in the department of computer science at the Technische Universität Darmstadt. The seminar room was equipped with tables, chairs and a projector. The projector was used during the presentations in the respective training workshop. Participants were provided with the necessary hardware equipment, monitors, a computer on which the tallying software (EasyVote prototype) was installed, a QR-Code reader, and a printer. Figure 10.1 shows one group of participants during the experiment.

Further, in the experiment we used an adapted implementation of the EasyVote prototype. The prototype implemented the algorithm to distribute votes in dependence of voters' direct selections automatically, and highlighted voters' direct selections in orange, as proposed in chapter 8. Figure 10.2 presents the adapted interface. In addition, electoral officials used the EasyVote ballot design proposed in chapter 8, see Figure 10.3.

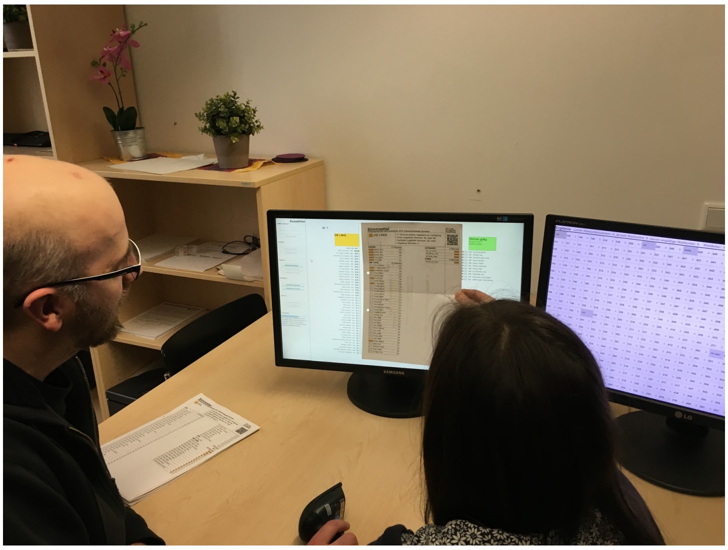

Figure 10.1: Electoral officials' perspective: Participants performing the EasyVote tallying process.

Last, but not least, we created a training workshop presentation, presented in section C in the appendix. We created the presentation based on the one, which was used in the 2011 local elections in Darmstadt.

Evaluation methodology

In the experiment, and therefore also in our evaluation, we distinguish between the following evaluation categories:

1. Verification setting.
2. Usability of EasyVote: Effectiveness, efficiency and satisfaction of the tallying process.

In the following we introduce the evaluation methodology for each of the above categories.

Verification setting In order to measure the effectiveness of the proposed verification setting, we manipulated a random set of the ballots to be tallied, and observed whether participants detected the introduced manipulations.

[23] `https://www.random.org/`, last accessed February, 7, 2016.

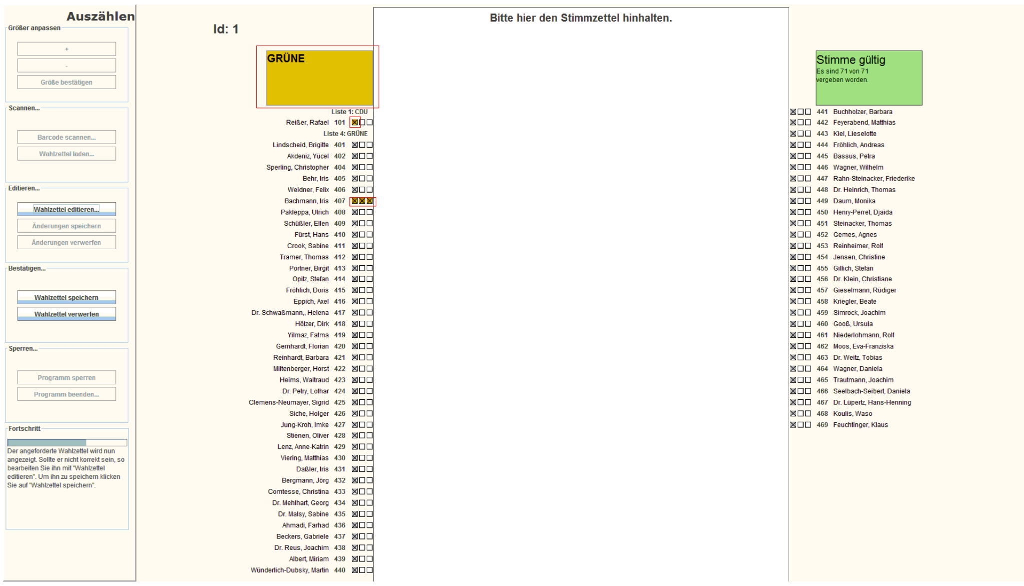

Figure 10.2: Electoral officials' perspective: Adapted interfaces for scanning and verifying the content of the current ballot.

Usability of EasyVote To evaluate the usability of the tallying process, we defined effectiveness, efficiency and satisfaction according to our context as follows:

Effectiveness: *The ability of participants to tally the correct election result.* We did not define any further sub-tasks to measure effectiveness, because, in contrast to vote casting, participants are trained to use the EasyVote tallying prototype. Note that effectiveness corresponds to the main goal of our experiment.

Efficiency: *The time participants spent tallying the election result.* We further recorded the following times:

1. Time spent to tally the first five ballots.

2. Time spent to manually tally the first five ballots and verify the correctness of the first step.

3. Time spent to tally the rest of the ballots.

We used a stopwatch to measure the time spent during the above time intervals.

Satisfaction: *The level of satisfaction participants experienced while tallying the election result.* In order to measure satisfaction we used a German translation [LS13] of the original SUS questionnaire [Bro96].

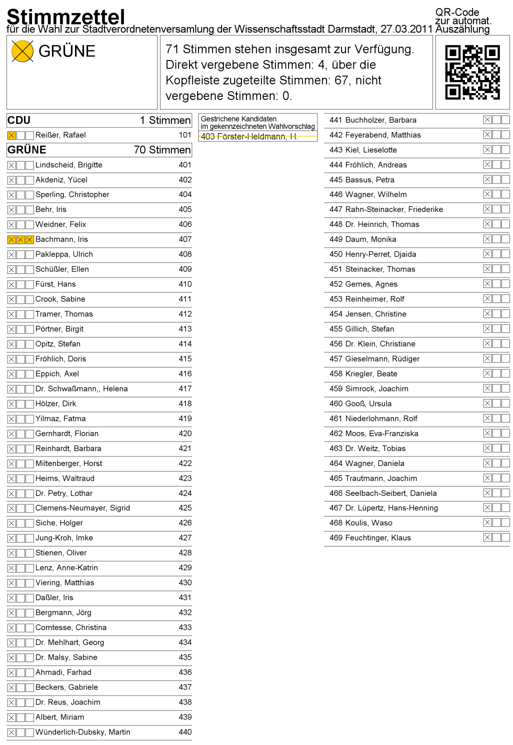

Figure 10.3: Electoral officials' perspective: The EasyVote ballot design.

10.2.2. Procedure

The participants were randomly assigned to different groups of two people. Further, each group had to perform the following sequential steps:

1. Read and sign the declaration of consent for participating in the experiment.
2. Participate in the training workshop.
3. Tally the ballots.
4. Debrief: Reveal the actual research goal.

In addition, participants of each group were randomly assigned to independently perform the following tasks:

1. Operate the prototype.
2. Scan the QR-Codes.

However, both participants had to verify that the QR-Code matched the human-readable ballot component simultaneously. Note that the training workshop last 30 minutes, and to address the problem of fatigue, we introduced a 10 minutes coffee break between the second and the third step.

10.2.3. Participants: Recruitment, incentives and sample

Participants were recruited via e-mail, advertising in social networks and flyers. Three different incentives encouraged participation: First, the employees of our university were interested in science and wanted to support our research. Second, some of the participants were psychology students, who are required by their department to participate in 30 hours of research studies. We compensated them with appropriate credits in dependence of the total time spent in the experiment. The rest of the participants were given €10 each. In the following we describe the samples according to the different experiments.

Sample: First experiment (EasyVote verification setting)

8 subjects participated (2 female, 6 male), who ranged in age from 19-26, with an average age of 22.5 years ($s = 2.1$) and a median age of 23. All participants had a high school degree or less.

Sample: Replication experiment (EasyVote + reading voter's direct selections out loud)

40 subjects participated (17 female, 23 male), who ranged in age from 18-54, with an average age of 26.3 years ($s = 8$) and a median age of 25. Five participants had completed an apprenticeship; 21 participants had a high school degree or less; and 13 participants had a bachelor's degree or equivalent. One participant did not reveal the level of education.

10.2.4. Results

We report the findings of our experiment according to the categories defined in the evaluation methodology:

1. Verification setting.
2. Usability of EasyVote: Effectiveness, efficiency and satisfaction of the tallying process.

Verification setting

Figure 10.4 presents the findings with respect to both experiments. Note that the first experiment (EasyVote verification setting) revealed very bad results with respect to detecting the introduced manipulations. Therefore, we aborted this experiment after the first four groups. This explains the difference in the group sizes between both experiments.

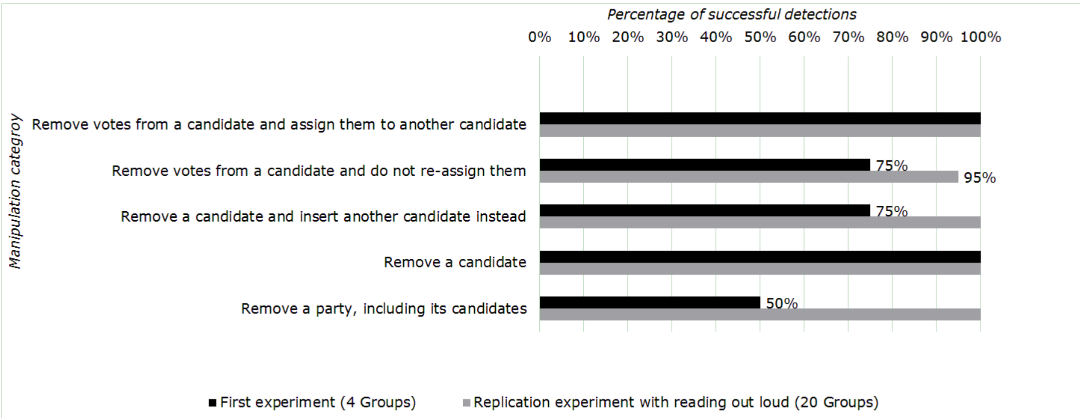

Figure 10.4: Electoral officials' perspective: The effectiveness of verification settings regarding the detection of manipulations.

