Privacy and Verifiability in Electronic Voting

Vom Fachbereich Informatik
der Technischen Universität Darmstadt
genehmigte

Dissertation

zur Erlangung des Grades
Doktor-Ingenieur (Dr.-Ing.)

von

Dipl.-Math. Barbara Lucie Langer
geboren in Darmstadt

Referenten: Prof. Dr. Johannes Buchmann
Prof. Dr. Rüdiger Grimm

Tag der Einreichung: 31. August 2010
Tag der mündlichen Prüfung: 20. Oktober 2010

Darmstadt 2010
Hochschulkennziffer D 17

To Jorge Cham

www.phdcomics.com

Wissenschaftlicher Werdegang

August 2006 – Juni 2010
Wissenschaftliche Mitarbeiterin und Doktorandin bei Prof. Johannes Buchmann am Lehrstuhl für Kryptographie und Computeralgebra an der Technischen Universität Darmstadt

Oktober 2003 – Juli 2006
Studium der Mathematik mit Schwerpunkt Informatik an der Technischen Universität Darmstadt und der Karlsuniversität Prag

September 2000 – Mai 2004
Studium der Mathematik mit Schwerpunkt Technik und Naturwissenschaften an der Fachhochschule Darmstadt

Erklärung

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

Selected publications

Book chapter

[1] Lucie Langer. Long-Term Verifiability of Remote Electronic Elections. In *Practical Studies in E-Government: Best Practices from Around the World*, chapter 8. To be published by Springer on Nov 28, 2010.

Journal articles

[2] Lucie Langer, Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. Ein PKI-basiertes Protokoll für sichere und praktikable Onlinewahlen. *eJournal of eDemocracy and Open Government (JeDEM)*, 2(1), 2010.

[3] Lucie Langer and Zoi Opitz-Talidou. Elektronische Aufbewahrung von Wahldokumenten bei Onlinewahlen: Beweggründe, rechtliche Anforderungen und technische Umsetzung. *Datenschutz und Datensicherheit (DuD)*, 33(7):418–422, 2009.

[4] Lucie Langer, Axel Schmidt, and Melanie Volkamer. Verifizierbarkeit elektronischer Wahlen. *eGovernment Review*, 2(4):20–21, July 2009.

Conference papers

[5] Lucie Langer, Hugo Jonker, and Wolter Pieters. Anonymity and Verifiability in Voting: Understanding (Un)Linkability. In *12th International Conference on Information and Communications Security (ICICS)*, 2010. To be published by Springer in the series *Lecture Notes in Computer Science*.

[6] Philipp Richter, Lucie Langer, Katharina Hupf, Melanie Volkamer, and Johannes Buchmann. Verifizierbarkeit und Öffentlichkeitsgrundsatz bei elektronischen Wahlen. In Erich Schweighofer, Anton Geist, and Ines Staufer, editors, *Globale Sicherheit und proaktiver Staat – Die Rolle der Rechtsinformatik, Tagungsband des 13. Internationalen Rechtsinformatik Symposions (IRIS)*, volume 266 of *books@ocg.at*, pages 61–66. OCG, 2010.

[7] Lucie Langer, Axel Schmidt, Johannes Buchmann, and Melanie Volkamer. A Taxonomy Refining the Security Requirements for Electronic Voting: Analyzing Helios as a Proof of Concept. In *Fifth International Conference on Availability, Reliability and Security (ARES)*, pages 475–480. IEEE Computer Society, 2010.

[8] Detlef Hühnlein, Ulrike Korte, Lucie Langer, and Alexander Wiesmaier. A Comprehensive Reference Architecture for Trustworthy Long-Term Archiving of Sensitive Data. In Khaldoun Al Agha, Mohamad Badra, and Gregory B. Newby, editors, *3rd International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5. IEEE, 2009.

[9] Lucie Langer, Melanie Volkamer, Stefan G. Weber, Axel Schmidt, and Johannes Buchmann. Towards Long-Term Free and Secret Electronic Elections Providing Voter-Verifiability in the Bulletin Board Model. In Jim Davies and Tomasz Janowski, editors, *3rd International Conference on Theory and Practice of Electronic Governance (ICEGOV)*, volume 322 of *ACM International Conference Proceeding Series*, pages 203–210. ACM, 2009.

[10] Lucie Langer, Axel Schmidt, Melanie Volkamer, and Johannes Buchmann. Classifying Privacy and Verifiability Requirements for Electronic Voting. In Stefan Fischer, Erik Maehle, and Rüdiger Reischuk, editors, *Im Focus das Leben, Beiträge der 39. Jahrestagung der Gesellschaft für Informatik e.V. (INFORMATIK)*, volume 154 of *Lecture Notes in Informatics*, pages 1837–1846. GI, 2009.

[11] Lucie Langer, Melanie Volkamer, Axel Schmidt, Alexander Stolfik, and Johannes Buchmann. Towards a Framework on the Security Requirements for Electronic Voting Protocols. In *First International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE)*, pages 61–68. IEEE Computer Society, 2009.

[12] Lucie Langer and Zoi Opitz-Talidou. Elektronische Aufbewahrung bei Onlinewahlen aus rechtlicher und sicherheitstechnischer Sicht. In *Semantisches und soziales Web und Recht, Tagungsband des 12. Internationalen Rechtsinformatik Symposions (IRIS)*, volume 259 of *books@ocg.at*. OCG, 2009.

[13] Lucie Langer. Towards Legally Binding Online Elections in Germany. In Dan Remenyi, editor, *4th International Conference on e-Government (ICEG)*, pages 247–254. ACI, 2008.

[14] Lucie Langer, Axel Schmidt, and Roberto Araujo. A Pervasively Verifiable Online Voting Scheme. In Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, and Christian Scheideler, editors, *Beherrschbare Systeme – dank Informatik, Beiträge der 38. Jahrestagung der Gesellschaft für Informatik e.V. (INFORMATIK)*, volume 133 of *Lecture Notes in Informatics*, pages 457–462. GI, 2008.

[15] Rotraud Gitter, Lucie Langer, Susanne Okunick, and Zoi Opitz-Talidou. Long-term Retention in E-Voting – Legal Requirements and Technical Implementation. In Robert Krimmer and Rüdiger Grimm, editors, *3rd International Conference on Electronic Voting (EVOTE)*, volume 131 of *Lecture Notes in Informatics*, pages 109–126. GI, 2008.

Acknowledgments

I would like to thank Johannes Buchmann, Rüdiger Grimm, Melanie Volkamer, Philipp Richter, Axel Schmidt, Alex Wiesmaier, Anja Lehmann, Roswitha Jäger-Beck, Marita Skrobic, and Daniel Olapade.

My work was financially supported by the Federal Ministry of Economics and Technology (BMWi) and the Research Institute for Interdisciplinary Studies on Politics, Law, Administration and Technology (ISPRAT).

Lucie Langer
Vienna, October 2010

Zusammenfassung

Privatheit und Verifizierbarkeit entsprechen fundamentalen Prinzipien demokratischer Wahlen und gehören deshalb zu den Sicherheitsanforderungen, die jedes elektronische Wahlsystem erfüllen muss. Dennoch existieren sehr unterschiedliche Ideen und Auffassungen von Privatheit und Verifizierbarkeit innerhalb der Wissenschaftsgemeinde. Obwohl die gewünschten Eigenschaften eines Wahlprotokolls außerdem getrennt vom jeweiligen Angreifermodell betrachtet werden sollten, beinhalten die Sicherheitsanforderungen der Quittungsfreiheit und Unzwingbarkeit, die in engem Bezug zur Privatheit stehen, implizite Annahmen hinsichtlich bestimmter Angreifermächtigkeiten, was die Analyse von Wahlprotokollen zusätzlich erschwert.

Der erste Teil dieser Arbeit stellt eine Taxonomie für Privatheit und Verifizierbarkeit bei elektronischen Wahlen vor. Wir stellen mögliche Stufen dieser beiden Anforderungen zusammen und untersuchen die Zusammenhänge zwischen Privatheit und Verifizierbarkeit. Dazu führen wir ein Begriffsmodell ein, welches beide Eigenschaften erfasst. Wir erstellen außerdem eine Liste möglicher Angreifermächtigkeiten, die als Basis für ein individuelles Angreifermodell dienen können.

Die Taxonomie trägt zu einem tieferen Verständnis von Privatheit und Verifizierbarkeit und dem Zusammenhang zwischen diesen beiden Eigenschaften bei. Wir zeigen, dass die Taxonomie zur Sicherheitsanalyse von Wahlprotokollen verwendet werden kann, indem die erreichte Stufe an Privatheit und Verifizierbarkeit in Abhängigkeit von den zugrunde gelegten Angreifermächtigkeiten bestimmt wird. Die Taxonomie erlaubt es außerdem, adäquate Stufen dieser beiden Sicherheitsanforderungen für verschiedene Wahlszenarien auszuwählen und ein angemessenes Angreifermodell festzulegen.

Der zweite Teil dieser Arbeit betrachtet langfristige Aspekte der Verifizierbarkeit bei Internetwahlen. Aufgrund einer möglichen Wahlanfechtung muss die Rechtmäßigkeit jeder gesetzlich bindenden Wahl auch nach Jahren beweisbar sein. Dazu müssen bestimmte Wahldokumente, wie zum Beispiel die Stimmzettel, aufbewahrt werden. Die Wahlunterlagen werden üblicherweise für die Dauer der Amtszeit des gewählten Organs archiviert. Bei laufenden Wahlprüfungsverfahren kann die notwendige Aufbewahrungsdauer jedoch ausgedehnt werden. Aufbewahrungspflichten gelten nicht nur für gewöhnliche papierbasierte Wahlen, sondern auch für Internetwahlen. Im Gegensatz zu Papierwahlen existieren für Internetwahlen jedoch keinerlei Bestimmungen oder Richtlinien hinsichtlich der Aufbewahrung elektronischer Wahldokumente. Insbesondere ist offen, welche Daten hierbei überhaupt zu archivieren sind.

Im zweiten Teil dieser Arbeit werden die Wahldokumente identifiziert, welche bei einer Internetwahl aufbewahrt werden müssen, um den korrekten Ablauf der Wahl nachweisen zu können. Ausgehend von gesetzlichen Bestimmungen für Bundestagswahlen leiten wir Anforderungen hinsichtlich der Aufbewahrung von Internetwahldaten ab und machen konkrete Vorschläge für die Umsetzung dieser Anforderungen.

Die Einführung von Internetwahlen auf parlamentarischer Ebene setzt voraus, dass ihre technische Umsetzung gesetzliche Anforderungen erfüllt, zu denen auch eine beweiskräftige Aufbewahrung von Wahldaten gehört. Unsere Arbeit trägt daher dazu bei, Internetwahlen als zusätzliche Option bei Bundestagswahlen zu etablieren, und kann gesetzgebende Organe darin unterstützen, eine entsprechende gesetzliche Basis zu schaffen. Weiterhin ist diese Arbeit bei der Entwicklung gesetzeskonformer Wahlsysteme von Wert, da die Notwendigkeit der Aufbewahrung bereits beim Entwurf von Wahlprotokollen berücksichtigt werden sollte.

Abstract

Privacy and verifiability refer to fundamental principles of democratic elections and therefore belong to the set of established security requirements which each electronic voting scheme is expected to meet. However, very different ideas and opinions about privacy and verifiability exist in the scientific community, which shows that both properties are not well understood yet. Moreover, although the desired properties (captured by the security requirements) should be separated from the assumed adversary model (expressed by adversary capabilities), specific adversary capabilities are inherently assumed for the privacy-related security requirements of receipt-freeness and coercion-resistance, which complicates the analysis of voting schemes.

The first part of this thesis presents a taxonomy for privacy and verifiability in electronic voting. We compile the conceivable levels of privacy and verifiability and investigate the relation between both properties. To this end, we introduce a conceptual model capturing both privacy and verifiability. We also provide a comprehensive adversary model for electronic voting by considering different adversary capabilities. The conceptual model, the levels of privacy and verifiability, and the adversary capabilities together form our taxonomy for privacy and verifiability in electronic voting.

The presented taxonomy provides a deeper understanding of privacy and verifiability and their correlation in electronic voting. We show how the taxonomy can be used to analyze the security of voting schemes by identifying the level of privacy and verifiability provided depending on the adversary capabilities assumed. Moreover, the taxonomy allows to select appropriate levels of the requirements for different types of elections, and to determine reasonable adversary models for individual election scenarios.

The second part of this thesis considers long-term aspects of verifiability in remote electronic voting. The lawfulness of any legally binding election must be provable for several years due to possible scrutiny proceedings. Therefore, specific documents such as the ballots must be retained. The election records are usually retained for the legislative period of the elected body; however, this period may be extended if scrutiny procedures are pending. Retention obligations apply not only to conventional paper-based elections, but also to remote electronic voting. But contrary to the case of paper-based elections, general regulations or guidelines on retention of remote electronic election data have not been issued so far. In particular, the question which records should be retained is yet unanswered.

The second part of this thesis sets out to identify the election records that have to be retained in order to prove the proper conduct of a remote electronic election. We derive retention requirements for online elections from legal regulations which apply

to Federal Elections for the German Bundestag, and we make recommendations on how to meet these requirements.