Note that due to the different group sizes, in the following we report about the usability evaluation only with respect to the replication experiment (EasyVote + reading voter's direct selections out loud).

Usability

We report the results of our usability evaluation in terms of effectiveness, efficiency and satisfaction.

Effectiveness: In accordance with the definition of effectiveness, refer to section 10.2.1, the tallying of the election result with the proposed verification setting was, in average, 99% effective. Thereby, 19 out of 20 groups were 100% effective, while one group was only 80% effective.

Efficiency. Figure 10.5 presents the average time spent by participants to tally the election result, according to the time intervals defined in section 10.2.1.

Satisfaction: The scoring of the completed SUS questionnaires resulted in an average value of 82.29 ($\sigma = 12.03$).

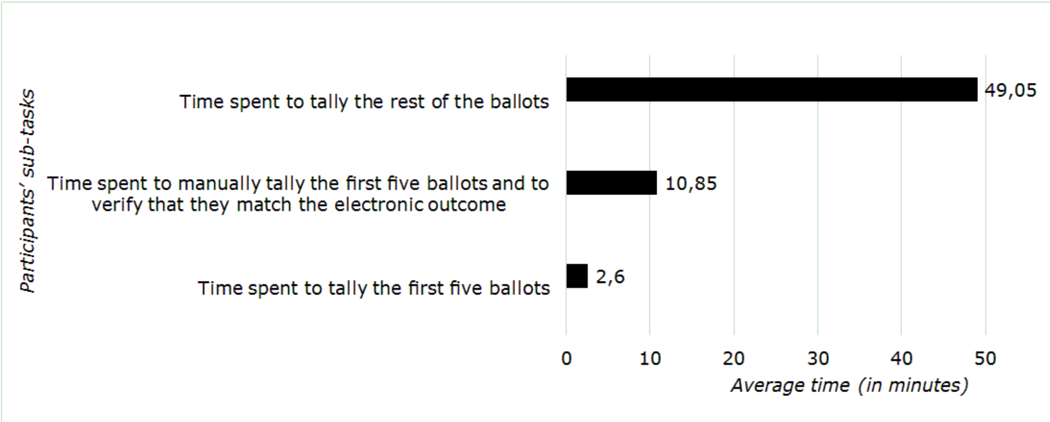

Figure 10.5: Electoral officials' perspective: The time (in minutes) that participants spent to tally the election result.

10.2.5. Summary, outlook and limitations

The findings of the study revealed that *reading voters' direct selections out loud* has a significant effect on detecting discrepancies between the human-readable ballot component and the associated QR-Code. These results validate our hypothesis.

The usability evaluation revealed that EasyVote (with *reading out loud*) is very effective with respect to tallying the correct election result. In average, in 99% of the cases, participants were able to tally the correct election result. While there exist no reference results with respect to efficiency, the SUS questionnaires resulted in an average value of 82.29 ($\sigma = 12.03$), which according to Sauro's normalisation method [Sau11] can be interpreted as a grade of A. Consequently, EasyVote (the implemented prototype) has a very high perceived usability.

While the above findings are very promising and can be applied to electronic voting schemes/systems similar to EasyVote, for instance [BCH$^+$12, BFL$^+$12, Veg12, BBE$^+$13, Vot08], three alternative verification settings could be considered:

1. Replication of the tallying process with different tallying devices, which are provided by independent developers.

2. Random audits of the electronically stored data, with a random set of ballots. Note that the tallying process can also be video recorded. Thus, a random audits can be also performed by using video fragments of the record.

3. Random verifications of the implemented algorithm for distributing votes automatically and of the second monitor, i.e. that votes are added correctly to the intermediate result.

4. Use of cryptographic primitives, for instance hash chains, and replication of the tallying process with a second, independent tallying device.

Note that the above list is not comprehensive, and it can be extended. Nevertheless, this list serves as a starting point for further discussion and future research. While in our opinion the third option seems the most adequate with respect to its practicality and applicability, it is important to consult the respective literature, for instance [Nef03, ST14], to determine the appropriate level of assurance. Furthermore, future research should address the issue of electoral officials' endurance/feasibility with respect to reading voters' direct selections out loud.

There are three limitations in the present study: First, the results regarding the detection of manipulations might be similar, even when direct selections are not highlighted in orange. Nevertheless, a significant difference with respect to efficiency and satisfaction can be assumed. To achieve better results with respect to effectiveness, efficiency and satisfaction, we suggest deploying both interventions, namely reading voters' direct selections out loud and highlighting them in orange. The second limitation is that most of the participants in this sample were university students. Hence, they are unlikely to be representative of the larger population (electoral officials) with respect to age and educational level. Last, but not least, in legally binding elections the results regarding the verification and detection of manipulations might be slightly different, depending on whether electoral officials support similar or different electoral goals (parties).

10.2.6. Additional insights

In this section we provide some additional insights with respect to efficiency measurements of the tallying process. Thereby, we conducted several studies with different ballots (EasyVote and local elections in Darmstadt) and tallying software (EasyVote and PC-Wahl). Note that the reported results serve to provide first insights rather than final results.

Table 10.1 presents the results of the efficiency comparison regarding different ballot designs with respect to the first phase of the tallying process. The following ballot types were used in the study:

1. Ballot of the local elections in Darmstadt 2011, refer to Figure 4.1.

2. The black-and-white EasyVote ballot, refer to Figure 8.3.

Further, electoral officials went through the following sequential steps:

1. Open ballot box and count the total number of ballots.
2. Classify ballots into four categories.
3. Verify that ballots are correctly classified.
4. Manually tally the ballots of category (1).
5. Review ballots of category (4) and assign them to (1-3).
6. Compute the intermediate result manually.

Table 10.1: Electoral officials' perspective: Efficiency (time in mins) comparison of the tallying process (first phase, 189 ballots).

Steps \ **Ballot types**	1	2
1	17	4
2	26	4
3	12	3
4	13	4
5	9	0
6	1	0
Total time	78	15
Groups of electoral officials	1	1

Note that the first column is borrowed from the master thesis by Jöris [Jör13]. Even though these results are obtained from a single study group, the difference between EasyVote and the local elections in Darmstadt is very obvious. The tallying process with the EasyVote ballots is five times faster than with the ballots from the local elections in Darmstadt.

Table 10.2 presents the results of the efficiency comparison regarding different ballot designs and different types of tallying software, with respect to the second phase of the tallying process. The following combinations of ballots and tallying software were used in the study:

1. Ballot of the local elections in Darmstadt 2011, refer to Figure 4.1, and PC-Wahl.
2. The black-and-white EasyVote ballot, refer to Figure 8.3, and PC-Wahl.

3. The hybrid orange EasyVote ballot, refer to Figure 8.4, and EasyVote tallying prototype.

4. The hybrid orange EasyVote ballot, refer to Figure 8.4, and EasyVote tallying prototype with reading out loud.

Further, electoral officials went through the following sequential steps:

1. Tally the first five ballots.

2. Manually tally and verify the correctness of the first steps.

3. Tally the rest of the ballot.

Table 10.2: Electoral officials' perspective: Efficiency (time in mins) comparison of the tallying process (second phase, 89 ballots).

Steps \ **Ballot + software**	1	2	3	4
1	6	4	1.25	2.6
2	21	10	11.25	10.85
3	84	62	36.25	49.05
Total time	111	76	49	63
Groups of electoral officials	1	1	4	20

Note that the first column is borrowed from the master thesis by Jöris [Jör13]. Even though these results cannot be conclusively compared due to the different group sizes, it is important to mention that EasyVote (with *reading out loud*) is as fast as the other alternative (EasyVote prototype) and almost twice as fast as PC-Wahl. Furthermore, PC-Wahl with the EasyVote ballots seems to improve the efficiency of the tallying process in the local elections in Darmstadt. This might be interesting in case EasyVote is used only for the vote casting process.

11 Summary and future work directions

The goal of this dissertation was to pave the way for the use of EasyVote in legally binding elections. To achieve this goal, this dissertation addressed five open, usable security, research questions.

The first research question aimed to determine whether voters have secrecy concerns with respect to the use of QR-Codes and, if so, to address such concerns effectively. The findings suggested that voters do have secrecy concerns in association with the use of QR-Codes. Furthermore, the findings revealed that the threat appraisal approach of the protection motivation theory [Rog75], is a viable approach to address and significantly allay such concerns.

The second research question aimed to identify a ballot design that enables voters to understand the impact of their selections and to verify their voting intention easily. Therefore, three different ballot designs, see Figures 8.3, 8.4 and 8.5 in section 8.1, were proposed and evaluated with respect to *understandability*, i.e. whether voters understand the impact of their selections (how their cast votes are tallied), and *verifiability*, i.e. whether voters can verify their cast vote easily. The findings revealed that the ballot design, which highlights voters' direct selections in orange, see Figure 8.4, represents an optimal ballot design with respect to understandability and verifiability of the cast vote.

The third research question aimed to develop an effective *stimulus*, i.e. verification instructions, that makes voters most likely to verify their ballot. The findings revealed that the developed *stimulus*, consisting of pre-printed verification instructions on the reverse of the ballot, see section 9.1, had a significant effect on participants' behaviour with respect to verifying their ballot and detecting potential discrepancies (manipulations). Hence, these findings show a significant improvement with respect to ensuring the integrity of cast votes and election result, in comparison to the results reported by similar, previous studies [Sel04, Coh05, HNH+05, mar06, SP06].

The fourth research question aimed to identify effective verification settings that make electoral officials most likely to detect potential discrepancies between the human-readable ballot component and the associated QR-Code. The findings revealed a significant increase with respect to detecting discrepancies (manipulations) when participants read voter's direct selections out loud, while verifying that the human-readable ballot component matches the data stored in the QR-Code. Hence, *reading out loud* significantly improves the security of EasyVote with respect to ensuring the integrity of the election result in the tallying process.

Last, but not least, the fifth question aimed to evaluate the usability of the implemented EasyVote prototype from the voters' and the electoral officials' perspective. From the voters' perspective, the findings revealed a significant improvement regarding effectiveness due to the presence of the *stimulus*, i.e. significantly more manipulations were detected when the *stimulus* was present. Further, EasyVote seems to be as efficient as other similar schemes/systems, for instance VoteBox [EGB+08b] representing DREs or EasyVote without the *stimulus* representing DREs with paper audit trails. In addition, the act of casting a vote with the implemented EasyVote prototype was perceived as satisfactory by the participants, which assigned the prototype the grade B (according to Sauro's normalisation method [Sau11]). From the electoral officials' perspective, the findings revealed a significant improvement regarding effectiveness due to *reading out loud*, i.e. significantly more manipulations were detected. While there exist no reference results with respect to efficiency, the tallying process with the implemented EasyVote prototype was perceived as very satisfactory by the participants, which assigned the prototype the grade A (according to Sauro).