Establishing Internet voting in parliamentary elections presupposes that its technical implementation meets certain legal requirements, and conclusive retention of election data is one of them. Thus, our work contributes to establishing online voting as an additional voting channel in parliamentary elections in Germany. It may support legislative organs when issuing a legal framework on remote electronic voting. Moreover, our work is valuable for developing legally compliant voting systems as the need for record keeping should be considered already when designing and implementing a remote electronic voting scheme.

Contents

List of Figures

List of Tables

1. Introduction

A fundamental principle of democratic elections is voter privacy, also known as secrecy of the vote. It requires that only the voter knows his voting decision and nobody else is able to gain information about it. Moreover, voter privacy is a precondition for expressing one's preference freely and without coercion. Therefore, privacy is not only an option which the voter is being offered—it must be enforced. In the controlled environment of a polling station, this is established by requiring the voters to fill in their ballot paper at tables equipped with privacy shields. For remote electronic voting in uncontrolled environments, the privacy-related requirements of receipt-freeness and coercion-resistance are usually imposed on the voting scheme. This shall prevent the voter from selling his vote, and protect him from being forced to abstain from voting or to vote in a specific way.

Transparency is another fundamental principle of democratic elections. Due to the public nature of democratic elections, all of their essential steps are subject to the possibility of public scrutiny. In conventional paper-based elections taking place at polling stations, transparency is established by allowing the interested public to be present during polling and tallying. As this kind of physical observation is not achievable for electronic elections, transparency is established by means of verifiability, which comes in two forms: while individual verifiability allows each voter to be assured that his vote was properly taken into account, universal verifiability gives anyone the possibility to verify the correct processing and tallying of the votes.

Although privacy and verifiability play a major role in electronic voting, we will see that both properties are not well understood yet. Therefore, this thesis sets out to explore privacy and verifiability in electronic voting.

Chapter overview

We motivate our work in Section 1.1. In Section 1.2 we formulate our research questions and outline the methodology used to answer them. Our contribution is presented in Section 1.3. An outline of this thesis and instructions for reading are given in Section 1.4. As this thesis consists of two independent parts, each of the Sections 1.1 to 1.4 is divided in two parts accordingly.

1.1. Motivation

Part I: A Taxonomy for Privacy and Verifiability in Electronic Voting

A plethora of remote electronic voting protocols has been proposed in the past (for a survey see [LGT+03, SP06]), and a number of promising electronic voting schemes for use in polling stations has also been developed, for example [BMQR07, CCC+08, CRS05, Nef04]. There is one thing they all have in common: each voting scheme is expected to meet the security requirements which have been established for electronic voting (definitions can be found for example in [BM03, Cet07, Hir01, Rie98, Smi05]). However, very different ideas and opinions about these requirements exist in the e-voting community, and the definitions are often vague and imprecise [Pie08]. This applies in particular to privacy and verifiability as these are the most complex security requirements. We cite two examples:

1. Universal verifiability is usually seen as the chance for any observer to check that the tally has been correctly computed from the votes that were cast. Some authors postulate that universal verifiability comprises checking that the tallied votes were cast by legitimate voters only [CMFP+06, JdV06, Smi05], while others do not require this [DKR09, Hir01, MN06].

2. Privacy in electronic voting is usually understood as the unlinkability of voter and vote. But what exactly does this mean? That it must not be possible to establish a link between the voter's name and his plaintext vote—or even his encrypted vote? And what if an attacker can reveal the link, but cannot prove it to third parties?

This shows that privacy and verifiability comprise many different levels at which they can be met. Consequently, voting schemes that claim to meet these security requirements may in fact meet different *levels* of privacy and verifiability. As long as these levels are not considered, the security of different voting protocols cannot be assessed and compared in a meaningful way.

While the security requirements capture the properties which the voting scheme should exhibit, the adversary model considers attackers seeking to compromise these properties [BBG07]. In light of security engineering, the desired properties should be separated from the assumed adversary capabilities. However, assumptions regarding adversary capabilities are inherent for example in the security requirements of receipt-freeness and coercion-resistance. Thus, the security requirements and the adversary models are not clearly separated at present, which complicates the analysis of voting schemes.

The goal of Part I is to establish a taxonomy for privacy and verifiability in electronic voting. Besides the fact that these requirements and their correlations are not well understood, the motivation for such a taxonomy is twofold: on the one hand, it may not be necessary for each election, or even possible in general, to achieve the maximum level for both requirements at the same time. On the other hand, in view of practicability, it may not be appropriate for every type of election to assume

an all-powerful adversary who is able to control the communication channels, inject illegal votes, and corrupt voters as well as election authorities, i.e. a more fine-tuned adversary model for specific use cases would be appropriate.

Part II: Long-Term Verifiability: Legal Issues and Technical Implications

The lawfulness of any legally binding election must be verifiable within a specific period of time after the election has been carried out. To this end, specific documents such as the ballots or the voters' register must be retained. These records allow for later review in case the election is challenged. Usually, the election documents are retained for the legislative period of the elected body. In Germany, this period ranges from two years for associations [Ges04] to six years for elections for the governing boards of social security institutions (see § 58 (2) of the German Social Security Code IV). However, this period may be extended if scrutiny procedures are pending. Thus, it is realistic to assume that election data must be retained for up to ten years.

Retention obligations apply not only to conventional paper-based elections, but also to electronic voting. But contrary to the case of paper-based elections, general legal regulations on keeping electronic election records have not been issued so far. Although plenty of research has been conducted into long-term preservation in general, long-term verifiability in electronic voting has not been studied thoroughly before, and there are no according specifications or guidelines. In particular, the question which records should be retained is yet unanswered. A naive approach would be to simply retain any data occurring during the election. This falls short for several reasons:

1. The data generated by the voting protocol may be insufficient or inappropriate to meet applicable legal requirements.

2. The principle of data minimization must be considered: personal data must only be collected for specified, explicit and legitimate purposes.

3. Voter privacy may be compromised if specific records are combined which, though, may not be a threat to privacy individually.

A one-to-one mapping from documenting a paper-based election at the polling station to keeping records of an electronic election is not possible due to their differing implementations. Thus, other ways of determining the according records in an electronic election must be found. Once these records have been identified, established methods for secure long-term retention can be applied.

The goal of Part II is to derive specifications regarding secure retention of electronic election data from existing electoral laws on paper-based elections. This comprises

- identifying the election records which should be retained, and

- making recommendations how to achieve secure and conclusive retention of the records.

In this part of the thesis we do not consider electronic voting machines since these are used in polling stations and, thus, are more close to classical paper-based voting. We rather focus on remote electronic voting as the underlying problem is more challenging and, therefore, more interesting in this case.

1.2. Research questions and methodology

Part I: A Taxonomy for Privacy and Verifiability in Electronic Voting

The first part of this thesis aims at answering the following research question:

> Which levels of privacy and verifiability are conceivable in electronic voting, and how are both properties related?

To answer this question, we approach the issue from two sides:

- we review existing literature (for example [BM03, Cet07, DKR09, Hir01, JCJ05, JdV06, KT09, Rie98, Smi05]) with regard to definitions of privacy and verifiability, and
- we consider existing works that have evaluated or compared voting protocols [Cet07, LGT+03, SP06]; in particular, we focus on different ratings of the same protocol, since this indicates differing perceptions of privacy or verifiability, respectively.

Both approaches are addressed in Chapter 3.

Part II: Long-Term Verifiability: Legal Issues and Technical Implications

The second part of this thesis aims at answering the following research question:

> Which records of a remote electronic election should be retained, and which protective measures should be applied?

The approach used to answer this question is referred to as KORA ("Konkretisierung rechtlicher Anforderungen", Implementation of Legal Requirements, see [HPR92]). KORA is an approved method to bridge the gap between law and technology by translating abstract legal norms into concrete technical measures, and can be used whenever a certain technology has to be (re)designed such that it complies with law. In a four-stage process, legal requirements are substantiated into technical implementation proposals:

1. **Legal requirements.** Starting from constitutional law and its specifications in simple statute law, legal requirements are identified.
2. **Legal criteria.** Next, legal criteria for the evaluation and the design of information technology systems are derived from the legal requirements.

3. **Implementation requirements.** Technical implementation requirements are determined, referring to the legal criteria established at stage 2.

4. **Implementation proposals.** Finally, technical implementation proposals are made, taking into account the implementation requirements which have been identified at stage 3.

KORA is explained more thoroughly in Chapter 7.

1.3. Contribution

Part I: A Taxonomy for Privacy and Verifiability in Electronic Voting

The first part of this thesis provides a taxonomy on privacy and verifiability in electronic voting. This taxonomy comprises three components:

1. a conceptual model considering both privacy and verifiability,

2. a compilation of the different levels which are conceivable for privacy and verifiability, and

3. a comprehensive set of different adversary capabilities.

The first component provides a deeper understanding of privacy and verifiability and their correlation in electronic voting. The second component demonstrates the scope of privacy and verifiability in voting, and allows to select appropriate levels of the requirements for different types of elections. The third component allows to determine reasonable adversary models for individual election scenarios. For example, parliamentary elections could require voter privacy to hold forever [Wil02], while it is not necessary for elections in associations to require privacy in such strictness. Similarly, for parliamentary elections a more powerful adversary should be assumed than for elections in associations. The taxonomy can also be used for analyzing the security of voting schemes, i.e. the level of privacy and verifiability provided depending on the adversary capabilities assumed.

Part II: Long-Term Verifiability: Legal Issues and Technical Implications

The second part of this thesis points out the importance of appropriate record keeping for secure electronic voting. The main contributions are the following:

– we identify the election records that should be retained in order to document the proper conduct of the online election, and

– we give concrete recommendations on how to implement secure and conclusive retention of electronic election data.

Secure and conclusive retention of election data is a precondition for introducing remote electronic voting as an additional voting channel in Federal Elections for the German Bundestag. Thus, our work contributes to establishing legally binding online elections on a parliamentary level in Germany. It may support legislative organs when issuing a legal framework on remote electronic voting. Moreover, it is valuable for developing legally compliant voting systems as the need for record keeping has to be considered already when designing and implementing a remote electronic voting protocol.

1.4. Outline and instructions for reading

This thesis is organized as follows. In Chapter 2 we introduce the security requirements for electronic voting and provide an overview of the cryptographic primitives used to support privacy and verifiability in electronic voting schemes. The remainder of this thesis is divided in two parts:

Part I: A Taxonomy for Privacy and Verifiability in Electronic Voting

In Chapter 3 we review existing literature on definitions of privacy and verifiability and consider related work. In Chapter 4 we compile the conceivable levels of privacy and verifiability in voting and investigate the relation between both properties. To this end, we introduce a conceptual model capturing both privacy and verifiability. Chapter 5 provides a comprehensive adversary model for electronic voting by considering different adversary capabilities. In Chapter 6 we analyze the security of state-of-the-art voting schemes in light of the taxonomy established in Chapters 4 and 5.

Part II: Long-Term Verifiability: Legal Issues and Technical Implications

Chapter 7 provides an introduction to long-term retention of election data and presents related work. In Chapter 8, retention requirements for online elections are derived from legal retention obligations for paper-based elections. Chapter 9 proposes how to implement secure and conclusive retention of electronic election data by deriving implementation requirements from legal requirements. The results of Chapter 8 and 9 are applied to a state-of-the-art voting protocol in Chapter 10.

Chapter 11 concludes the thesis at hand by providing a summary of both Parts I and II and considering future work.

In this thesis, the expressions “remote electronic voting” and “online voting” are used synonymously, referring to voting in uncontrolled environments using the Internet. References listed in the bibliography are referred to by alphanumeric labels containing the authors’ initials and the year of publication (for example [KOV07]), while publications of the author of this thesis (see page vii) are referred to by numbers (for example [1]). Legal texts are frequently referred to especially in the second

part of this thesis. As usual in such cases, laws and regulations are not listed in the bibliography, but rather referred to by their official German abbreviations (see page 129). We refer to the respective version as amended, which can be found in the Federal Law Gazette (Bundesgesetzblatt[1]). We provide references to English translations of the respective texts if available. Note, however, that the English version may be outdated, and that only the version published in the Federal Law Gazette is official.

[1] Available at `http://www.bgbl.de/`.

2. Preliminaries

This chapter lays the foundations for the following considerations by introducing the security requirements for electronic voting and explaining the cryptographic primitives which are usually employed to meet these requirements. Implementation requirements such as scalability or usability are not considered here (see for example [LGT+03, SP06]).

Chapter overview

This chapter briefly introduces the security requirements for electronic voting in Section 2.1 and provides an overview over the common cryptographic primitives used in electronic voting schemes in Section 2.2.

2.1. Security requirements

An approved set of security requirements for electronic voting schemes has been established to date. In the following we give common definitions of these requirements (see for example [Rie98, Hir01, BM03, Smi05, Cet07, Pas07]) in order to introduce them to the reader prior to considering specific requirements more thoroughly in the following chapters.