In summary, by making the detection of election fraud significantly more likely, the findings of this dissertation contribute to the improvement of security for electronic voting schemes/systems that provide voters with paper audit trails (printed ballot). The latest information and findings about EasyVote, for instance list of publications, implemented prototype and user studies, can be found at SECUSO[24].

While this dissertation successfully addressed the above research questions, there are still open research questions to be addressed before EasyVote can be used in legally binding elections. For instance, more research is needed to better understand voters' mental models regarding trust and secrecy concerns with respect to new voting technologies. Furthermore, future work should determine, and allay factors which make participants to perceive ballot verification as error prone. In addition, future work should address the alignment of EasyVote with respect to legal requirements, in particular with respect to the *public nature of elections*, not only

[24] `https://secuso.org/easyvote/`, last accessed February, 7, 2016.

from a concept perspective, as already shown by Henning *et al.* [17], but rather from a system perspective. Moreover, future work should address the issue of ensuring vote secrecy with respect to side-channel attacks, for instance electromagnetic emissions [VE85], tempest [Fri72] or differential power analysis [KJJ99]. Last, but not least, other future work directions include the extension of EasyVote with cryptographic verifiability [Joa14] or the use of EasyVote as a tool for supporting postal voters.

Bibliography

[AILL13] Michael R. Alvarez, Julia Pomares Ines Levin, and Marcelo Leiras. Voting Made Safe and Easy: The Impact of e-voting on Citizen Perceptions. *Political Science Research and Methods*, 1(1):117–137, 3013. Cited on pages 9 and 10.

[AKBW14] Claudia Z. Acemyan, Philip Kortum, Michael D. Byrne, and Dan S. Wallach. Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems (JETS)*, 1(3):26–56, 2014. Cited on pages 9 and 10.

[AKBW15] Claudia Z. Acemyan, Philip Kortum, Michael D. Byrne, and Dan S. Wallach. From Error to Error: Why Voters Could not Cast a Ballot and Verify Their Vote With Helios, Prêt à Voter, and Scantegrity II. *The USENIX Journal of Election Technology and Systems (JETS)*, pages 1–25, 2015. Cited on pages 9 and 10.

[AKLM09] Michael R. Alvarez, Gabriel Katz, Ricardo Llamosa, and Hugo E. Martinez. Assessing voters' attitudes towards electronic voting in latin america: Evidence from colombia's 2007 e-voting pilot. In Peter Y. A. Ryan and Berry Schoenmakers, editors, *E-Voting and Identity*, volume 5767 of *LNCS*, pages 75–91. Springer Berlin Heidelberg, 2009. Cited on pages 9, 10, and 48.

[AKP11] Michael R. Alvarez, Gabriel Katz, and Julia Pomares. The impact of new technologies on voter confidence in latin america: evidence from e-voting experiments in argentina and colombia. *Journal of Information Technology & Politics*, 8(2):199–217, 2011. Cited on pages 9 and 10.

[AKP13] Claudia Ziegler Acemyan, Philip Kortum, and David Payne. Do Voters Really Fail to Detect Changes to Their Ballots? An Investigation of

Ballot Type on Voter Error Detection. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 57, pages 1405–1409. SAGE Publications, 2013. Cited on pages 9 and 10.

[AMBS07] Joerg Arzt-Mergemeier, Willi Beiss, and Thomas Steffens. The digital voting pen at the hamburg elections 2008: Electronic voting closest to conventional voting. In *E-Voting and Identity*, pages 88–98. Springer, 2007. Cited on page 10.

[Ame16] American Institute of Graphic Arts. TOP 10 ELECTION DESIGN GUIDELINES, 2016. `http://www.aiga.org/election-design-top-ten/`, last accessed February, 7, 2016. Cited on pages 63, 75, and 77.

[BBE+13] Josh Benaloh, Michael D. Byrne, Bryce Eakin, Philip Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, Dan S. Wallach, Gail Fisher, Julian Montoya, Michelle Parker, and Michael Winn. Star-vote: A secure, transparent, auditable, and reliable voting system. *The USENIX Journal of Election Technology and Systems (JETS)*, 1(1):18–37, 2013. Cited on pages 3, 4, 47, 73, and 108.

[BCH+12] Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter YA Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, and Zhe Xia. Using prêt à voter in victorian state elections. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*. USENIX, 2012. Cited on pages 3, 47, 73, and 108.

[BCT10] Johann A. Briffa, Chris Culnane, and Helen Treharne. Imperceptible printer dot watermarking for binary documents. In *SPIE Photonics Europe*, pages 77230M–77230M. International Society for Optics and Photonics, 2010. Cited on page 48.

[Ben06] Josh Benaloh. Simple verifiable elections. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*, pages 5–5. USENIX, 2006. Cited on page 73.

[Ben07] Josh Benaloh. Ballot casting assurance via voter-initiated poll station auditing. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*, pages 14–14. USENIX, 2007. Cited on page 73.

[BFL+12] Jonathan Ben-Nun, Niko Fahri, Morgan Llewellyn, Ben Riva, Alon Rosen, Amnon Ta-Shma, and Douglas Wikström. A new implementation of a dual (paper and cryptographic) voting system. In Arslan Brömme and Christoph Busch, editors, *Proceedings of the 5th International Conference on Electronic Voting (EVOTE)*, pages 315–329. Bonn: Gesellschaft für Informatik (GI), 2012. Cited on pages 3, 4, 47, 73, and 108.

[BHMQ+08] Michael Bär, Christian Henrich, Jörn Müller-Quade, Stefan Röhrich, and Carmen Stüber. Real world experiences with bingo voting and a comparison of usability. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*. USENIX Association, 2008. Cited on pages 9 and 10.

[BJV14] Jurlind Budurushi, Roman Jöris, and Melanie Volkamer. Implementing and evaluating a software-independent voting system for polling station elections. *Journal of Information Security and Applications*, 19(2):1–10, 2014. Cited on page 27.

[BKA15] Grant M. Belton, Philip Kortum, and Claudia Acemyan. How hard can it be to place a ballot into a ballot box?: usability of ballot boxes in tamper resistant voting systems. *Journal of Usability Studies*, 10(4):129–139, 2015. Cited on pages 7 and 9.

[BNSV14] Jurlind Budurushi, Stephan Neumann, Genc Shala, and Melanie Volkamer. Entwicklung eines Common Criteria Schutzprofils für elektronische Wahlgeräte mit Paper Audit Trail. In Erhard Plödereder, Lars Grunske, Eric Schneider, and Dominik Ull, editors, *INF14 - Workshop: Elektronische Wahlen: Unterstützung der Wahlprozesse mittels Technik*, volume 232 of *Lecture Notes in Informatics*, pages 1415–1426. Köllen Druck+Verlag GmbH, Bonn, 2014. Cited on page 4.

[Boa14] Board of Elections City of New York. Ballot Marking Device, 2014. `http://vote.nyc.ny.us/html/newway_en/using_bmd.shtml`, last accessed February, 7, 2016. Cited on pages 3 and 73.

[Bro96] John Brooke. SUS-A quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996. Cited on pages 89 and 104.

[BS95] Curt C. Braun and N Clayton Silver. Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance. *Ergonomics*, 38(11):2207–2220, 1995. Cited on page 66.

[Bur09] Ed Burnette. *Hello, Android: introducing Google's mobile development platform*. Pragmatic Bookshelf, 2009. Cited on page 16.

[Cam13] Bryan A. Campbell. *The Usability Implications of Long Ballot Content for Paper, Electronic, and Mobile Voting Systems*. PhD thesis, Rice University, Houston, TX, 2013. Cited on pages 9 and 10.

[CB09] Bryan A. Campbell and Michael D. Byrne. Now do voters notice review screen anomalies? a look at voting system usability. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*. USENIX Association, 2009. Cited on page 9.

[CB14] Lorrie Faith Cranor and Norbou Buchler. Better Together: Usability and Security Go Hand in Hand. *IEEE Security & Privacy*, 12(6):89–93, 2014. Cited on page 16.

[CBL+09] Frederick G. Conrad, Benjamin B. Bederson, Brian Lewis, Emilia Peytcheva, Michael W. Traugott, Michael J. Hanmer, Paul S. Herrnson, and Richard G. Niemi. Electronic voting eliminates hanging chads but introduces new usability challenges. *International Journal of Human-Computer Studies*, 67(1):111–124, 2009. Cited on pages 9 and 10.

[CEP09] Ernesto Calvo, Marcelo Escolar, and Julia Pomares. Ballot design and split ticket voting in multiparty systems: Experimental evidence on information effects and vote choice. *Electoral Studies*, 28(2):218–231, 2009. Cited on pages 9 and 10.

[CG05] Lorrie F. Cranor and Simson Garfinkel, editors. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly Media, Inc., 2005. Cited on page 16.

[Cha04] David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy*, 2(1):38–47, 2004. Cited on page 73.

[CLP+06] Frederick G. Conrad, Brian Lewis, Emilia Peytcheva, Michael W. Traugott, Michael J. Hanmer, Paul S. Herrnson, Richard G. Niemi, and

Benjamin B. Bederson. The usability of electronic voting systems: Results from a laboratory study. *Midwest Political Science Association*, 2006. Cited on pages 9 and 10.

[Coh05] Sharon B. Cohen. Auditing Technology for Electronic Voting Machines. Master's thesis, California Institute of Technology and Massachusetts Institute of Technology, 2005. `http://vote.caltech.edu/sites/default/files/vtp_wp46.pdf`, last accessed February, 7, 2016. Cited on pages 3, 7, 9, 73, 77, 78, 81, 82, and 113.

[CVB+15] Gamze Canova, Melanie Volkamer, Clemens Bergmann, Roland Borza, Benjamin Reinheimer, Simon Stockhardt, and Ralf Tenberg. Learn To Spot Phishing URLs with the Android NoPhish App. In *Information Security Education Across the Curriculum - 9th (IFIP)*, IFIP Advances in Information and Communication Technology, pages 87–100. Springer, 2015. Cited on page 16.