2.1.1. Accuracy

Accuracy (also referred to as "correctness" [Pie08] or "integrity" [Rya08]) is the primary goal of any voting system. It comprises the following subrequirements [LGT+03, Jon09]:

soundness: all counted votes are valid

completeness: all valid votes are counted

inalterability: any cast vote cannot be altered

According to [LK02, Pas07], inalterability is already included in the notion of completeness which then requires that all valid votes are counted *correctly*. The term "valid" means that the vote is not spoilt; however, some authors also associate the fact that the vote was legitimately cast with the notion of accuracy [Cet07, Rya08].

2.1.2. Democracy

Democracy is also referred to as "authenticity" [Pie08] and comprises two subrequirements according to [Rie98, BM03, JdV06]:

eligibility: only eligible voters can vote

uniqueness: each eligible voter casts at most one vote that counts

The first subrequirement is referred to as "eligibility" in [Hir01, LK02, LGT+03, Jon09], whereas [SP06, DKR09] use this expression for both subrequirements (and thus synonymously with our definition of democracy). The second subrequirement is referred to as unreusability in [LK02, LGT+03] and named "no double-voting" in [Hir01].

2.1.3. Fairness

Fairness requires that all votes remain secret until the voting phase ends as voters must not be influenced by intermediate results [Rie98, LGT+03, SP06, Cet07, DKR09].

2.1.4. Privacy

Privacy is also known as "secrecy" [Hir01] and requires that no one can tell how a voter voted. This requirement is rarely also referred to as "anonymity" [Rie98], whereas Hirt [Hir01] understands anonymity as the infeasibility of determining whether or not a particular voter has participated in the election. We consider the various existing definitions of privacy more thoroughly in Section 3.1.

2.1.5. Receipt-freeness

The notion of receipt-freeness was introduced in [BT94]. It requires that no voter can prove his vote to an adversary by showing a receipt, even if he wants to do so. This requirement shows that privacy is not a mere option for the voter but rather must be *enforced*. We consider receipt-freeness more thoroughly in Section 3.1.

2.1.6. Coercion-resistance

Coercion-resistance (also referred to as "uncoercibility" [Rie98] or "incoercibility" [Hir01]) requires that no voter can be coerced to vote in a specific way. It has been introduced by Juels, Catalano and Jakobsson [JCJ05] as an amplification of receipt-freeness. According to [JCJ05], a voting scheme is coercion-resistant if it is receipt-free and not susceptible to the following attacks:

randomization: the voter is forced to cast a vote for a random candidate

forced-abstention: the voter is forced to abstain from voting

simulation: the voter is forced to disclose his private keying material

We consider coercion-resistance more thoroughly in Section 3.1.

2.1.7. Verifiability

Verifiability is required for electronic voting schemes in order to assure the participants that the election has been performed correctly. This requirement comes in two different forms:

individual verifiability: each voter can verify that his (valid) vote was counted

universal verifiability: anyone can verify that all valid votes have been counted

Universal verifiability is also referred to as "auditability" [Sch00]. We consider verifiability and related concepts such as cast-as-intended or counted-as-cast [KSW05] more thoroughly in Section 3.2.

2.2. Cryptographic primitives

In the following we briefly describe the cryptographic primitives which are usually employed to meet the security requirements for electronic voting.

2.2.1. ElGamal cryptosystem

The ElGamal encryption scheme is a probabilistic public-key cryptosystem named after its inventor Taher ElGamal [Gam84]. Its security relies on the computational Diffie-Hellman assumption, which implies the hardness of computing discrete logarithms [DH76].

Let G be a multiplicative cyclic group of order q with generator g. The secret key x is randomly chosen from $\mathbb{Z}_q$, and the corresponding public key is computed as $h = g^x$. To encrypt a message $m \in G$, pick a random value $r \in \mathbb{Z}_q$ and compute the ciphertext $\mathcal{E}_r(m) = (c_1, c_2) = (g^r, h^r m) \in G \times G$. To decrypt a ciphertext (c_1, c_2), compute $c_2/c_1^x = h^r m/g^{rx} = m$.

ElGamal encryption is semantically secure, provided that the decisional Diffie-Hellman problem [Bon98] is hard in G. Therefore, G usually is a multiplicative subgroup of $\mathbb{Z}_p^*$ of prime order q.

Application to electronic voting. ElGamal encryption is frequently used in electronic voting schemes due to its homomorphic property (see also Section 2.2.5) and because it allows reencryption, i.e. changing the ciphertext of a message without changing the corresponding plaintext (see also Section 2.2.6): suppose we have a ciphertext $\mathcal{E}_r(m) = (c_1, c_2) = (g^r, h^r m)$. This ciphertext is reencrypted by choosing a random s and computing $(c_1 g^s, c_2 h^s) = (g^{r+s}, h^{r+s} m) = \mathcal{E}_{r+s}(m)$. As c_2/c_1^x still yields m, reencryption does not affect the decryption process—in fact, reencryption

equals multiplication by $\mathcal{E}_s(1)$, i.e. the ElGamal encryption of 1 [Adi06]. Furthermore, reencryption does not require knowledge of the message m or the secret key x.

2.2.2. Secret sharing

Secret sharing techniques are used to distribute the knowledge of a secret s between n trustees such that a subset of k trustees must cooperate in order to reconstruct s, whereas any number of trustees below this threshold cannot learn anything about s.

The method described in the following goes back to Shamir [Sha79]: to share a secret $s \in \mathbb{F}_p$, a random polynomial $f \in \mathbb{F}_p[X]$ of degree k is picked such that $f(0) = s$. Shares $s_i = f(i)$, $i = 1, \ldots, n$ are computed and distributed among the trustees. s is recovered from k shares with indices $\mathcal{S}$ by computing $s = \sum_{i \in \mathcal{S}} s_i \lambda_{i,\mathcal{S}}$, where $\lambda_{i,\mathcal{S}} = \prod_{j \in \mathcal{S} \setminus \{j\}} \frac{j}{j-i}$ are the Lagrange coefficients.

Application to electronic voting. Secret sharing is mostly used in electronic voting to distribute the decryption key of an election authority, for example in homomorphic encryption schemes (see Section 2.2.5). Another application is a reencryption mixnet: the decryption key is shared in order to achieve robustness [Adi06] (see Section 2.2.6).

2.2.3. Zero-knowledge proofs

A zero-knowledge proof (ZKP) is a cryptographic protocol which allows one party (the prover $\mathcal{P}$) to convince another party (the verifier $\mathcal{V}$) of a certain statement in a way such that $\mathcal{V}$ learns nothing beyond the truth of the statement. A ZKP usually consists of three rounds:

1. $\mathcal{P}$ commits to a certain information
2. $\mathcal{V}$ submits a random challenge
3. $\mathcal{P}$ responds and $\mathcal{V}$ verifies the truth of the claim made by $\mathcal{P}$.

Thus, ZKPs require interaction between $\mathcal{P}$ and $\mathcal{V}$. However, interactive ZKPs can be turned into non-interactive ZKPs by applying the Fiat-Shamir heuristic [FS86], which replaces the random challenge by the output of a secure hash function.

In the following we briefly explain the ZKPs frequently used in electronic voting schemes.

ZKP of knowledge of discrete logarithm

$\mathcal{P}$ wants to convince $\mathcal{V}$ of the fact that he knows the discrete logarithm of a given value $h = g^x$ in a prime-order group G without revealing the value of x (g, h, G are public). This can be accomplished using the Schnorr protocol [Sch91].

ZKP of equality of discrete logarithms

$\mathcal{P}$ wants to convince $\mathcal{V}$ of the fact that two given values $h = g^x$ and $l = k^x$ in a group G have the same discrete logarithm x without revealing the value of x (g, h, k, l, G are public). This can be accomplished using the Chaum-Pedersen protocol [CP92].

ORing ZKPs, I: designated-verifier ZKPs

A ZKP for the statement "A or B" can be established whenever we have a random-challenge ZKP for each A and B separately [Smi05]. This can be taken advantage of in the following situation: suppose $\mathcal{P}$ wants to issue a designated-verifier proof [JSI96], i.e. $\mathcal{P}$ wants to prove a statement $\mathcal{S}$ to $\mathcal{V}$ without giving $\mathcal{V}$ the chance to reuse this proof to convince $\mathcal{W}$ of $\mathcal{S}$. $\mathcal{P}$ can accomplish this by proving the statement "$\mathcal{S}$ is true or I am $\mathcal{V}$" to $\mathcal{V}$. The proof that "I am $\mathcal{V}$" can be a ZKP of knowledge of $\mathcal{V}$'s secret key, for example. $\mathcal{V}$ will be convinced by this proof issued by $\mathcal{P}$. Conversely, $\mathcal{W}$ will not be convinced upon receiving this proof from $\mathcal{V}$.[1]

ORing ZKPs, II: ZKP of exponential ElGamal encryption of ± 1

Suppose we have an ElGamal encryption $(c_1, c_2) = (g^r, h^r v^{\pm 1})$ of the message $v^{\pm 1}$ in a prime-order group G (g, h, v, G are public). $\mathcal{P}$ wants to prove to $\mathcal{V}$ that (c_1, c_2) indeed is an ElGamal encryption of either v or v^{-1} without revealing which of both is the case and, also, without revealing the value r. This amounts to proving the equality of the base-g discrete logarithm of c_1 and either the base-h discrete logarithm of $c_2 v$ or $c_2 v^{-1}$. An according protocol can be found in [CGS97].

Application to electronic voting. Provable exponential ElGamal encryption of ± 1 is needed for proving well-formedness of ballots in electronic voting schemes with homomorphic encryption (see Section 2.2.5).

The non-transferability of designated-verifier ZKPs is important with regard to receipt-freeness in electronic voting: the voter must not be able to reuse a proof obtained from an election authority to prove his vote to a vote-buyer or a coercer.

Equality of discrete logarithms is used to prove correct decryption in threshold ElGamal encryption: the secret key x is divided into n shares $x_1, \ldots, x_n$ which are distributed among n trustees. Each trustee commits to his share by publishing his verification key $h_i = g^{x_i}$. To decrypt a ciphertext $(c_1, c_2) = (g^r, h^r m)$, the trustees broadcast their decryption shares $c_{1,i} = c_1^{x_i}$. The trustees with indices $\mathcal{X}$ then implicitly[2] reconstruct the secret x according to Section 2.2.2: $\prod_{i \in \mathcal{X}} c_{1,i}^{\lambda_{i,\mathcal{X}}} = \prod_{i \in \mathcal{X}} c_1^{x_i \lambda_{i,\mathcal{X}}} = c_1^{\sum_{i \in \mathcal{X}} x_i \lambda_{i,\mathcal{X}}} = c_1^x$. Dividing c_2 by this term then yields the plaintext m. A ZKP of correct decryption is then given by proving equality of two discrete

[1] Note that the prover must be certain that his designated-verifier ZKP is transmitted to the designated verifier over an untappable channel. Otherwise, an eavesdropper could be certain who authored the proof and thus be convinced by it [Smi05].

[2] Note that for decrypting the ciphertext it is not necessary to reconstruct the secret s.

logarithms (decryption share and verification key): $\log_{c_1} c_{1,i} = \log_g h_i$, which is equivalent to $\log_{c_1} c_1^{x_i} = \log_g g^{x_i}$

ZKPs of equality of discrete logarithms can also be used for **plaintext equality tests**: suppose we have two ElGamal encryptions $(c_1, d_1) = (g^{r_1}, h^{r_1} m_1)$ and $(c_2, d_2) = (g^{r_2}, h^{r_2} m_2)$ and want to prove that they encrypt the same plaintext, i.e. that $m_1 = m_2$. This equals proving that $(c_1 c_2^{-1}, d_1 d_2^{-1})$ is an ElGamal encryption of 1. Since $d_1 d_2^{-1} = h^{r_1 - r_2} m_1 m_2^{-1}$ and $c_1 c_2^{-1} = g^{r_1 - r_2}$, this amounts to proving the equality of discrete logarithms.

2.2.4. Blind signatures

A blind signature provides the possibility to have a message signed without revealing its content. Blind signatures have been proposed by Chaum [Cha82], who used the following example to illustrate his idea: a paper document is covered with a sheet of carbon paper and put into an envelope which is sealed. Upon signing the envelope, the signature is transferred onto the document through the carbon paper. Still, the signer is not able to inspect the signed document, nor will he recognize it afterward. Blind signature schemes can be implemented using several common public-key signature schemes such as RSA and DSA (see [CPS94]).

Application to electronic voting. Blind signatures can be used to authorize voters while maintaining privacy: a designated election authority receives blinded votes from voters who authenticate themselves, for example by providing their electronic signature. Upon verifying the eligibility of the voters, the authority signs the blinded vote and sends it back to the voter. The voter unblinds the received message and obtains a signed vote. Thus, the voter can cast an authorized vote without revealing its content to the authority who signed it (see for example [OMA+99]).

2.2.5. Homomorphic encryption

An encryption function $\mathcal{E}$ is said to be homomorphic if $\mathcal{E}(m_1) \otimes \mathcal{E}(m_2) = \mathcal{E}(m_1 \oplus m_2)$ for some appropriate algebraic operations $\otimes, \oplus$; i.e. applying the operation $\otimes$ to two ciphertexts equals the encryption of the plaintext obtained by applying the operation $\oplus$ to the plaintexts m_1, m_2. The RSA [RSA83] and ElGamal [Gam84] encryption systems, for example, are homomorphic with both $\otimes, \oplus$ denoting multiplications. ElGamal encryption can also be made homomorphic such that $\oplus$ denotes an addition operation by putting the plaintext in the exponent: suppose we modify ElGamal such that m is encrypted as $\mathcal{E}_r(m) = (g^r, h^r g^m)$. This gives us $\mathcal{E}_{r_1}(m_1) = (g^{r_1}, h^{r_1} g^{m_1}), \mathcal{E}r_2(m_2) = (g^{r_2}, h^{r_2} g^{m_2})$. The product of these two encryptions is $(g^{r_1+r_2}, h^{r_1+r_2} g^{m_1+m_2}) = \mathcal{E}_{r_1+r_2}(m_1 + m_2)$ which equals the encryption of the sum $m_1 + m_2$ using the random value $r_1 + r_2$.

Application to electronic voting. In many elections, tallying the votes simply amounts to adding them. Thus, homomorphic encryption schemes can be used,

and they bring about a significant advantage: tallying can be accomplished by simply decrypting the product of all encryptions using exponential ElGamal as noted above, i.e. without ever decrypting individual ballots and revealing individual voting decisions. Suppose we have n votes $v_1, \ldots, v_n$, then multiplying their encryptions $(g^{r_1}, h^{r_1} g^{v_1}), \ldots, (g^{r_n}, h^{r_n} g^{v_n})$ and subsequent decryption gives us $g^{\sum_i^n v_i}$. To obtain the election result $\sum_i^n v_i$, we then have to solve a discrete logarithm problem, which is feasible using exhaustive search as long as $\sum_i^n v_i$ is sufficiently small.

To make homomorphic voting schemes work, we need to be sure that each voter provided a well-formed encryption of either $+1$ or -1. To accomplish this, ZKPs of (exponential) ElGamal encryption of ± 1 can be used (see Section 2.2.3).

The drawback of homomorphic encryption schemes is that they can only be used if the votes are combined additively (see [Smi05, 7.2] for counterexamples).

2.2.6. Mixnets

A **mix** $\mathcal{M}$ receives a bunch of encrypted messages and processes them in a way that hides the link between input and output without changing the messages. To achieve robustness, a cascade of mixes $\mathcal{M}_1, \ldots, \mathcal{M}_n$ is normally used; this construction is referred to as a **mixnet**. The communication among the mixes can be accomplished through bulletin boards (see Section 2.2.7).

There exist two basic types of mixnets: decryption mixnets introduced by Chaum [Cha81] and reencryption mixnets introduced by Park et al. [PIK93].

Each mix $\mathcal{M}_1, \ldots, \mathcal{M}_n$ in a **decryption mixnet** has an asymmetric encryption key pair. The input messages have all been encrypted using the public keys of $\mathcal{M}_n, \ldots, \mathcal{M}_1$ (in this order). Mix $\mathcal{M}_i$ then removes one layer of encryption by using his secret key, scrambles the messages (which are still encrypted with the public keys of $\mathcal{M}_{i+1}, \ldots, \mathcal{M}_n$), and passes them on to mix $\mathcal{M}_{i+1}$. The last mix $\mathcal{M}_n$ performs the final decryption, permutes and outputs the plaintext messages. Note that if one single mix denies its service, the messages cannot be decrypted. In particular, the last mix may abort if it dislikes the decrypted messages. Although this can be prevented by distributing the secret key of $\mathcal{M}_n$ among several parties (see also Section 2.2.2), decryption mixnets are scarcely used in e-voting systems in practice.

A **reencryption mixnet** $\mathcal{M}_1, \ldots, \mathcal{M}_n$ receives a bunch of messages which have been encrypted using a cryptosystem with reencryption property (for example ElGamal [Gam84], see also Section 2.2.1). Mix $\mathcal{M}_i$ scrambles the encrypted messages and reencrypts them, i.e. changes their ciphertexts without changing the corresponding plaintexts. The reencrypted messages are then passed on to mix $\mathcal{M}_{i+1}$ which repeats the procedure using random reencryption values. The output of the last mix $\mathcal{M}_n$ then has to be decrypted in order to obtain the plaintext messages. Secret sharing techniques are usually applied to the decryption key in order to achieve robustness [Adi06] (see Section 2.2.2). Note that reencryption mixnets are more robust than decryption mixnets as a single mix denying service does not disrupt the mixing process.

A mixnet is usually required to prove (or, at least, to provide strong evidence of) the fact that it has processed the input messages correctly, i.e. that

1. each mix has decrypted or reencrypted the messages correctly, and
2. the output of each mix is indeed a permutation of its input.

Since the 1990s, a plenty of different techniques has been proposed for making mixnets verifiable (for example [SK95, FS01, Nef01, JJR02]). The reader is referred to [Adi06] for a detailed review of verifiable mixnets.

Application to electronic voting. Electronic voting schemes use mixnets to create an anonymous channel for vote casting: voter privacy is established by hiding the link between the received votes (i.e. the input of the voting system) and the tallied votes (i.e. the output of the voting system). Thus, the voting decision of a specific voter cannot be traced back by recording the time the vote was cast and checking the bulletin board for the corresponding vote.

2.2.7. Bulletin boards

A bulletin board, as introduced by Benaloh et al. [Ben87, CF85], is a public broadcast channel. Data is published by authorized parties only and, once published, cannot be deleted or modified by anyone.

Bulletin boards are usually operated in a distributed setting to achieve robustness and prevent denial of service. The reader is referred to [Rei95, LLR06] for possible implementations of a bulletin board.

Application to electronic voting. Bulletin boards are crucial for individual as well as universal verifiability: the information published allows voters to check upon their own votes and provides the public with the data needed to verify the correct processing of the ballots. The bulletin board may contain, for example, the voters' register, encrypted votes next to voter names or identification numbers, and outputs of the single stages of a mixnet including proofs of correctness.

Part I.

A Taxonomy for Privacy and Verifiability in Electronic Voting

3. Survey of existing literature

In this chapter we review literature on electronic voting in terms of existing definitions of privacy and verifiability. We will see that, while the basic concept of these security requirements is understood consistently (see common definitions in Section 2.1), their content and scope has been interpreted in many different ways by the e-voting community. This will lead us to considering different levels of privacy and verifiability in Chapter 4.

Chapter overview

Definitions of privacy, receipt-freeness and coercion-resistance are considered in Section 3.1, while definitions of individual and universal verifiability and related concepts are considered in Section 3.2. Section 3.3 focuses on related work, i.e. other frameworks comparing different voting protocols and measuring privacy and/or verifiability. A summary of the findings is given in Section 3.4.

3.1. Definitions of privacy, receipt-freeness and coercion-resistance

In the literature reviewed there is a general consent that a voting scheme offers privacy if it is not possible to link a vote with the voter who cast it. More precisely, privacy means that nobody should learn more about any voter's decision than what is leaked by the tally [CMFP$^+$06, MN06]: if all voters vote identically, then it is clear how each voter voted. The notions of (voter) privacy and (ballot) secrecy are often used synonymously [Hir01, CRS05, MN06]; Riera refers to anonymity instead [Rie98]. Hirt distinguishes between secrecy and anonymity: while secrecy is defined as the infeasibility to assign votes to voters, anonymity refers to the impossibility to tell whether a certain voter participated in the election or not [Hir01]. The importance of long-term voter privacy is referred to in [CMFP$^+$06, MN06, Cet07]: [CMFP$^+$06] uses the expression "unconditional privacy", [MN06] uses "everlasting privacy".

However, it is not sufficient for a voting system to *offer* privacy—as noted by Benaloh and Tuinstra [BT94], privacy must be *enforced*. Receipt-freeness is commonly defined as the infeasibility for the voter to prove his vote even if he wants to do so. Smith illustratively names this property "no sale" [Smi05]. Jonker and Pieters [JP06] distinguish weak and strong receipt-freeness as follows: weak receipt-freeness states that the voter cannot prove to the adversary that he sent a specific message representing the vote. Strong receipt-freeness means that, for all possible votes, the adversary cannot be certain that the voter did *not* cast this vote.

Moran and Naor provide a very strong notion of receipt-freeness [MN06]: the adversary can coerce the voter at any time during the execution of the voting protocol and is not limited to passive queries. Similarly, for their definition of receipt-freeness, Chevallier-Mames et al. allow interactions with the adversary before and after the vote is cast [CMFP$^+$06]. They also assume that the adversary can tap the channel between the voter and the voting authority.

In contrast to this, Hirt and Sako state that receipt-freeness cannot be achieved without some physical assumptions, the weakest assumption being one-way untappable channels from the authorities to the voters [HS00]. In literature, the following types of communication channels have been assumed as a precondition for receipt-freeness [Jon09]:

- anonymous channels [JCJ05]
- private channels [CGS97]
- untappable channels (realized by tamper-resistant hardware devices [LK02], voting booths [BT94], or mail service [JCJ05])
- anonymous untappable channels [Oka97]

Similarly, Juels et al. state that anonymous channels are a minimal requirement for any coercion-resistant scheme, since if the attacker can identify who has participated, he can mount a forced-abstention attack [JCJ05]. Resistance against this kind of attack is one of the specifics of a coercion-resistant scheme according to Juels et al.: they consider coercion-resistance to be an extension of receipt-freeness by resistance against randomization, forced-abstention and simulation attacks [JCJ05]. In general, coercion-resistance (also referred to as uncoercibility or incoercibility) is understood as the infeasibility for an adversary to coerce a voter into casting his vote in a particular way. Riera defines a voting scheme to be coercion-resistant if "no voter can prove that he voted in a particular way" [Rie98] and hence takes coercion-resistance for what is generally understood as receipt-freeness.

According to Hirt, "the concept of incoercibility is weaker than receipt-freeness" [Hir01]. This is also claimed by Burmester and Magkos [BM03]: deniable encryption allows a voter to lie about his encrypted vote, but he can refrain from using this mechanism if he wants to prove his vote. Thus, Burmester and Magkos assert that it is possible to have a voting scheme which is coercion-resistant and yet not receipt-free. However, the relation between receipt-freeness and coercion-resistance is usually understood contrarily: coercion-resistance is stronger than receipt-freeness [JCJ05, Smi05, Cet07, DKR09, KT09]. According to [DKR09] and [KT09], coercion-resistance even implies receipt-freeness, which is formally proven by the authors.

Delaune et al. [DKR09] provide formal definitions for privacy-type properties of voting schemes using the applied pi calculus. They model privacy as observational equivalence of the process where voter A votes a and voter B votes b and the process where voters A and B swap their votes (i.e. A votes b and B votes a). The authors also prove the intuitive relation between the privacy-type properties, namely

that coercion-resistance implies receipt-freeness and receipt-freeness implies privacy. However, their definition of coercion-resistance does not consider randomization and forced-abstention attacks as introduced in [JCJ05]. Also, note that under a strict interpretation, receipt-freeness does not imply privacy: consider an election where each voter announces the candidate he is voting for. Without an official record, the voter cannot prove *afterward* how he voted, which satisfies receipt-freeness. Yet there is no privacy with respect to observers present *during* vote casting. In literature, definitions of receipt-freeness are usually less strict and do include vote privacy.

Juels et al. provide formal definitions of coercion-resistance and universal verifiability in a computational model [JCJ05]. Their definitions hinge on several experiments involving an adversary in interaction with components of the voting system: the adversary tries to guess whether the coerced voter complied with his demands. His success is measured by comparison with another adversary in an ideal voting system who is unable to determine whether coercion is successful or not. The formal definition of coercion-resistance is tailored to the specific structure of the protocol proposed by the authors.

Küsters and Truderung propose a definition of coercion resistance in a symbolic setting, following an epistemic approach [KT09]. Their definition is independent of a specific adversary model. It requires that coerced voters can apply counter strategies such that the voter always achieves his own goal and the coercer does not know whether the coerced voter followed his instructions.

Chevallier-Mames et al. provide formal definitions of universal verifiability, unconditional privacy and receipt-freeness [CMFP+06]. The authors show that, in their setting, one cannot achieve universal verifiability of the tally and unconditional anonymity of the votes unless all the registered voters participate in the election. Similarly, it is not possible to have both universal verifiability and receipt-freeness unless the existence of secure channels is assumed.

3.2. Definitions of verifiability

Universal verifiability gives any observer the possibility to check that the tally has been correctly computed from the ballots cast. It is closely related to accuracy, which requires that no vote can be altered, duplicated or eliminated [Rie98, BM03]. Cetinkaya states that verifiability is "the provability that the election is accurate" [Cet07]. However, he does not regard universal verifiability to be an actual security requirement as accuracy should be provable anyway: "if a protocol claims that it satisfies accuracy, it should be able to prove its claim" [Cet07]. Formal definitions of universal verifiability have been provided in [JCJ05, CMFP+06] (see Section 3.1).