[CVBB14] Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Roland Borza. NoPhish: An Anti-Phishing Education App. In Sjouke Mauw and ChristianDamsgaard Jensen, editors, *10th International Workshop on Security and Trust Management in conjunction with ESORICS 2014*, volume 8743 of *Lecture Notes in Computer Science*, pages 188–192. Springer International Publishing, 2014. Cited on page 16.

[EGB+08a] Sarah P. Everett, Kristen Greene, Michael Byrne, Dan Wallach, Kyle Derr, Daniel Sandler, and Ted Torous. Is newer always better? The usability of electronic voting machines versus traditional methods, 2008. Cited on pages 9 and 10.

[EGB+08b] Sarah P. Everett, Kristen K. Greene, Michael D. Byrne, Dan S. Wallach, Kyle Derr, Daniel Sandler, and Ted Torous. Electronic voting machines versus traditional methods: Improved preference, similar performance. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 883–892. ACM, 2008. Cited on pages 9, 10, 94, and 114.

[ELE15] ELECTION ASSISTANCE COMMISSION. Voluntary Voting System Guidelines 1.1 Volume 1, 2015. `http://www.eac.gov/assets/1/Documents/VVSG.1.1.VOL.1.FINAL.pdf`, last accessed February, 7, 2016. Cited on pages 63, 75, and 86.

[Eve07] Sahra P. Everett. *The usability of electronic voting machines and how votes can be changed without detection.* PhD thesis, Rice University, Houston, TX, 2007. Cited on pages 9, 10, and 82.

[Fed09] Federal Constitutional Court of Germany. Decisions: Order of 03 March 2009 - 2 BvC 3/07, 2009. `http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html`, last accessed February, 7, 2016. Cited on page 44.

[FMS07] Ivan Flechais, Cecilia Mascolo, and Angela M. Sasse. Integrating Security and Usability into the Requirements and Design Process. *International Journal of Electronic Security and Digital Forensics*, 1(1):12–26, May 2007. Cited on page 16.

[FP96] Diamanto Filippatou and Peter D. Pumfrey. Pictures, Titles, Reading Accuracy and Reading Comprehension: a research review (1973-95). *Educational Research*, 38(3):259–291, 1996. Cited on pages 69 and 77.

[Fri72] Jeffrey Friedman. Tempest: A signal problem. *NSA Cryptologic Spectrum*, 1972. Cited on pages 4 and 115.

[GB07] Stephen N. Goggin and Michael D. Byrne. An examination of the auditability of voter verified paper audit trail (vvpat) ballots. pages 10–10. USENIX Association, 2007. Cited on pages 7 and 9.

[GBG+08] Stephen N. Goggin, Michael D. Byrne, Juan E. Gilbert, Gregory Rogers, and Jerome McClendon. Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems, 2008. Cited on pages 7 and 9.

[GDOS13] Juan E. Gilbert, Jerone Dunbar, Alvitta Ottley, and John Mark Smotherman. Anomaly detection in electronic voting systems. *Information Design Journal*, 20(3), 2013. Cited on pages 9 and 10.

[GHDD13] Alan S. Gerber, Gregory A. Huber, David Doherty, and Conor M. Dowling. Is there a secret ballot? Ballot secrecy perceptions and their implications for voting behaviour. *British Journal of Political Science*, 43(01):77–102, 2013. Cited on pages 2 and 48.

[GHJV94] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Desing Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional, 1994. Cited on pages 16 and 29.

[GMR+12] Juan E. Gilbert, Aqueasha M. Martin, Gregory Rogers, Jerome McClendon, and Josh Ekandem. Hey, that's not who i voted for!: a study on touchscreen ballot design. *Interactions*, 19(6):34–39, 2012. Cited on page 9.

[Gog08] Stephen N. Goggin. Usability of election technologies: Effects of political motivation and instruction use. *The Rice Cultivator: A Student Journal of Public Policy Research*, 1:30–45, 2008. Cited on pages 9 and 10.

[Gre08] Kristen K. Greene. Usability of new electronic voting systems and traditional methods: Comparisons between sequential and direct access electronic voting interfaces, paper ballots, punch cards, and lever machines. Master's thesis, Rice University, Houston, TX, 2008. Cited on pages 9 and 10.

[GSR+04] David Gur, Jules H. Sumkin, Howard E. Rockette, Marie Ganott, Christiane Hakim, Lara Hardesty, William R. Poller, Ratan Shah, and Luisa Wallace. Changes in breast cancer detection and mammography recall rates after the introduction of a computer-aided detection system. *Journal of the National Cancer Institute*, 96(3):185–190, 2004. Cited on pages 3 and 99.

[HA14] Yasser M. Hausawi and William H. Allen. Usablity and security tradeoff: a design guideline. In *Proceedings of the 2014 ACM Southeast Regional Conference*, page 21. ACM, 2014. Cited on page 16.

[HBV14] Maria Henning, Jurlind Budurushi, and Melanie Volkamer. Elektronsiche Wahlen durch Stimmzettelbelege? Untersuchung möglicher Umsetzungen des Öffentlichkeitsgrundsatzes bei elektronischen Wahlen. *MultiMedia und Recht (MMR)*, pages 154–158, 2014. Cited on pages 2 and 63.

[HCB15] Jeffrey Hsu, Qiyang Chen, and Gary Bronson. Evaluating the usability of e-voting technologies. *International Journal of Information Systems and Social Change*, 6(2):16–33, 2015. Cited on pages 9 and 10.

[HNH+05] Paul S. Herrnson, Richard G. Niemi, Michael J. Hanmer, Peter L. Francia, Benjamin B. Bederson, Fred Conrad, and Michael Traugott. The promise and pitfalls of electronic voting: results from a usability field test, 2005. `http://www.capc.umd.edu/rpts/Promise_and_Pitfalls_of_Electronic_Voting.pdf`, last accessed February, 7, 2016. Cited on pages 3, 73, 77, 78, 79, 81, and 113.

[HNH+06a] Paul S. Herrnson, Richard G. Niemi, Michael J. Hanmer, Benjamin B. Bederson, Frederick G. Conrad, and Michael Traugott. The importance of usability testing of voting systems. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop*. USENIX Association, 2006. Cited on page 3.

[HNH+06b] Paul S. Herrnson, Richard G. Niemi, Michael J. Hanmer, Benjamin B. Bederson, Frederick G. Conrad, and Michael W. Traugott. Voters' abilities to cast their votes as intended. In *Workshop on the Usability and Security of Electronic Voting System*, 2006. Cited on pages 9 and 10.

[HNH+08] Paul S. Herrnson, Richard G. Niemi, Michael J. Hanmer, Peter L. Francia, Benjamin B. Bederson, Frederick G. Conrad, and Michael W. Traugott. Voters' Evaluations of Electronic Voting Systems Results From a Usability Field Study. *American Politics Research*, 36(4):580–611, 2008. Cited on pages 9 and 10.

[HVB12] Maria Henning, Melanie Volkamer, and Jurlind Budurushi. Elektronische Kandidatenauswahl und automatisierte Stimmermittlung am Beispiel hessischer Kommunalwahlen. *Die Öffentliche Verwaltung (DÖV)*, (20):789–796, 2012. Cited on pages 4 and 45.

[Int98] International Organization For Standardization. ISO 9241-11: Ergonomics of Human System Interaction – Part 11: Guidance on Usability, 1998. `https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-1:v1:en`, last accessed February, 7, 2016. Cited on pages 17, 81, 100, and 101.

[Int07] International Organization For Standardization. ISO 216:2007: Writing paper and certain classes of printed matter – Trimmed sizes – A and B series, and indication of machine direction, 2007. `https://www.iso.org/obp/ui/#iso:std:36631:en`, last accessed February, 7, 2016. Cited on page 25.

[Int10] International Organization For Standardization. ISO 9241-210: Ergonomics of Human System Interaction – Part 210: Human-centred design processes for interactive systems, 2010. `https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en`, last accessed February, 7, 2016. Cited on pages 57, 68, and 101.

[Int15] International Organization For Standardization. ISO/IEC 18004:2015: Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specificationn, 2015. `https://www.iso.org/obp/ui/#iso:std:62021:en`, last accessed February, 7, 2016. Cited on pages 2, 25, and 48.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant Electronic Elections. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 61–70. ACM, 2005. Cited on page 11.

[JHG07] Menno Jong, Joris Hoof, and Jordy Gosselt. User research of a voting machine: Preliminary findings and experiences. *Journal of Usability Studies*, 2(4):180–189, 2007. Cited on pages 9 and 10.

[JHG08] Menno De Jong, Joris Van Hoof, and Jordy Gosselt. Voters' Perceptions of Voting Technology Paper Ballots Versus Voting Machine With and Without Paper Audit Trail. *Social Science Computer Review*, 26(4):399–410, 2008. Cited on pages 7 and 9.

[Joa14] Rui Joaquim. How to prove the validity of a complex ballot encryption to the voter and the public. *Journal of Information Security and Applications*, 19(2):130–142, 2014. Cited on page 115.

[Jon05] Douglas W. Jones. Chain voting. In *Developing an Analysis of Threats to Voting Systems: Workshop Summary*. National Institute of Standards and Technology, 2005. `http://www.nist.gov/itl/vote/upload/threatworksummary.pdf`, last accessed February, 7, 2016. Cited on page 11.

[Jör13] Roman Jöris. Implementation and evaluation of the vote casting device. Master thesis, Technische Universität Darmstadt, 2013. Cited on pages 2, 29, 63, 110, and 111.

[KAC^{+}11] Gabriel Katz, Michael R. Alvarez, Ernesto Calvo, Marcelo Escolar, and Jurlia Pomares. Assessing the Impact of Alternative Voting Technologies on Multi-Party Elections: Design Features, Heuristic Processing and Voter Choice. *Political Behaviour*, 33(2):247–270, 2011. Cited on pages 9 and 10.

[Kas14] Jakob Kasbauer. Usable security. *Fun, Secure, Embedded*, pages 20–25, 2014. Cited on page 15.

[KJJ99] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology—CRYPTO'99*, pages 388–397. Springer, 1999. Cited on pages 4 and 115.

[KPW06] Cynthia Kuo, Adrian Perrig, and Jesse Walker. Designing an evaluation method for security user interfaces: lessons from studying secure wireless network configuration. *Journal of Interactions*, 13(3):28–31, 2006. Cited on page 45.

[Kra95] Sherry Kragler. The transition from oral to silent reading. *Reading Psychology: An International Quarterly*, 16(4):395–408, 1995. Cited on page 100.