There is no consensus on the question whether universal verifiability comprises verifying eligibility, i.e. the fact that only eligible voters cast a vote (this aspect of verifiability is also referred to as "eligibility verifiability" by Smyth et al. [SRKK09], but the authors subsume uniqueness under eligibility). An affirmative answer is given in [AN06]. [CMFP+06, Smi05, Cet07] even go one step further and claim that univer-

sal verifiability includes verifying eligibility and uniqueness (recall that uniqueness requires that each eligible voter casts at most one vote that counts, cf. Section 2.1). According to [Ben06], end-to-end verifiability (considered below) amounts to verifying the "accurate count of legitimate votes". Similarly, Schoenmakers claims that anyone should be able to verify "that the published election result corresponds to the ballots cast by legitimate voters" [Sch00]. However, in both cases it is not clear whether this restricts to eligibility, or whether it includes uniqueness. Eligibility is not explicitly subject to verifiability according to [Hir01, MN06, Pie06, DKR09].

Individual verifiability is commonly referred to as the possibility for any voter to verify that his vote was included in the tally [Hir01]. Some authors consider individual verifiability to comprise the correct counting of the individual votes [Rie98, CRS05, Smi05]. [Rie98, BM03, LGT+03] also take into account the chance for open objections made by the voter: in case his vote has been miscounted, he should have the possibility to file a complaint.

Concerning the relation between universal and individual verifiability, [LGT+03] and [BM03] state that individual verifiability is weaker than universal verifiability. In Section 4.4 we will see that both requirements are closely intertwined; however, universal verifiability does not generally imply individual verifiability.

In the last couple of years, concepts such as cast-as-intended and counted-as-cast have emerged and become common in parallel to the established terms of universal and individual verifiability:

cast-as-intended: each voter can verify that the ballot correctly represents his choice [KSW05, AN06, Riv06].

counted-as-cast: each voter can verify that his ballot has been counted as it was cast, i.e. that it has been processed and tallied correctly [Riv06]. However, it has also been claimed that counted-as-cast should be universally verifiable, i.e. that anyone should be able to verify that the final tally is an accurate count of the ballots cast [KSW05, Ben07].

Some authors also break counted-as-cast down into the following two concepts (see for example [AN06, BMQR07, CCC+08]):

recorded-as-cast: each voter can verify that his ballot has been recorded by the voting system as it was cast by the voter.

counted-as-recorded: anyone can verify that all ballots have been counted as they were recorded by the voting system.

In [AN06], cast-as-intended and recorded-as-cast are combined into the concept of **ballot casting assurance**, which "complements universal verifiability" [AN06]. All of these concepts are closely related to the notion of **end-to-end (E2E) verifiability**, which postulates that each step of the election from casting one's vote to computing the tally should be verifiable, thus providing a chain of custody [AN06, Riv06,

CCC+08]. Chaum et al. state that "E2E systems allow voters to verify that their ballots are processed correctly, giving voters assurance that their votes are cast, collected, and counted as intended" [CCC+08]. According to Benaloh, end-to-end verifiability also includes verifying eligibility [Ben06].

3.3. Related work

We consider related work to comprise

- other frameworks designed to measure or classify privacy and verifiability, and
- other approaches that have been used to evaluate voting protocols in light of the security requirements.

We also consider the adversary models which are assumed in each case.

3.3.1. Other classifications of privacy and verifiability

Lambrinoudakis et al. provide only a rough distinction between different levels of privacy and verifiability by distinguishing computational and information-theoretic privacy, and individual verifiability with(out) open objection [LGT+03]. The same differentiation of privacy is made by Sampigethaya and Poovendran [SP06].

Pieters [Pie06] distinguishes a "classical" and a "constructive" variant of both individual and universal verifiability: constructive individual verifiability allows the voter to verify that his vote has been counted correctly by reconstructing his vote from the information provided about the received votes, while for the classical form the voter cannot reconstruct his vote from this information. Similarly, constructive universal verifiability means that the correct calculation of the election result from the received votes can be publicly verified by retallying the votes independently of the election authorities, while the classical form provides the possibility for verification without publishing the information necessary for performing the tally.

Jonker provides a framework which allows to quantify privacy and, as such, can be used to measure the privacy offered by different voting schemes [Jon09]. A voter's choice group is defined to contain all candidates that a voter might have chosen. Any modification to voter privacy is captured by changes to the size of this voter's choice group. Jonker uses an adversary model following the standard one as suggested by Dolev and Yao [DY83]: cryptography works perfectly, and all communication channels except the untappable ones are under control of the adversary.

3.3.2. Other evaluations of voting protocols

Lambrinoudakis et al. [LGT+03] provide definitions of the security requirements for electronic voting and analyze several voting protocols in light of these requirements. Their definitions of the security requirements are rather imprecise. For example, universal verifiability is defined as the ability for anyone to "verify the election outcome

after the announcement of the tally" [LGT+03]. The term "election outcome" is not specified; it is thus not clear whether universal verifiability is limited to retallying the votes or whether it includes verifying that all votes cast by legitimate voters (and *only* those) have been counted. The authors provide only a rough distinction between different levels of the respective property, such as computational versus information-theoretic privacy and individual verifiability with(out) open objection. The voting protocols are classified into three categories: involving trusted authorities, anonymous voting using tokens, and homomorphic encryption. An adversary model is not provided.

Sampigethaya and Poovendran [SP06] provide a framework for comparing electronic voting schemes. The authors specify different types of requirements: security requirements, counter-attack requirements, and system requirements. The protocols are classified into three types according to the way in which voter anonymity is established: hidden voter, hidden vote, and hidden voter with hidden vote. It is checked whether the protocols considered meet the different types of requirements. Besides distinguishing computational and information-theoretic privacy, the authors do not discern different levels of the security requirements. They do, however, distinguish security requirements from resilience requirements aimed at preventing adversarial attacks, thus reflecting that for example receipt-freeness and coercion-resistance are of a different nature than the other security requirements.

Some of the protocols considered both in [LGT+03] and [SP06] are rated differently in the two works. For example, the protocol proposed by Hirt and Sako [HS00] is rated to be universally verifiable in [SP06], but not in [LGT+03]. The same protocol is said to be coercion-resistant in [LGT+03], but not in [SP06]. While [LGT+03] assigns fairness to [HS00] and [BFP+01], [SP06] assesses the fairness provided by both protocols to be only conditional.

Cetinkaya [Cet07] provides a taxonomy of cryptographic voting protocols by adapting [SP06] with minor changes. Again, some of the protocols are rated differently in [SP06] and [Cet07], respectively. As for the discrepancies between the evaluation in [SP06] and [LGT+03], this is due to the different definitions of the security requirements by the authors, in particular with regard to verifiability. While individual and universal verifiability are seen as either one side of verifiability in [SP06], [Cet07] argues that universal verifiability is redundant to the set of security requirements as it is equivalent to "the provability that the election is accurate" (cf. Section 3.2).

Common Criteria

The Common Criteria for Information Technology Security Evaluation (CC), accompanied by the Common Methodology for Information Technology Security Evaluation (CEM), is an international standard [Inta, Intb] which ensures that IT systems (such as electronic voting systems) can be evaluated by independent licensed laboratories against specific security requirements.[1] CC allows developers to specify the security

[1] See also `http://www.commoncriteriaportal.org/`.

attributes of their products, and provides evaluators with the means to determine if IT products indeed fulfill the security standards claimed [GKM+06]. The current version CC v3.1 consists of three parts: Introduction and general model (Part I), Security functional requirements (Part II), and Security assurance requirements (Part III) [CCp09a, CCp09b, CCp09c]. The accompanying document CEM v3.1 provides evaluators with guidance on applying the CC [CEM09].

The core documents used in the the certification process are Protection Profiles and Security Targets. A Protection Profile specifies security requirements for a family of IT products, referred to as Targets of Evaluation, in a way which is independent of implementation issues (see [VV08] for a Protection Profile for online voting products). More specifically, a Protection Profile defines a security problem, identifies threats, states the assumptions that are made regarding the intended use and the operational environment of the Target of Evaluation, and specifies security objectives as well as security requirements. It also determines the Evaluation Assurance Level indicating the depth of the security evaluation. A Security Target defines the security properties of a specific IT product. It is to be defined by the product vendor or the system developer, and usually complies with one or more Protection Profiles.

The assumed adversary model is inherent in the assumptions made within the Protection Profile regarding the intended use and the operational environment of the Target of Evaluation. For example, the assumption that nobody is watching the voter while he casts his vote (see [VV08, Assumption 139]) implies that a remote adversary is assumed. Furthermore, the attack potential for a given vulnerability, which expresses the strength of the assumed adversary, is determined as a function of elapsed time, expertise and equipment of the adversary, and knowledge of the Target of Evaluation and access to it [CEM09, B.4.2.2]. The resulting attack potential (basic, enhanced-basic, moderate, high) determines the level of the vulnerability analysis (1 to 5). This level correlates with the Evaluation Assurance Level as indicated by Part 3 of the CC [CCp09c, Table 1], which implies that the assumed strength of the adversary affects the Protection Profile and is, in particular, *fixed* for each Protection Profile. The strength of cryptographic algorithms is outside the scope of the CC [CEM09, B.2.1.3].

Overall, the CC is an approved method to define specific security requirements that apply to the given Target of Evaluation, and to evaluate the latter against these requirements. However, as our goal is to classify *existing* security requirements by identifying the levels which are conceivable, in the following we use a different approach which also allows us to define security requirement levels independent of adversary capabilities.

3.4. Summary

We have seen that various definitions have been proposed for privacy, receipt-freeness, coercion-resistance as well as individual and universal verifiability. Obviously, there is no consensus on the exact scope and content of the considered security requirements,

and some of the existing interpretations are even contradictory. Also, the relation between the privacy-related properties is not well understood, as well as the relation between individual and universal verifiability. While the informal definitions tend to be sketchy and imprecise, the formal definitions are precise, but quite complex. Moreover, the formal definitions are usually tailored for specific scenarios given in specific voting protocols or assuming particular adversary models. Therefore, these definitions are in general not suitable for comparing different voting protocols.

In light of security engineering, the desired properties (captured by the security requirements) should be separated from the assumed adversary model (defined by the adversary capabilities). However, assumptions regarding adversary capabilities are inherent for example in the notion of receipt-freeness and coercion-resistance. Thus, the security requirements and the adversary models are not clearly separated at present, which complicates the analysis of voting schemes.

The remainder of Part I deals with a taxonomy for privacy and verifiability in electronic voting. In Chapter 4 we define the conceivable levels of these security requirements and provide a conceptual model which captures both privacy and verifiability. Different adversary capabilities are compiled in Chapter 5 in order to allow for a fine-tuned adversary model. In Chapter 6 the taxonomy is applied to several state-of-the-art voting schemes.

4. Classifying privacy and verifiability

The variety of definitions that have been proposed for privacy and verifiability in electronic voting (see Section 3.1 and 3.2, respectively) indicates that these security requirements are still not well understood. Therefore, this chapter sets out to compile the conceivable levels of privacy and verifiability and to investigate the relation between the two. To this end, we introduce a conceptual model capturing both privacy and verifiability.

Chapter overview

After some remarks on terminology and notation in Section 4.1, an (un)linkability model capturing both privacy and verifiability in voting is introduced in Section 4.2. Different levels of privacy and verifiability are identified in Section 4.3 and 4.4, respectively. Section 4.5 considers interrelations between specific levels of privacy and verifiability.

Section 4.2 is joint work with Hugo Jonker and Wolter Pieters published in [5], while the Sections 4.3 and 4.4 are based on joint work with Melanie Volkamer and, in an earlier version, have been published in [11].

4.1. Terminology and notation

On a high level, any election can be described as follows: each eligible **voter** prefers a certain **candidate** and expresses this preference via his **vote**.[1] The vote is input to the **voting system** in form of the **ballot**: the ballot represents the vote and usually conceals it at the same time, for example by means of cryptography. It can be thought of as an envelope containing the vote. Thus, a ballot is what the voter inputs to the voting system in order to cast a vote for a specific candidate.

Distinguishing between vote and candidate may seem artificial; however, we want to clearly differentiate between real-life *persons* (voters, candidates) and *objects* (votes, ballots) belonging to the voting system. We consider the **voting phase** as the stage during which votes may be cast, and the **tallying phase** as the stage in which cast votes are processed and tallied.[2]

[1] Spoiling one's vote can be modeled by voting for an empty candidate. Such votes do not affect the election result.

[2] Here, we restrict our model to voting and tallying phase. However, verifiability must be considered also beyond the end of the election. This long-term aspect of verifiability is dealt with in Part II of this thesis.

We use the following notation for the entities present in our model:

- $\mathcal{V}$: set of all eligible voters
- $\mathcal{C}$: set of all selectable candidates
- $\mathcal{B}$: set of possible ballots
- $\mathcal{S}$: set of possible votes (or selections)

The links between these entities are expressed by the following functions:

- $\gamma : \mathcal{V} \to \mathcal{C}$ maps a voter v to his preferred candidate c
- $\beta : \mathcal{V} \to \mathcal{B}$ maps a voter v to his ballot b
- $\sigma : \mathcal{V} \to \mathcal{S}$ maps a voter v to his vote s
- $\tau : \mathcal{B} \to \mathcal{S}$ maps a ballot b to the contained vote s
- $\pi : \mathcal{S} \to \mathcal{C}$ maps a vote s to the selected candidate c

Note that $\tau \circ \beta = \sigma$ and $\pi \circ \sigma = \pi \circ \tau \circ \beta = \gamma$. We also use common logical connectives ($\neg$, $\wedge$, $\vee$, $\rightarrow$) and quantifiers ($\forall$, $\exists$) in the following.

4.2. (Un)linkability model

Both privacy and verifiability can be expressed in terms of (un)linkability: while privacy requires unlinkability of voter and vote, verifiability requires linkability of voters and election result. Therefore, this section introduces an intuitive (un)linkability model for voting which captures privacy as well as verifiability. At the same time, this model provides an introduction to the classification of privacy and verifiability which follows in Section 4.3 and 4.4, respectively.

4.2.1. Modeling privacy as unlinkability

Since privacy concerns *individuals*, we consider an *individual-related* model first. It considers individual entities (i.e. a single voter, ballot, vote, candidate) and the mappings between them as introduced in Section 4.1: voter v inputs a ballot $b = \beta(v)$ to the voting system in order to cast a vote $s = \tau(b)$ for his preferred candidate $c = \pi(s)$ (see Figure 4.1).

Privacy requires *unlinkability of voter v and selected candidate $c = \gamma(v)$*, meaning that this link—which certainly exists at the moment the voter casts his ballot containing the vote for the preferred candidate—must remain secret. We assume that there is no *direct* link between the voter and his preferred candidate since such a link would not be under the control of the voting system. Hence, in practice, we always have the decomposition $\gamma = \pi \circ \tau \circ \beta$. The function π which maps a vote to the selected candidate is assumed to be public.

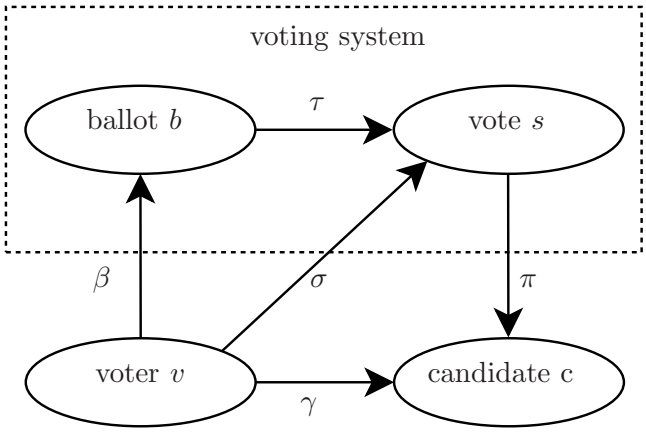

Figure 4.1.: Individual-related model

Thus, privacy can be broken down to unlinkability of voter v and vote $\sigma(v)$, which (due to $\sigma = \tau \circ \beta$) can be established in two ways:

1. unlinkability of voter v and ballot $\beta(v)$
2. unlinkability of ballot b and contained vote $\tau(b)$

Either approach is commonly used in electronic voting schemes: for example, cryptographic primitives such as blind signatures (see Section 2.2.4) or mixnets (see Section 2.2.6) can be used to conceal the link between voter and ballot. Unlinkability of ballot and vote is provided in homomorphic schemes (see Section 2.2.5) where an individual ballot is never decrypted, which means that the corresponding vote is not revealed.

4.2.2. Modeling verifiability as linkability

As (universal) verifiability concerns *groups* of individuals and *sets* of ballots/votes, we now extend our model related to individuals (i.e. a single voter, ballot, vote, candidate) to a scenario which considers *sets* (i.e. all voters, ballots, votes, candidates): the set of received ballots $B(\mathcal{V})$ cast by all voters $\mathcal{V}$ is transformed to the set of all votes $\Sigma(\mathcal{V})$ which determine the election result (see Figure 4.2). We now look at these sets and the mappings between them more closely.

Consider the set of all received ballots:

$$B(\mathcal{V}) = \{b \in \mathcal{B} | \exists v \in \mathcal{V} : \beta(v) = b\}$$

Here we assume that all ballots are unique, which is justified as otherwise ballot duplications (for example by replay attacks) would be easy. Note that $B(\mathcal{V}) = \beta(\mathcal{V})$, which is the image of $\mathcal{V}$ under β. However, we stick to the upper-case notation here in order to ensure consistency with the following definitions.

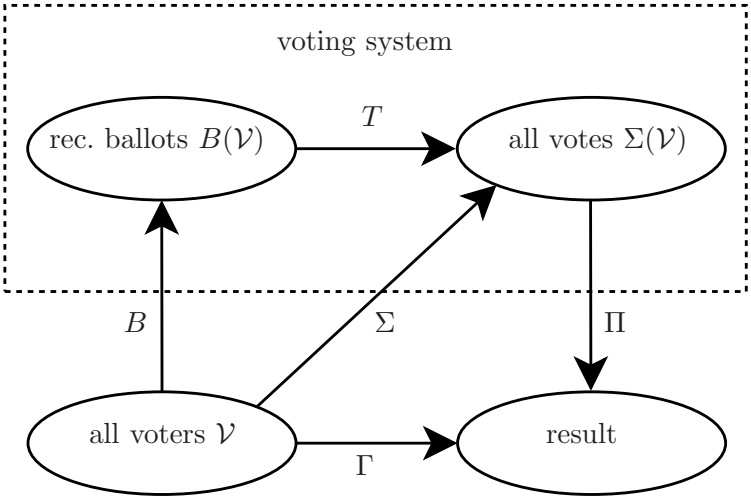

Figure 4.2.: Set-related model

We define

$$\Sigma(\mathcal{V}) = \{(s,n) \in \mathcal{S} \times \mathbb{N} | \exists b \in \mathcal{B} : \tau(b) = s \wedge n = (\#b \in \mathcal{B} : \tau(b) = s)\}$$

as the set of all votes that have been cast, where each cast vote originates from a ballot. Using the definition of $B(\mathcal{V})$ as well as $\tau \circ \beta = \sigma$ (see Section 4.1), we also have

$$\Sigma(\mathcal{V}) = \{(s,n) \in \mathcal{S} \times \mathbb{N} | \exists v \in \mathcal{V} : \sigma(v) = s \wedge n = (\#v \in \mathcal{V} : \sigma(v) = s)\}\,.$$

Note that we do not assume uniqueness of the votes, which means that all votes for candidate c have the same form. The set of received ballots is mapped to the set of cast votes by some transformation T. The election result, for example the number of seats held by different parties in parliament, is obtained by some public transformation Π of the set of all votes $\Sigma(\mathcal{V})$. In the model, the election result is also determined by applying a transformation Γ to the set of all voters $\mathcal{V}$.

Universal verifiability (as introduced in Section 2.1.7) is established by the link between the set of received ballots $B(\mathcal{V})$ and the set of cast votes $\Sigma(\mathcal{V})$ as this link expresses that the received ballots have been transformed into the votes correctly. Eligibility and uniqueness verifiability (see Section 3.2) both refer to the relation between voters and ballots, and are therefore expressed by the link between the set of received ballots $B(\mathcal{V})$ and the set of all voters $\mathcal{V}$. Since the link between the result and the set of all votes is public, universal verifiability (as introduced in Section 2.1.7) is thus expressed by *linkability of the set of all eligible voters $\mathcal{V}$ and the election result.*

Individual verifiability is established by the sum of the following links:

1. $v \mapsto \beta(v)$: the voter is able to identify his ballot
2. $b \mapsto \tau(b)$: the ballot contains the correct vote
3. $b \in B(\mathcal{V})$: the ballot is contained in the set of received ballots

The sum of the first two links corresponds to the concept of cast-as-intended (see Section 3.2): each voter can verify that his ballot correctly represents his choice [KSW05, AN06, Riv06]. The third link matches the established notion of recorded-as-cast: each voter can verify that his ballot has been recorded by the voting system correctly [AN06, BMQR07]. The combination of cast-as-intended and recorded-as-cast has been named "ballot casting assurance" in [AN06]; our definition of individual verifiability matches this concept. By the link between the vote s and the set of all votes $\Sigma(\mathcal{V})$, the voter knows that his vote is included in the tally. Still, the voter cannot pinpoint his vote within the set of all votes as we assume that the votes are not unique.

4.2.3. Unified (un)linkability model

We now merge the individual-related and the set-related model into one (un)linkability model which captures privacy (i.e. desired unlinkability) as well as verifiability (i.e. desired linkability). This model is depicted in Figure 4.3. The individual-related part (see Figure 4.1) is at the bottom, while the set-related part (see Figure 4.2) appears at the top of Figure 4.3, oriented upside down. For better readability we have omitted the function names alongside the arrows as provided in Figure 4.1 and 4.2.

In Section 4.2.1 we have shown that privacy is expressed as unlinkability of voter v and selected candidate $c = \gamma(v)$, while in Section 4.2.2 we have explained that universal verifiability is expressed as linkability of the set of all eligible voters $\mathcal{V}$ and the election result $\Gamma(\mathcal{V})$. Correspondingly, at the bottom of Figure 4.3, privacy is depicted with a "$\times$" alongside the link between voter v and selected candidate $\gamma(v)$, and, at the top of Figure 4.3, universal verifiability is depicted with a "$\checkmark$" alongside the link between the set of all eligible voters $\mathcal{V}$ and the election result $\Gamma(\mathcal{V})$.

At this point a remarkable symmetry of the proposed (un)linkability model becomes apparent: with respect to privacy, we require unlinkability of voter and candidate, whereas, from the set-related perspective, it is exactly the linkability of all voters with the election result that we want in terms of verifiability. Although there is an obvious trade-off between privacy and verifiability, in our model, both are expressed by the same link in the individual-related and the set-related scenario, respectively, which shows the close relation between privacy and verifiability in electronic voting. In the following sections we will frequently refer to our (un)linkability model and consider in more detail how it captures different levels of privacy and verifiability.

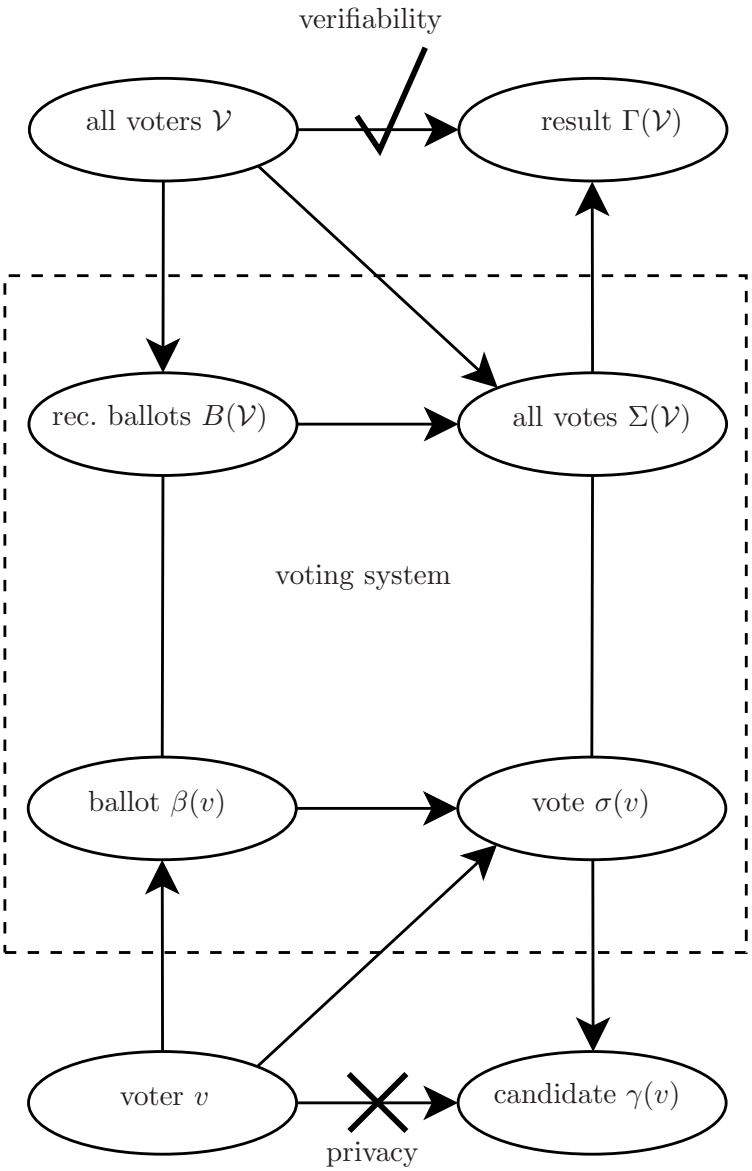

Figure 4.3.: (Un)linkability model

4.3. Privacy

The (un)linkability model introduced in the previous section has provided us with a better intuition for privacy and verifiability in voting and the relation between the two. Our next goal is to gain a deeper and more precise understanding for both properties by decomposing them into different levels. We start by considering different levels of privacy; verifiability is considered in Section 4.4. Note that we consider only levels that are more or less desirable, i.e. we do not provide zero levels such as no privacy at all. In separate paragraphs we investigate whether there exists an order for the different levels, consider these levels in terms of the (un)linkability model provided, and give examples in existing literature that match our definitions.