[LAC^{+}04] Sharon J. Laskowski, Marguerite Autry, John Cugini, William Killam, and James Yen. Improving the usability and accessibility of voting systems and products. Technical report, National Institute of Standards and Technology, 2004. `http://user-centereddesign.com/files/NISTHFReport.pdf`, last accessed February, 7, 2016. Cited on page 63.

[Lee15] Seunghyun Lee. *Impact of universal design ballot interfaces on voting performance and satisfaction of people with and without vision loss.* PhD thesis, Georgia Institute of Technology, 2015. Cited on pages 9 and 10.

[Lev79] Harry Levin. Reading silently and aloud. *Perception and its development*, 1979. Cited on page 100.

[LFH10] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*, volume 1. John Wiley & Sons, 2010. Cited on pages xi, 39, 40, 41, 43, and 44.

[LR06] Sharon J Laskowski and Janice Redish. Making ballot language understandable to voters. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*, pages 1–1. USENIX Association, 2006. Cited on page 77.

[LS13] Kris Lohmann and Jörg Schäffer. System Usability Scale (SUS) – An Improved German Translation of the Questionnaire, 2013. `http://minds.coremedia.com/2013/09/18/sus-scale-an-improved-german-translation-questionnaire/`, last accessed February, 7, 2016. Cited on pages 89 and 104.

[LSX+13] Morgan Llewellyn, Steve Schneider, Zhe Xia, Chris Culnane, James Heather, Peter Y.A. Ryan, and Sriram Srinivasan. Testing Voters' Understanding of a Security Mechanism Used in Verifiable Voting. *The USENIX Journal of Election Technology and Systems (JETS)*, 1(1):53–61, 2013. Cited on pages 2, 9, 10, 48, 54, and 55.

[LUB+13] Benedikt Lebek, Jorg Uffen, Michael H. Breitner, Markus Neumann, and Bernd Hohler. Employees' information security awareness and behavior: A literature review. In *46th Hawaii International Conference on System Sciences (HICSS)*, pages 2978–2987. IEEE, 2013. Cited on page 80.

[Mac10] John Mace. Printer Identification Techniques and Their Privacy Implications. Technical Report CS-TR-1211, 2010. `http://www.cs.ncl.ac.uk/publications/trs/papers/1211.pdf`, last accessed February, 7, 2016. Cited on page 48.

[mar06] A Study of Vote Verification Technology Conducted for the Maryland State Board of Elections Part II: Usability Study, 2006. `http://www.cs.umd.edu/~bederson/voting/verification-study-jan-2006.pdf`, last accessed February, 7, 2016. Cited on pages 3, 73, 77, 78, 79, 81, and 113.

[Mar13] Sara J. Margolin. Can Bold Typeface Improve Readers' Comprehension and Metacomprehension of Negation? *Reading Psychology*, 34(1):85–99, 2013. Cited on pages 69 and 77.

[MCD09] Tamaryn Menneer, Kyle R. Cave, and Nick Donnelly. The cost of search for multiple targets: Effects of practice and target similarity.

Journal of Experimental Psychology: Applied, 15(2):125–139, 2009. Cited on page 100.

[MGO12] Damien MacNamara, Paul Gibson, and Ken Oakley. A preliminary study on a dualvote and prêt à voter hybrid system. In *Conference for E-Democracy and Open Government*, page 77. Edition Donau-Universität Krems, 2012. Cited on pages 9 and 10.

[MM10] David J. Madden and Stephen R. Mitroff. Aging and top-down attentional control in visual search, 2010. Institute for Homeland Security Solutions Research Brief. `https://www.ihssnc.org`, last accessed February, 7, 2016. Cited on pages 3 and 99.

[MSG+11] Damien MacNamara, Ted Scully, Paul J. Gibson, Francis Carmody, Ken Oakley, and Elizabeth Quane. DualVote: Addressing Usability and Verifiability Issues in Electronic Voting Systems. In Peter Parycek, Manuel J. Kripp, and Noella Edelmann, editors, *International Conference for E-Democracy and Open Government 2011*, pages 313–322. Edition Donau-Universität Krems, 2011. Cited on page 73.

[Nef03] Andrew C. Neff. Election Confidence: A Comparison of Methodologies and Their Relative Effectiveness at Achieving It, 2003. `http://www.verifiedvoting.org/wp-content/uploads/downloads/20031217.neff.electionconfidence.pdf`, last accessed February, 7, 2016. Cited on page 109.

[Nie94] Jakob Nielsen. Heuristic Evaluation. In *Usability Inspection Methods*. John Wiley and Sons, 1994. Cited on page 76.

[NKQC08] Lawrence Norden, David Kimball, Whitney Quesenbery, and Margaret Chen. Better ballots. Technical report, 2008. `http://www.brennancenter.org/sites/default/files/legacy/Democracy/Better%20Ballots.pdf`, last accessed February, 7, 2016. Cited on pages 17, 63, 80, and 100.

[NSN06] Donald F. Norris, Andrew Sears, and Charles Nicholas. A Study of Vote Verification Technologies Part I: Technical Study, 2006. `http://mipar.umbc.edu/files/2015/01/Vote-Verification-Study-Report-FINAL.pdf`, last accessed February, 7, 2016. Cited on pages 2 and 48.

[OBV13] Maina M. Olembo, Steffen Bartsch, and Melanie Volkamer. Mental models of verifiability in voting. In Vanessa Teague Steve Schneider, James Heather, editor, *4th International Conference on e-Voting and Identity (VoteID13)*, volume 7985 of *Lecture Notes in Computer Science*, pages 142 – 155. Springer, 2013. Cited on page 16.

[OdB04] Anne-Marie Oostveen and Peter Van den Besselaar. Internet voting technologies and civic participation: the users' perspective. *Javnost-the public*, 11(1):61–78, 2004. Cited on page 48.

[OdB09] Anne-Marie Oostveen and Peter Van den Besselaar. Users' experiences with e-voting: A comparative case study. *International Journal of Electronic Governance*, 2(4):357–377, 2009. Cited on pages 9, 10, and 48.

[ORBV14] Maina M. Olembo, Karen Renaud, Steffen Bartsch, and Melanie Volkamer. Voter, what message will motivate you to verify your vote? In *Workshop on Usable Security (USEC)*. Internet Society, 2014. Cited on page 78.

[ORSB08] Shannon O'Malley, Michael G. Reynolds, Jennifer A. Stolz, and Derek Besner. Reading aloud: spelling-sound translation uses central attention. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 34(2):422, 2008. Cited on page 100.

[OV13] Maina M. Olembo and Melanie Volkamer. *E-Voting System Usability: Lessons for Interface Design, User Studies, and Usability Criteria*, chapter 11, pages 172 – 201. IGI Global, 2013. Cited on page 7.

[PE08] Bryan D Payne and Keith W. Edwards. A brief introduction to usable security. *Internet Computing*, 12(3):13–21, 2008. Cited on page 15.

[PLA+14] Julia Pomares, Ines Levin, Michael R. Alvarez, Guillermo Mirau, and Teresa Ovejero. From piloting to roll-out: voting experience and trust in the first full e-election in argentina. In Robert Krimmer and Melanie Volkamer, editors, *Proceedings of the 6th International Conference on Electronic Voting (EVOTE): Verifying the Vote*, pages 1–10. IEEE, 2014. Cited on pages 9, 10, and 56.

[Poz14] Juan Pozo. Implementation Project Electronic Voting Azuay – Ecuador 2014. In Robert Krimmer and Melanie Volkamer, editors, *Proceedings of the 6th International Conference on Electronic Voting (EVOTE)*, pages 47–60. TUT Press, Tallinn, 2014. Cited on page 56.

[Ric12] Philip Richter. *Wahlen im Internet rechtsgemäß gestalten*. PhD thesis, Universität Kassel, 2012. Cited on page 31.

[RKW+08] Anina N. Rich, Melina A. Kunar, Michael J. Van Wert, Barbara Hidalgo-Sotelo, Todd S. Horowitz, and Jeremy M. Wolfe. Why do we miss rare targets? Exploring the boundaries of the low prevalence effect. *Journal of Vision*, 8(15):15, 2008. Cited on page 100.

[RL09] Janice G. Redish and Sharon J. Laskowski. Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers. Technical Report 7596, National Institute of Standards and Technology, 2009. `http://www.nist.gov/itl/vote/upload/032906PlainLanguageRpt-2.pdf`, last accessed February, 7, 2016. Cited on pages 63, 75, 76, and 77.

[Rog75] Ronald W Rogers. A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology: Interdisciplinary and Applied*, 91(1):93–114, 1975. Cited on pages 47, 57, 58, and 113.

[Sau11] Jeff Sauro. Measuring Usability With The System Usability Scale (SUS), 2011. `http://www.measuringu.com/sus.php`, last accessed February, 7, 2016. Cited on pages 97, 108, and 114.

[SC90] Anselm Strauss and Juliet Corbin. *Basics of qualitative research*, volume 15. Sage Publications, 1990. Cited on page 52.

[Sch00] Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2000. Cited on page 16.

[SDNK+13] Daniela Simić-Draws, Stephan Neumann, Anna Kahlert, Philipp Richter, Rüdiger Grimm, Melanie Volkamer, and Alexander Roßnagel. Holistic and law compatible it security evaluation: Integration of common criteria, iso 27001/it-grundschutz and kora. *International Journal of Information Security and Privacy (IJISP)*, 7(3):16–35, 2013. Cited on page 4.

[Sel04] Ted Selker. Processes can improve electronic voting: a case study of an election. 2004. `http://www.vote.caltech.edu/sites/default/`

files/vtp_wp19.pdf, last accessed February, 7, 2016. Cited on pages 3, 73, 77, 78, 79, 81, and 113.

[SF05] Angela M. Sasse and Ivan Flechais. Usable Security: Why Do We Need It? How Do We Get It? chapter 2, pages 13–30. O'Reilly Media, Inc., 2005. Cited on page 16.

[SGH+06] Alan T. Sherman, Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, Gunes A. Koru, Chris M. Law, Donald F. Norris, John Pinkston, Andrew Sears, and Dongsong Zhang. An examination of vote verification technologies: Findings and experiences from the Maryland Study. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*, pages 10–10. USENIX Association, 2006. Cited on pages 9 and 10.

[SHB10] Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 'I did it because I trusted you': Challenges with the study environment biasing participant behaviours. In *SOUPS Usable Security Experiment Reports (USER) Workshop*, 2010. Cited on page 46.

[SHGS05] Ted Selker, Matt Hockenberry, John Goler, and Shawn Sullivan. Orienting graphical user interfaces reduces errors: The low error voting interface. 2005. Cited on pages 31 and 78.