Recall that voter privacy can be expressed as unlinkability of voter and vote (see Section 4.2), and that voters might also wish to keep it private whether they participated in the election or not (see Section 3.1). Receipt-freeness and coercion-resistance are not considered here; these privacy-related requirements depend on specific adversary capabilities and will therefore be considered within our adversary model in Chapter 5.

Levels

Voter privacy comprises two components: unlinkability of voter and vote (UL) and undecidable voter abstention (A). Unlinkability of voter and vote requires unlinkability of either voter and ballot or voter and vote (see Section 4.2). Furthermore, any of these relations may be provable or not. Thus, we distinguish the following levels of privacy, considering an arbitrary voter:

A.1 Undecidable abstention. It is not possible to decide whether a voter abstained from voting.

A.2 Unprovable abstention. If it is possible to decide whether a voter abstained from voting, then this fact is not provable to third parties.

UL.1 Unlinkability.

- **a** It is not possible to establish a link between voter and ballot.
- **b** It is not possible to establish a link between ballot and vote.

UL.2 Unprovable linkability.

- **a** If it is possible to establish a link between voter and ballot, then the link is not provable to third parties.
- **b** If it is possible to establish a link between ballot and vote, then the link is not provable to third parties.

Order

In order to achieve a better understanding of the different privacy levels, we now investigate the (logical) relations between them. UL.1a establishes unlinkability of voter and ballot, whereas UL.1b establishes unlinkability of ballot and vote. Thus, UL.1a and UL.1b are orthogonal in the sense that they correspond to the two ways in which unlinkability of voter and vote can be established (see Section 4.2). Similarly, UL.2a and UL.2b are orthogonal as UL.2a refers to unprovable linkability of voter and ballot, whereas UL.2b refers to unprovable linkability of ballot and vote. Let therefore UL.1 denote the disjunction UL.1a $\vee$ UL.1b, which reflects that unlinkability of voter and vote is established by means of unlinkability of voter and ballot or unlinkability of ballot and vote (see Section 4.2). Analogously, let UL.2 denote the disjunction UL.2a $\vee$ UL.2b.

Note that UL.2a can be expressed as $p \rightarrow \neg q$, where p is the proposition "it is possible to establish a link between voter and ballot" (which is, in fact, $\neg$UL.1a), and q is the proposition "the link between voter and ballot is provable to third parties". As $p \rightarrow \neg q$ is equivalent to $\neg p \vee \neg q$, $\neg$UL.2a is equivalent to $p \wedge q$, which means that "it is possible to establish a link between voter and ballot, and this link is provable to third parties". Therefore, $\neg$UL.2a expresses that a provable link between voter and ballot can be established. Analogously, $\neg$UL.2b expresses that a provable link between ballot and vote can be established. An unprovable link between voter and ballot or between ballot and vote is expressed by $\neg$UL.1a $\wedge$ UL.2a or $\neg$UL.1b $\wedge$ UL.2b, respectively.

Furthermore, the following logical relations can be identified:

- A.1 $\rightarrow$ A.2: while A.1 is a statement of the form $\neg x$, A.2 can be expressed as $x \rightarrow y$, which is equivalent to $\neg x \vee y$. Thus, A.1 $\rightarrow$ A.2 can be expressed as $x \vee \neg x \vee y$, which is true.
- UL.1a $\rightarrow$ UL.2a (for the same reason why A.1 $\rightarrow$ A.2)
- UL.1b $\rightarrow$ UL.2b (for the same reason why A.1 $\rightarrow$ A.2)
- A.1 $\rightarrow$ UL.1a: if a link between voter v and his ballot can be established, then v must have voted. Thus, $\neg$UL.1a $\rightarrow \neg$A.1 or, equivalently, A.1 $\rightarrow$ UL.1a.
- A.2 $\rightarrow$ UL.2a: if a provable link between a voter v and his ballot can be established, then v must have voted, which can also be proven. Thus, $\neg$UL.2a $\rightarrow$ $\neg$A.2, or, equivalently, A.2 $\rightarrow$ UL.2a.

Summary. Since in Chapter 6 we will frequently refer to the relations just established, let us recall the key findings.

The logical relations between the different privacy levels are summarized in Figure 4.4, where the arrows represent implications. Furthermore, we have defined UL.1 and UL.2 as UL.1a $\vee$ UL.1b and UL.2a $\vee$ UL.2b, respectively, thus expressing the following:

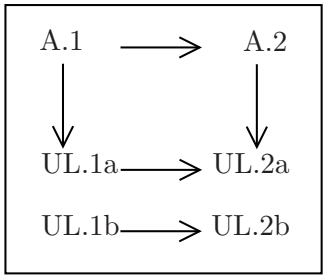

Figure 4.4.: Logical relations between different privacy levels

UL.1 It is not possible to establish a link between voter and vote.

UL.2 If it is possible to establish a link between voter and vote, then the link is not provable to third parties.

We have also learned that we can use the following logical abbreviations in order to derive certain levels of privacy from the original ones defined at the beginning of Section 4.3:

¬UL.2a It is possible to establish a provable link between voter and ballot.

¬UL.2b It is possible to establish a provable link between ballot and vote.

¬UL.1a ∧ UL.2a It is possible to establish an unprovable link between voter and ballot.

¬UL.1b ∧ UL.2b It is possible to establish an unprovable link between ballot and vote.

Reference to model

UL.1a corresponds to unlinkability of voter v and ballot $\beta(v)$ in our model introduced in Section 4.2, while UL.1b refers to unlinkability of ballot b and vote $\tau(b)$ (see Figure 4.5). If at least one of them is provided, unlinkability of voter v and vote $\sigma(v)$ is ensured, which corresponds to UL.1. UL.2a and UL.2b are not directly evident from the model, but refer to the link between voter and ballot or, respectively, to the link between ballot and vote. Voter abstention is not evident from the model.

Examples

Undecidable abstention (A.1) is referred to as invisible abstention by Smith [Smi05], while Hirt names it anonymity [Hir01]. Lambrinoudakis et al. [LGT+03] understand this privacy level contrarily: with regard to cases where voter participation is compulsory and must be verifiable (for example in Belgium, Greece, or Australia), it

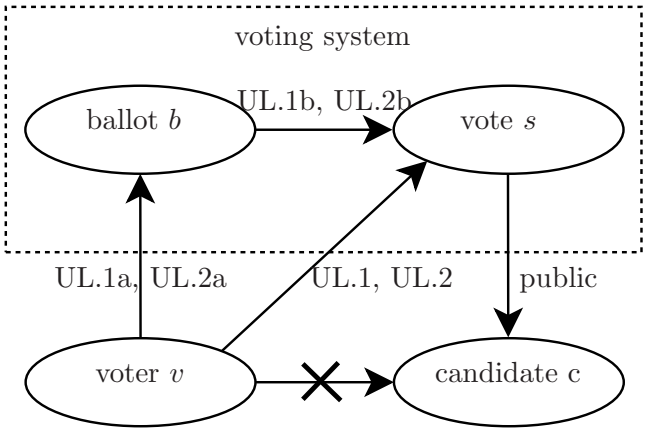

Figure 4.5.: Privacy in the (un)linkability model

must be ascertainable that a certain voter has indeed cast a vote. Thus, they refer to this privacy level as verifiable participation or declarability [LGT+03].

Unlinkability of voter and ballot (UL.1a) is referred to in [VV08, Objective 162]: "the data [...] cannot be used to link the voter to his vote (in plaintext or in encrypted form)". Recall that, in our terms, the encrypted vote is the ballot, see Section 4.1. The definitions of privacy provided in [Rie98, BM03, LGT+03, Cet07] correspond to our definition of unlinkability of voter and vote (UL.1). Unprovable linkability of voter and vote (UL.2) is referred to in [VK06].

4.4. Verifiability

Verifiability is, first of all, closely related to accuracy. However, it has also been claimed that eligibility and uniqueness should be verifiable (see Section 3.2). Therefore, we consider these security requirements first. The existence of a public bulletin board is assumed as a precondition for verifiability in the following.[3]

Accuracy

Accuracy states that only valid votes should be counted (soundness), and that each valid vote should be counted correctly (completeness and inalterability), see Section 2.1.1. This is equivalent to requiring that no cast vote may be altered, deleted or duplicated, and no invalid votes may be counted in the final tally (i.e. spoilt votes are to be counted as such without incorporating them into the tally). Thus, accuracy

[3] Electronic voting schemes using direct recording electronic (DRE) voting machines usually provide for a paper trail which can be used for a manual recount without referring to a public bulletin board. However, as we explicitly include online voting in our considerations, the existence of a public broadcast channel must be assumed for verifiability.

essentially refers to the *integrity* of the votes.[4] In voting systems, we have two types of integrity:

Integrity of the individual vote: no vote is deleted or altered in voting and tallying phase.

Integrity of the set of all votes: no vote is deleted or altered in tallying phase, and no vote is added to the set of all votes in tallying phase.

The latter is restricted to the tallying phase since the integrity of the set of all votes can only be assessed once this collection is complete, that is, after the voting phase has ended (cf. [Pie06]). Note that we speak about integrity of *votes* as the ballots may be processed and, thus, modified in tallying phase, for example by a reencryption mixnet [JJR02].

While individual verifiability refers to the integrity of the individual vote, universal verifiability usually refers to the integrity of the set of all votes: each voter can verify the integrity of his own vote, and anyone can verify the integrity of the set of all votes. However, it has been claimed that eligibility and uniqueness should also be universally verifiable, i.e. verifiable by anyone (see Section 3.2). Therefore, both must be considered to be potentially subject to universal verifiability. Thus, we refer to the accuracy-related component of universal verifiability as **accuracy verifiability** in the following.[5]

Eligibility and uniqueness

Eligibility requires that only eligible voters cast a vote, while uniqueness requires that each voter casts at most one vote that is counted; together they are referred to as democracy (see Section 2.1.2). This security requirement should also be universally verifiable, i.e. anyone should be able to verify that only eligible voters cast a vote, and that each voter cast at most one vote. As for accuracy verifiability, we consider **eligibility verifiability** and **uniqueness verifiability** to be components of universal verifiability.

4.4.1. Universal verifiability

Levels

In the previous paragraphs we have seen that accuracy as well as eligibility and uniqueness should be universally verifiable. Thus, we distinguish the following levels of universal verifiability:

[4] According to Pieters, integrity is the security variant of the safety property of accuracy: safety aims at preventing errors (i.e. unintentional failure), while security refers to preventing unauthorized data manipulation (i.e. intentional tampering) [Pie08].

[5] Note an important difference between privacy and accuracy: while privacy must not be compromised, accuracy must not be compromised *unnoticed*. It is, of course, preferable to prevent any violations of accuracy in order to avoid having to rerun the election. Still, privacy is usually not considered to be subject to verifiability (cf. [VSL+09]).

AV.1 Continuous accuracy verifiability. Anyone can verify all parts of the correct processing of the ballots in tallying phase.[6]

AV.2 Discrete accuracy verifiability. Anyone can verify certain (but not all) parts of the correct processing of the ballots in tallying phase.

EV.1 Unconditional eligibility verifiability. Anyone can verify that only eligible voters cast votes without having to trust any party involved in establishing eligibility.

EV.2 Conditional eligibility verifiability. Anyone can verify that only eligible voters cast votes; however, it is required to trust certain parties involved in establishing eligibility.

QV.1 Unconditional uniqueness verifiability. Anyone can verify that each voter cast at most one vote that has been counted without having to trust any party involved in establishing uniqueness.

QV.2 Conditional uniqueness verifiability. Anyone can verify that each voter cast at most one vote that has been counted; however, it is required to trust certain parties involved in establishing uniqueness.

Order

There is no relation between the different levels of universal verifiability in terms of logic. However, one thing is common to all three components: the two main levels distinguish the two cases that you either can verify all steps by yourself, or that you have to trust certain parties involved. If a voting scheme offers discrete accuracy verifiability, this implies that you have to trust certain parties involved in processing the votes, while this is not required for continuous accuracy verifiability. Unconditional eligibility verifiability allows to verify that ballots have been cast only by eligible voters without having to trust anyone, while conditional eligibility verifiability requires trust in certain parties involved in establishing eligibility. Analogously, unconditional uniqueness verifiability allows to verify that each voter cast at most one vote without having to trust anyone, while conditional uniqueness verifiability requires trust in certain parties involved in establishing uniqueness. Thus, the level of universal verifiability is directly related to the level of *trust* which must be put into the voting system. A high level of verifiability is, of course, preferable to a strong need for trust.

Reference to model

In terms of linkability, universal verifiability comprises

[6] Recall that accuracy verifiability refers to the integrity of the set of all votes and, therefore, is restricted to the tallying phase since the integrity of the set of all votes can only be assessed once this collection is complete, that is, after the voting phase has ended (cf. [Pie06]).

1. linkability of all voters with the set of received ballots (eligibility and uniqueness verifiability), and

2. linkability of received ballots and counted votes (accuracy verifiability).

In terms of the (un)linkability model introduced in Section 4.2, accuracy verifiability refers to the link between the received ballots $B(\mathcal{V})$ and the set of all votes $\Sigma(\mathcal{V})$ (and, thus, matches the concept of counted-as-recorded [AN06]). Eligibility and uniqueness verifiability are expressed by the link between all voters $\mathcal{V}$ and the set of received ballots $B(\mathcal{V})$. These relations are depicted in Figure 4.6.