[SJWM06] Debbie Stone, Caroline Jarrett, Mark Woodroffe, and Shailey Minocha. User interface design and evaluation. *Information Visualization*, 5(1):77–78, 2006. Cited on page 32.

[SLC+11] Steve Schneider, Morgan Llewellyn, Chris Culnane, James Heather, Sriramkrishnan Srinivasan, and Zhe Xia. Focus group views on prêt à voter 1.0. In *International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE)*, pages 56–65. IEEE, 2011. Cited on pages 9 and 10.

[SMA16] SMARTMATIC. Voting technology and services, 2016. http://www.smartmatic.com/voting/hardware/, last accessed February, 7, 2016. Cited on page 73.

[SMN+13] Tim Storer, Stephen Marsh, Sylvie Noël, Babak Esfandiari, Khalil El-Khatib, Pam Briggs, Karen Renaud, and Mehmet V. Bicakci. Encouraging second thoughts: obstructive user interfaces for raising security awareness. In *2013 Eleventh Annual Conference on Privacy, Security and Trust*, 2013. Cited on page 16.

[SP06] Ted Selker and Anna Pandolfo. A methodology for testing voting systems. *Journal of Usability Studies*, 2(1):7–21, 2006. Cited on pages 3, 7, 73, 77, 78, 81, 82, and 113.

[SS75] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975. Cited on page 15.

[ST14] Philip B. Stark and Vanessa Teague. Veriable european elections: Risk-limiting audits for d'hondt and its relatives. *The USENIX Journal of Election Technology and Systems (JETS)*, 1(3):18–39, 2014. Cited on page 109.

[SVB10] Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. An evaluation and certification approach to enable voting service providers. In Rüdiger Grimm Robert Krimmer, editor, *Electronic Voting 2010, EVOTE 2010, 4th International Conference, Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC, July 21st - 24th, 2010, in Castle Hofen, Bregenz, Austria*, volume 167 of *LNI*, pages 135–148. GI, 2010. Cited on page 4.

[Swa72] James E. Swalm. A comparison of oral reading, silent reading and listening comprehension. *Education*, 92(4):111–5, 1972. Cited on page 100.

[Swa12] Melanie Swan. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks*, 1(3):217–253, 2012. Cited on page 16.

[THhP+05] Michael W. Traugott, Michael Hanmer, Won ho Park, Paul Herrnson, Richard Niemi, Ben B. Bederson, and Frederick G. Conrad. The impact of voting systems on residual votes, incomplete ballots, and other measures of voting behavior. In *Annual conference of the Midwest Political Science Association*, pages 7–10, 2005. Cited on pages 17 and 81.

[Tid10] Jenifer Tidwell. *Designing interfaces.* O'Reilly Media, 2010. Cited on page 31.

[VBD11] Melanie Volkamer, Jurlind Budurushi, and Denise Demirel. Vote casting device with VV-SV-PAT for elections with complicated ballot papers. In *International Workshop on Requirements Engineering for Electronic Voting Systems (REVOTE)*, pages 1–8. IEEE, 2011. Cited on pages 1, 2, 10, 19, 25, 33, and 63.

[vBSB13] Joost van Beusekom, Faisal Shafait, and Thomas M. Breuel. Automatic authentication of color laser print-outs using machine identification codes. *Pattern Analysis and Applications*, 16(4):663–678, 2013. Cited on page 48.

[vBSN+09] Jan vom Brocke, Alexander Simons, Bjoern Niehaves, Bjorn Niehaves, Kai Reimer, Ralf Plattfaut, and Anne Cleven. Reconstructing the giant: on the importance of rigour in documenting the literature search process. In *Proceedings of the European Conference on Information Systems*, volume 9, pages 2206–2217, 2009. Cited on page 5.

[VE85] Wim Van Eck. Electromagnetic radiation from video display units: an eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985. Cited on pages 4 and 115.

[Veg12] Carlos Vegas. The new belgian e-voting system. In Arslan Brömme and Christoph Busch, editors, *Proceedings of the 5th International Conference on Electronic Voting (EVOTE)*, pages 199–211. Bonn: Gesellschaft für Informatik (GI), 2012. Cited on pages 3, 4, 10, 11, 47, 73, and 108.

[VEOS13] Anthony Vance, David Eargle, Kirk Ouimet, and Detmar Straub. Enhancing password security through interactive fear appeals: A web-based field experiment. In *46th Hawaii International Conference on System Sciences (HICSS)*, pages 2988–2997. IEEE, 2013. Cited on page 80.

[Vol09] Melanie Volkamer. *Evaluation of Electronic Voting -Requirements and Evaluation Procedures to Support Responsible Election Authorities*. Springer, 2009. Cited on page 4.

[Vot08] Vot.ar. Vot.ar., 2008. `http://www.vot-ar.com.ar/`, last accessed February, 7, 2016. Cited on pages 3, 4, 47, 73, and 108.

[VR13] Melanie Volkamer and Karen Renaud. Mental models–general introduction and review of their application to human-centred security. In *Number Theory and Cryptography*, pages 255–280. Springer, 2013. Cited on page 16.

[WBB+15] Peter Wolf, Jordi Barrat, Eden Bolo, Alejandro Bravo, Robert Krimmer, Stephan Neumann, Al A. Parreño, Carsten Schürmann, and Melanie Volkamer. *Certification of ICTs in Elections*. 2015. Cited on page 4.

[WBP+09] Marco Winckler, Regina Bernhaupt, Philippe Palanque, David Lundin, Kieran Leach, Peter Y. A. Ryan, Eugenio Alberdi, and Lorenzo Strigini. Assessing the usability of open verifiable e-voting systems: a trial with the system Prêt à Voter. *International Conference on Theory and Practice of Electronic Governance*, pages 281–296, 2009. Cited on pages 9 and 10.

[WHK05] Jeremy M. Wolfe, Todd S. Horowitz, and Naomi M. Kenner. Cognitive psychology: Rare items often missed in visual searches. *Nature*, 435(7041):439–440, 2005. Cited on pages 3 and 99.

[WHW+07] Jeremy M. Wolfe, Todd S. Horowitz, Michael J. Van Wert, Naomi M. Kenner, Skyler S. Place, and Nour Kibbi. Low target prevalence is a stubborn source of errors in visual search tasks. *Journal of Experimental Psychology: General*, 136(4):623, 2007. Cited on page 100.

[WV08] Komminist Weldemariam and Adolfo Villafiorita. Modeling and Analysis of Procedural Security in (e)Voting: The Trentino's Approach and Experiences. In *Proceedings of the USENIX Workshop on Electronic Voting Technology*, pages 1–10. USENIX, 2008. Cited on page 73.

[WW02] Jane Webster and Richard T. Watson. Analyzing the past to prepare for the future: writing a literature review. *Management Information Systems Quarterly*, 26(2):13–23, 2002. Cited on page 5.

[Yee04] Ka-Ping Yee. Aligning security and usability. *IEEE Security & Privacy*, (5):48–55, 2004. Cited on page 15.

[YW90] Stephen L. Young and Michael S. Wogalter. Comprehension and memory of instruction manual warnings: Conspicuous print and pictorial icons. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 32(6):637–649, 1990. Cited on page 66.

[ZF97] Barbara Zenger and Manfred Fahle. Missed targets are more frequent than false alarms: A model for error rates in visual search. *Journal of Experimental Psychology: Human Perception and Performance*, 23(6):1783, 1997. Cited on page 100.

Appendices

A. Interfaces for the vote casting process

Figure 1 to Figure 8 introduce all interfaces for the vote casting process.

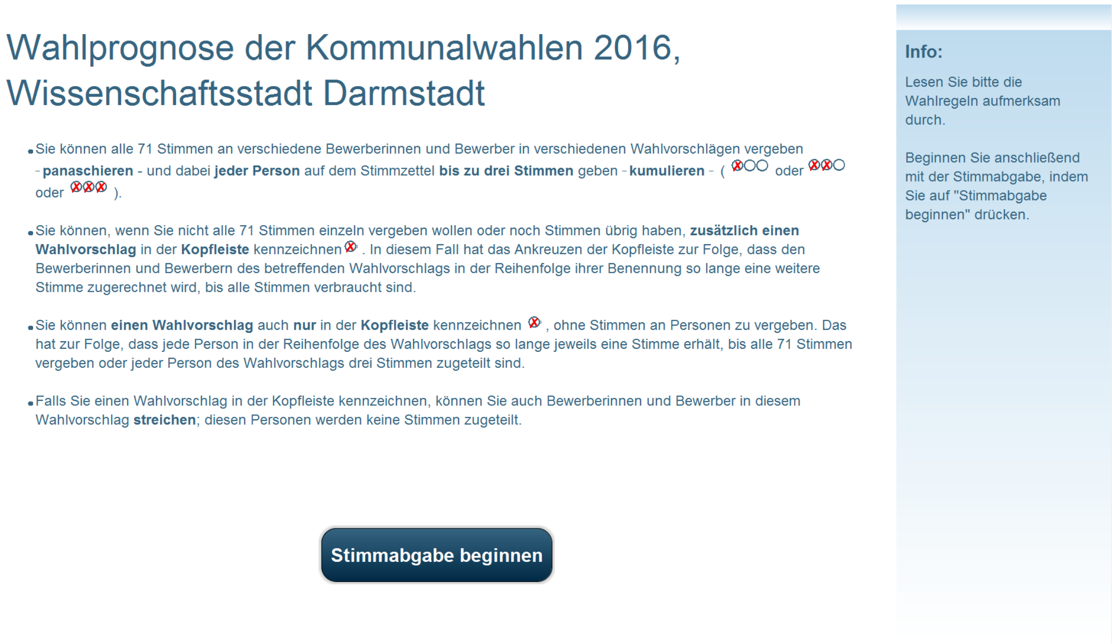

Figure 1: Vote casting prototype: Welcome screen containing the voting rules.

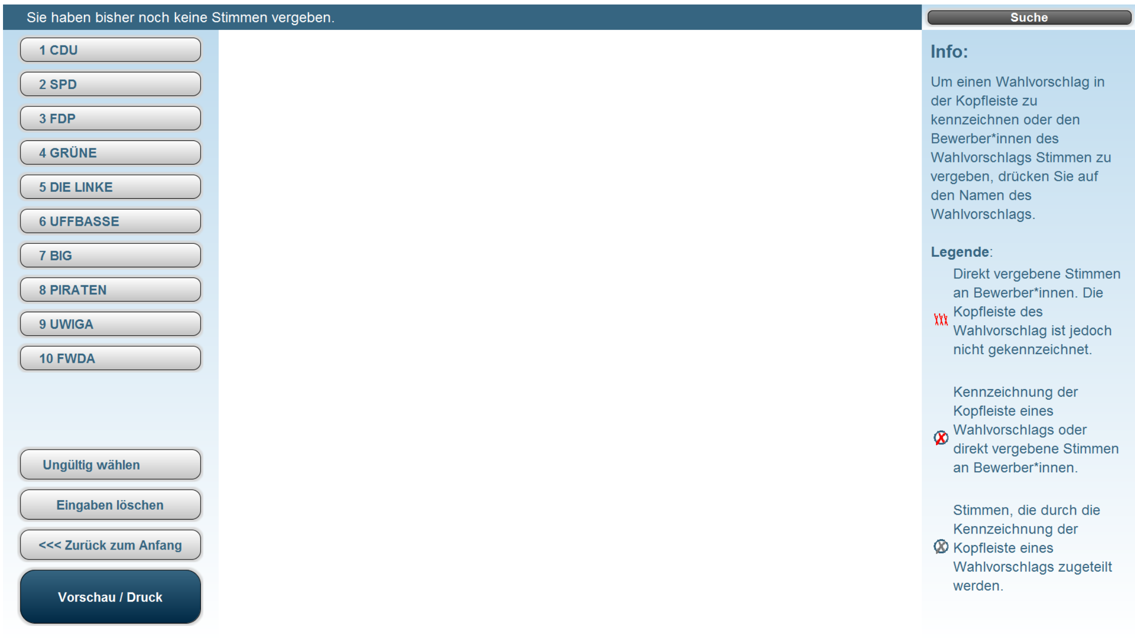

Figure 2: Vote casting prototype: Main screen.

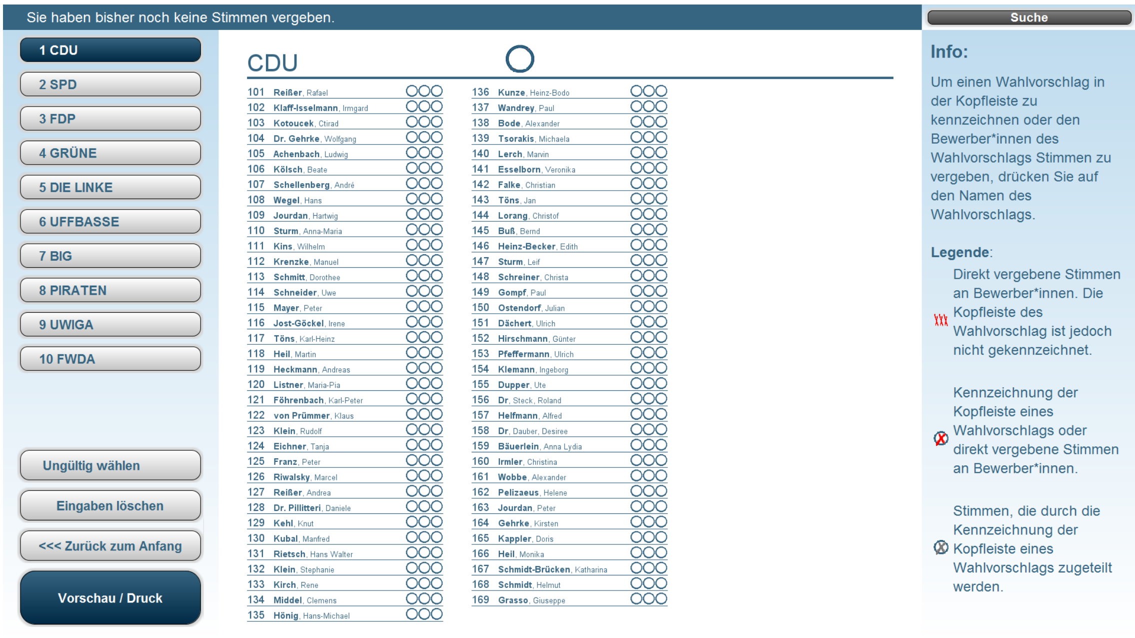

Figure 3: Vote casting prototype: Showing the candidates of the CDU party.

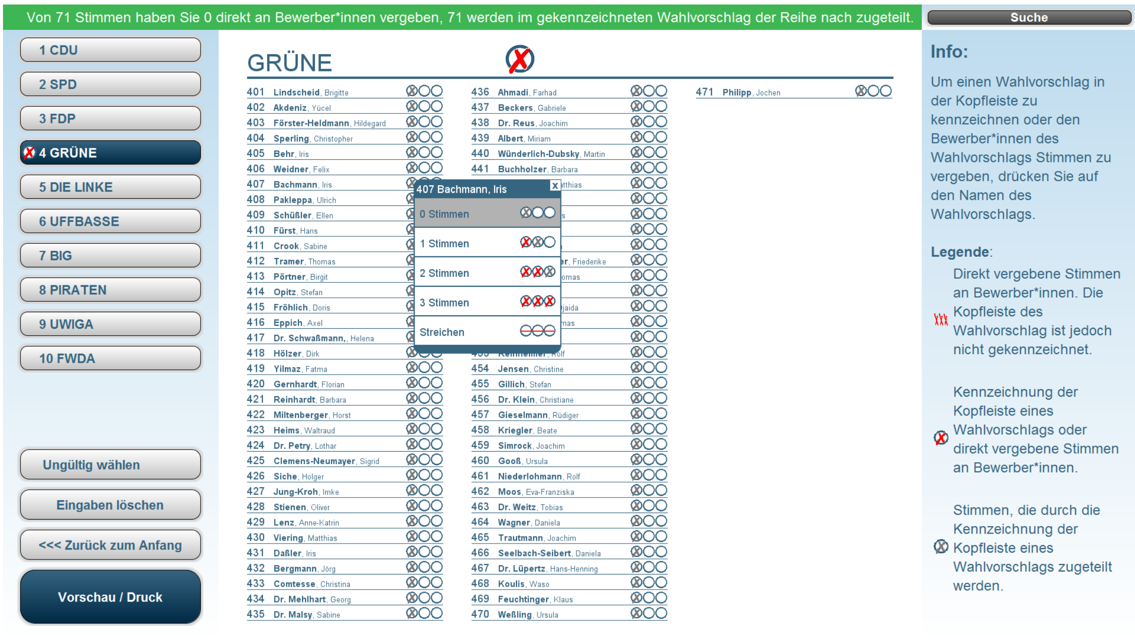

Figure 4: Vote casting prototype: Searching for a candidate using the search function.

Figure 5: Vote casting prototype: Casting direct votes to candidate number 407.

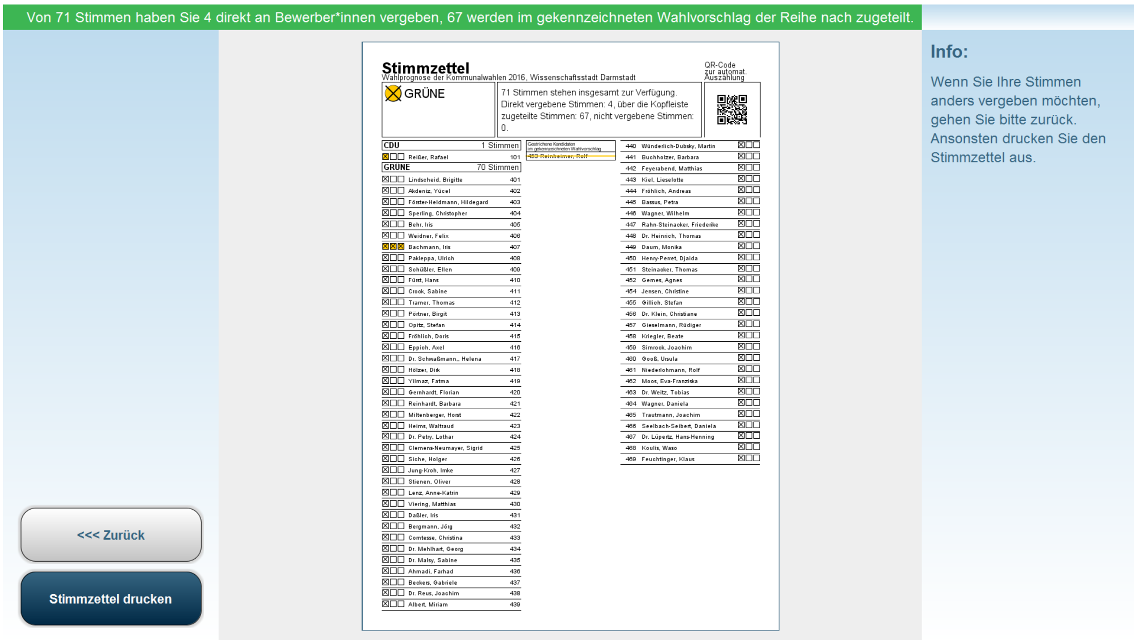

Figure 6: Vote casting prototype: View on the current selections in the GRÜNE party.

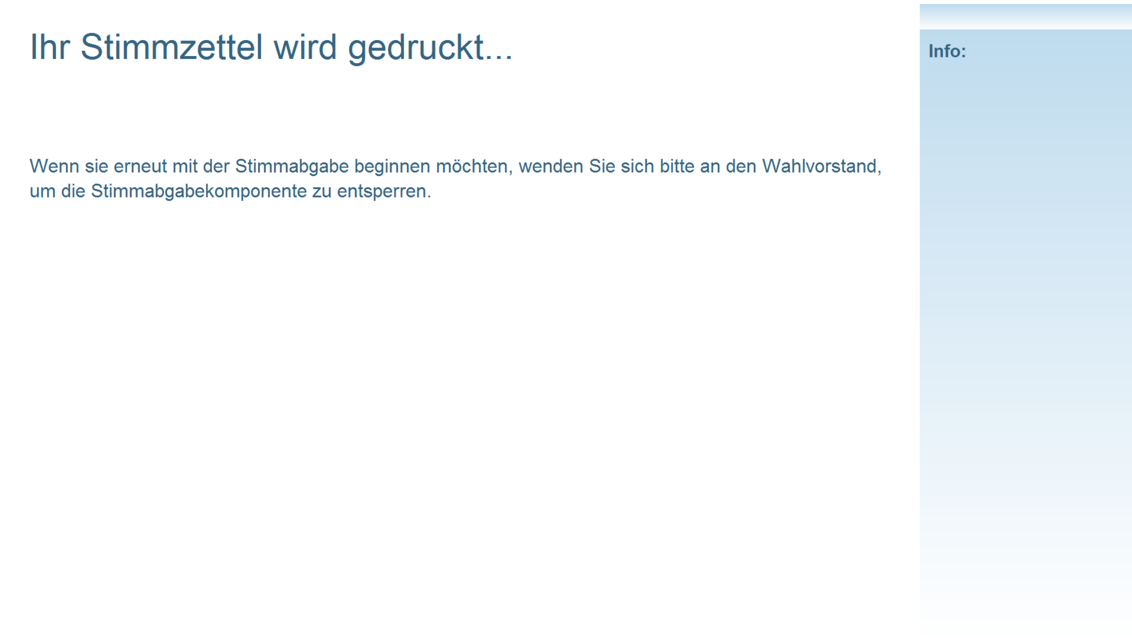

Figure 7: Vote casting prototype: Review screen.

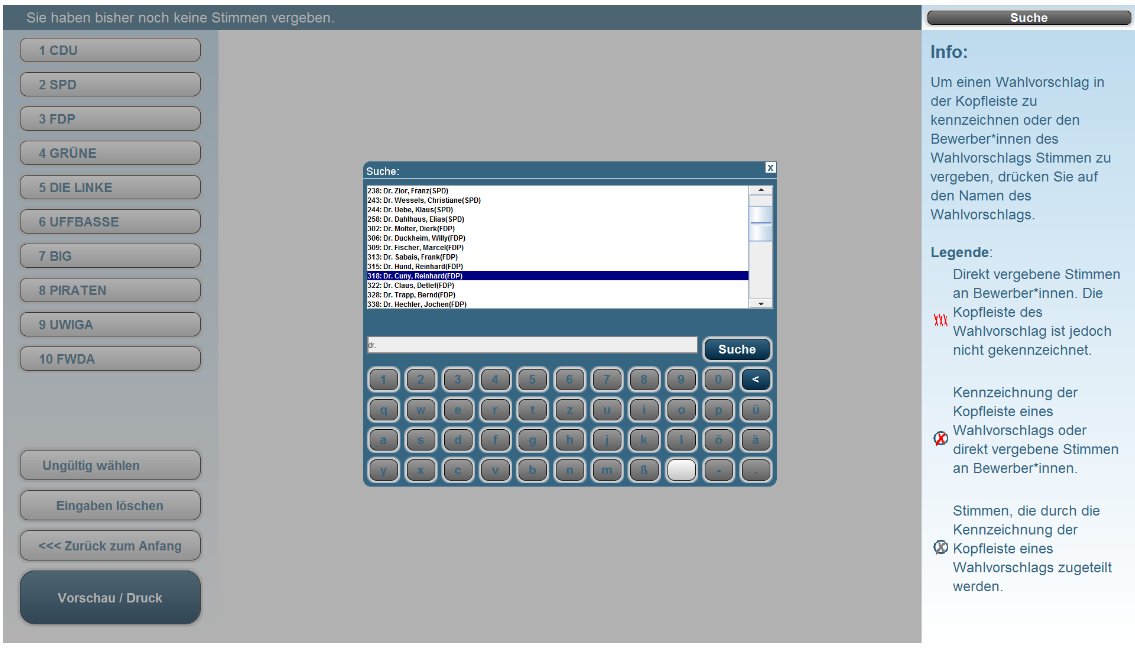

Figure 8: Vote casting prototype: Ballot is printed and the voting device is disabled.

B. Vote casting instructions for voters

Figure 9 introduces the developed poster, which served to instruct voters on how to cast a vote with EasyVote.

Figure 9: Poster: Vote casting instructions for voters.

C. Training workshop for electoral officials

Figure 10: Training for electoral officials: First slide.

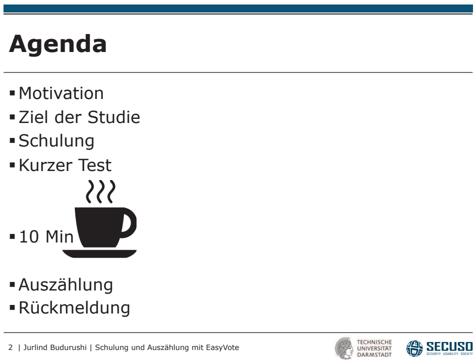

Figure 11: Training for electoral officials: Second slide.

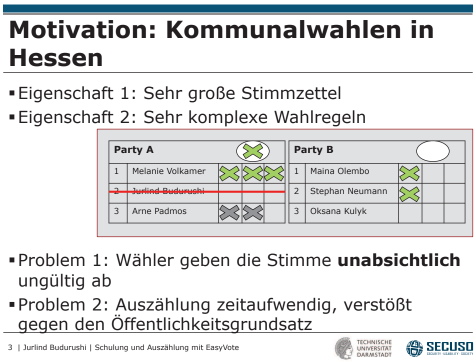

Figure 12: Training for electoral officials: Third slide.

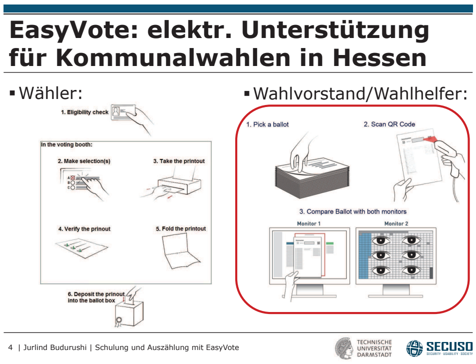

Figure 13: Training for electoral officials: Fourth slide.

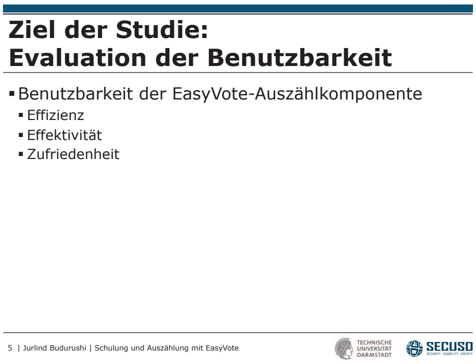

Figure 14: Training for electoral officials: Fifth slide.

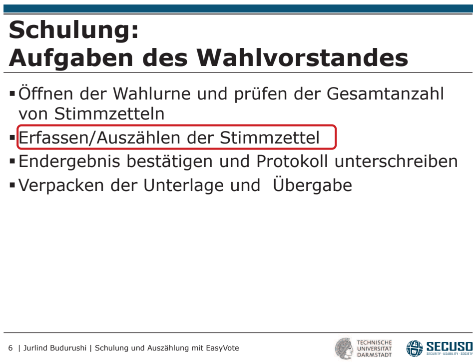

Figure 15: Training for electoral officials: Sixth slide.

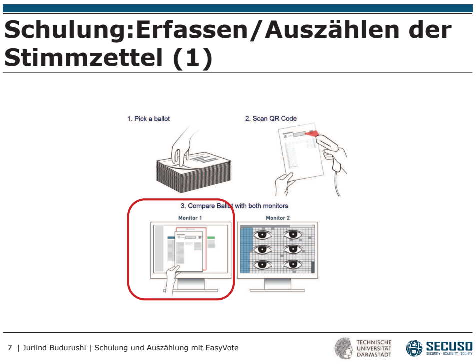

Figure 16: Training for electoral officials: Seventh slide.

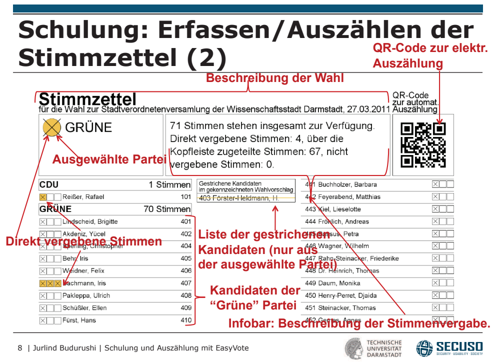

Figure 17: Training for electoral officials: Eighth slide.

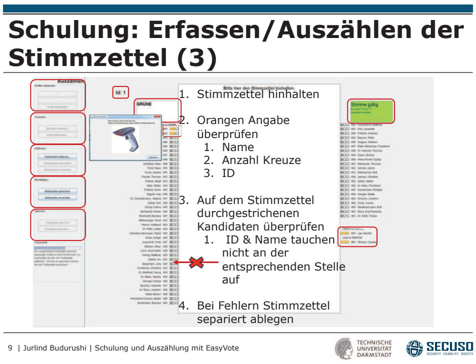

Figure 18: Training for electoral officials: Ninth slide.

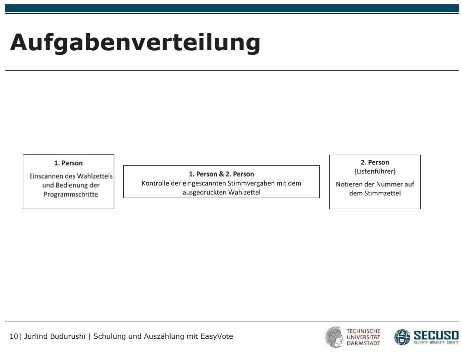

Figure 19: Training for electoral officials: Tenth slide.

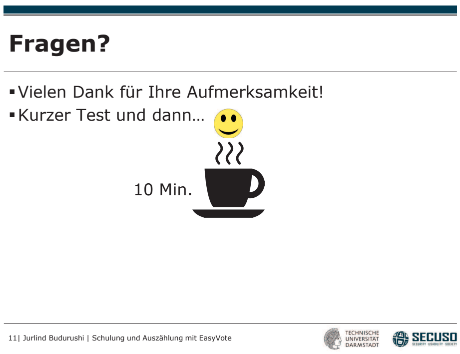

Figure 20: Training for electoral officials: Eleventh slide.

Wissenschaftlicher Werdegang

Mai 2012 - März 2016 Wissenschaftlicher Mitarbeiter und Promotionsstudent am Lehrstuhl von Professorin Melanie Volkamer, Fachbereich Informatik, Fachgebiet Benutzbarkeit von IT-Sicherheitslösungen, Technische Universität Darmstadt

Oktober 2010 - April 2012 Studium der Informatik (Master IT-Sicherheit) an der Technischen Universität Darmstadt

Oktober 2010 - April 2012 Studium der Informatik (Master) an der Technischen Universität Darmstadt

Oktober 2004 - September 2010 Studium der Informatik (Bachelor) an der Technischen Universität Darmstadt

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit – abgesehen von den in ihr ausdrücklich genannten Hilfen – selbständig verfasst habe.

Darmstadt, ________________________