In the model, eligibility requires that for each ballot in the set of received ballots, there is a voter in the set of all eligible voters who maps to this ballot. This is provided due to our definition of the set of received ballots $B(\mathcal{V})$ (see Section 4.2). Uniqueness additionally requires that each voter is mapped to one ballot only. The difference between the two levels of each component of universal verifiability (i.e. AV.1 and AV.2, EV.1 and EV.2, QV.1 and QV.2) is not evident from the model.

Examples

The definitions of universal verifiability provided in [CMFP+06, Cet07, Smi05] correspond to our definition of continuous accuracy verifiability including verifiability of eligibility and even uniqueness, while the definition in [AN06] corresponds to continuous accuracy verifiability including verifying eligibility, but not uniqueness. The definitions of universal verifiability provided in [Hir01, MN06, Pie06, DKR09] match continuous accuracy verifiability without verifying eligibility or uniqueness.

4.4.2. Individual verifiability

Levels

Recall that individual verifiability gives the voter the possibility to verify that his ballot is contained in the set of received ballots and contains the correct vote, i.e. the vote which the voter intended to cast (see Section 4.2). Also, individual verifiability is useless unless the voter can file a complaint in case there is something wrong with his ballot (see Section 3.2). Thus, we distinguish the following levels of individual verifiability:

IV.1 Inner individual verifiability. The voter can verify whether his ballot contains the vote which the voter intended to cast.

IV.2 Outer individual verifiability. The voter can verify whether his ballot is correctly included in the set of received ballots which will be counted.

CO.1 Chance of objection w.r.t. inner individual verifiability. If his ballot does not contain the vote which the voter intended to cast, the voter can claim this and prove that his objection is justified.

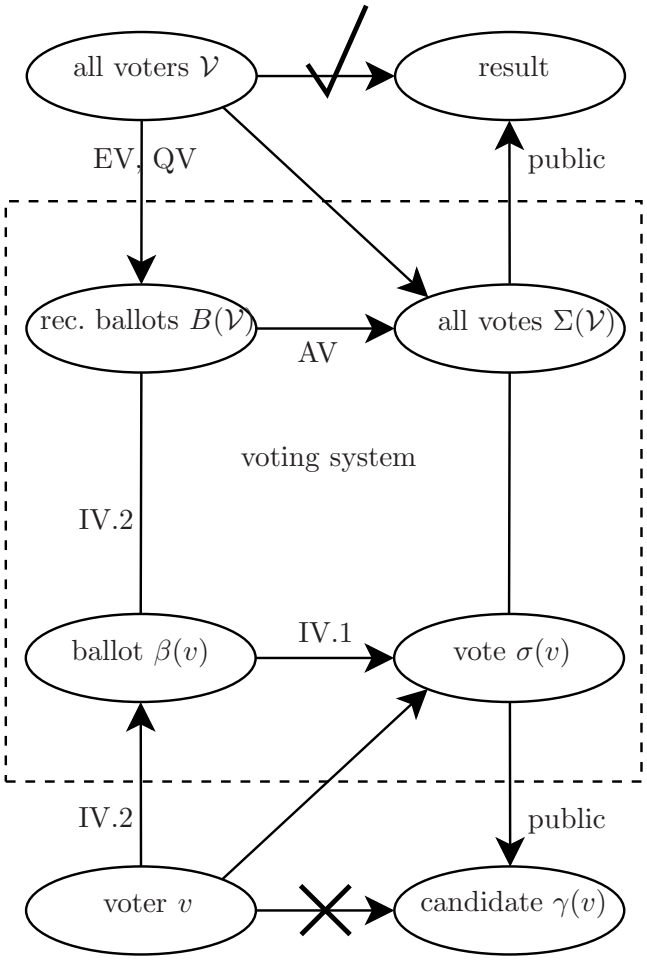

Figure 4.6.: Verifiability in the (un)linkability model

CO.2 Chance of objection w.r.t. outer individual verifiability. If his ballot does not appear on the bulletin board correctly, the voter can claim this and prove that his objection is justified.

Order

IV.1 and IV.2 are orthogonal in the following sense: IV.1 refers to the vote contained in the ballot, and IV.2 refers to the ballot contained in the set of received ballots. In particular, the ballot referred to by IV.1 *has not necessarily been cast yet*. Therefore, it may be a different ballot than the one referred to by IV.2. For instance, IV.1 can refer to dummy ballots which are audited by the voter before he casts his actual vote (we will see examples for this in Section 6). Therefore, in line with our above definitions, the voter can only be assured that his *cast* ballot contains the vote he intended to cast if IV.1 applies to the *cast* ballot, in which case IV.1 and IV.2 refer to the same ballot.

Furthermore, CO.1 implies IV.1: if the voter cannot verify whether his ballot contains the vote he intended to cast, he has no chance of objection. Similarly, CO.2 implies IV.2: if the voter cannot verify whether his ballot has been published on the bulletin board, he has no chance of objection. On the other hand, if individual verifiability without a chance of objection is provided, this means that the voter is able to recognize that his ballot was not processed correctly, but has no chance to claim this. This implies that the voter's preference is not captured by the voting system correctly, or even not at all.

Reference to model

IV.1 refers to the link between the ballot b and the vote $\tau(b)$. IV.2 refers to the link between the ballot b and the set of received ballots $B(\mathcal{V})$ and, additionally, requires the voter to recognize his own ballot, which is expressed by the link between the voter v and his ballot $\beta(v)$. These relations are depicted in Figure 4.6. Note that IV.1 $\wedge$ IV.2 matches the definition of ballot casting assurance in [AN06] (cf. Section 4.2). The voter's chance of objection is not captured by the model.

Examples

The definitions of individual verifiability provided in [Hir01, SP06, DKR09] correspond to our definition of outer individual verifiability, while the definitions in [Cet07, LGT+03, Smi05] match inner individual verifiability. The voter's chance of objection is also considered in [Rie98, BM03, LGT+03]. [LGT+03] distinguishes a privacy-preserving and a privacy-compromising variant hereof. We do not consider this differentiation since any chance of objection seems to be useless if it forces the voter to disclose his voting decision.

4.5. Interrelations

In the following we analyze the interrelations between universal and individual verifiability on the one hand and privacy and verifiability on the other hand. We also investigate whether certain levels of privacy and verifiability are incompatible in our model. Relations between different levels of either privacy, universal or individual verifiability are not considered here as these have already been addressed in Section 4.3, 4.4.1 and 4.4.2, respectively.

First we consider the relation between individual and universal verifiability. Recall that individual verifiability refers to the integrity of the individual vote in voting phase. Note that the corresponding property in terms of being *universally* verifiable is accuracy verifiability, not universal verifiability, since the latter comprises the possibility to verify other properties (i.e. eligibility and uniqueness) as well. Accuracy verifiability refers to the integrity of the set of all votes in tallying phase (see Section 4.4). Both properties are related with each other as follows: by individual verifiability, the voter can be assured that his ballot contains the correct vote (IV.1) and that it has been included in the set of received ballots which will be counted (IV.2). By continuous accuracy verifiability (AV.1), anyone can be assured that the received ballots have been processed correctly and revealed exactly the votes that had been cast in voting phase. If only discrete accuracy verifiability (AV.2) is provided, some of the steps involved when processing the ballots may not be verifiable.

A sequential view of individual verifiability and accuracy verifiability is depicted in Figure 4.7, assuming that the voter verifies his cast ballot after the voting phase has ended. The lines delimited by arrows denote the range of the different levels of individual verifiability and accuracy verifiability, respectively. The dashed line used to depict AV.2 indicates that, for discrete accuracy verifiability, not all steps of the correct processing of the ballots in tallying phase are verifiable. The dashed line used for extending IV.1 toward the end of the voting phase indicates that IV.1 can apply both to cast and uncast ballots (see Section 4.4.2). If IV.1 applies to the *cast* ballot, both IV.1 and IV.2 refer to the *same* ballot (i.e. the one cast by the voter), and the two corresponding lines can be thought of as collapsing into one single line. In that case, accuracy is verifiable throughout the whole voting and tallying phase. The transition from *individual* votes in voting phase to *all* votes in tallying phase is required since we do not want anyone (not even the voter himself) to be able to track individual votes in tallying phase, as this would imply establishing a link between voter and vote.

Now we turn to the relation between privacy and verifiability. We have already seen that, in the (un)linkability model, both privacy and verifiability are expressed by the same link in the individual-related and the set-related scenario, respectively (see Section 4.2). Viewed more closely, the following correspondence between our definitions of privacy and verifiability becomes apparent: UL.1a, UL.2a and IV.2 refer to the link between voter v and ballot $\beta(v)$ (see Figures 4.5 and 4.6): UL.1a requires unlinkability of voter and ballot, while UL.2a requires unprovable linkability of voter and ballot. IV.2 presupposes that the voter recognizes his ballot, which is

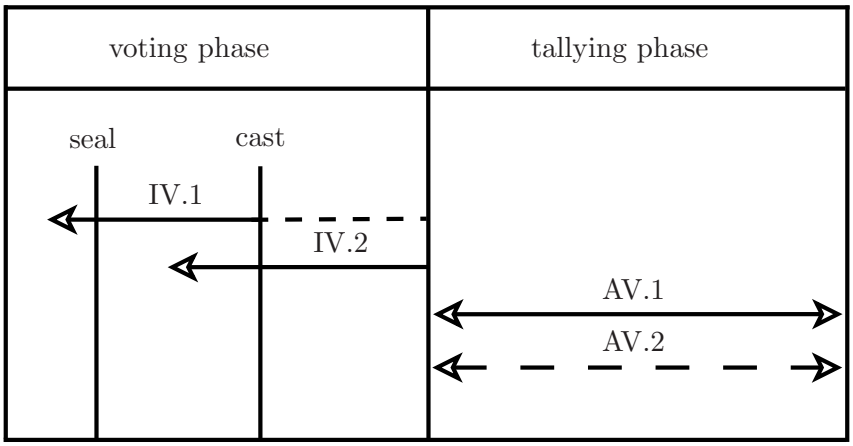

Figure 4.7.: Sequential view of individual verifiability and accuracy verifiability

as well expressed by the link between voter and ballot, and additionally requires that the ballot can be linked to the set of received ballots. If both UL.1a and IV.2 are supposed to hold, then the link between the voter and his ballot must not be identifiable by any other entity. If both UL.2a and IV.2 shall hold, then any link between the voter and his ballot must not be provable to third parties. In particular, this implies that the ballot must not be published on the bulletin board next to the voter's name.

Similarly, UL.1b, UL.2b and IV.1 refer to the link between ballot b and vote $\tau(b)$: UL.1b requires unlinkability of ballot and vote, while UL.2b requires unprovable linkability of ballot and vote. IV.1 requires that the voter is able to link ballot and vote. If both UL.1b and IV.1 are supposed to hold, then it must not be possible for any other entity to establish the link between the ballot and the contained vote, while for providing UL.2b and IV.1 at the same time, this link must not be provable to third parties. Therefore, inner individual verifiability (IV.1) can easily be reconciled with unlinkability of ballot and vote if IV.1 is provided for *uncast* ballots only. We get back to this in Chapter 6.

5. Adversary model

In the previous chapter we have proposed an (un)linkability model for voting, and we have compiled the conceivable levels of privacy and verifiability. We can already apply the results to existing voting schemes by determining the level of privacy and verifiability provided. However, for a more profound analysis we need to consider the scheme in the presence of an adversary.

One approach would be to take the adversary model proposed by Dolev and Yao [DY83]. However, this model has two drawbacks:

1. It may be too strong: with respect to our goal of establishing a taxonomy for privacy and verifiability in voting, we want to differentiate not only between several levels of these security properties, but also between different levels of adversarial power. For example, elections in associations may require a less powerful adversary than parliamentary elections, or it may be of interest to determine the impact of a single person with limited power, not an adversary who can control all communications. The Dolev-Yao attacker model lacks the flexibility required to accomplish this.

2. It may be too *weak*: the Dolev-Yao model assumes that that cryptography works perfectly. However, cryptographic schemes may turn out to be broken, and messages encrypted with such schemes may eventually be decrypted without using the secret key. In electronic voting schemes, encrypted data is often published for the sake of verifiability (for example encrypted votes posted to a bulletin board next to the voters' names). Thus, such attack scenarios constitute a serious threat in electronic voting, but they are not captured by the Dolev-Yao model.

Therefore, this chapter provides a comprehensive collection of different adversary capabilities. They constitute building blocks which can be combined in order to obtain a fine-tuned adversary model for specific use cases. We also analyze how the individual adversary capabilities can be used to mount attacks on privacy and verifiability.

Chapter overview

In Section 5.1 we define the setting which is taken as a basis for the following considerations. Subsequently, we consider different adversary capabilities in Section 5.2. In Section 5.3 and 5.4 we consider which attacks on privacy or, respectively, verifiability arise from specific adversary capabilities. Sections 5.1 and 5.2 of this chapter are joint work with Hugo Jonker and Wolter Pieters published in [5].

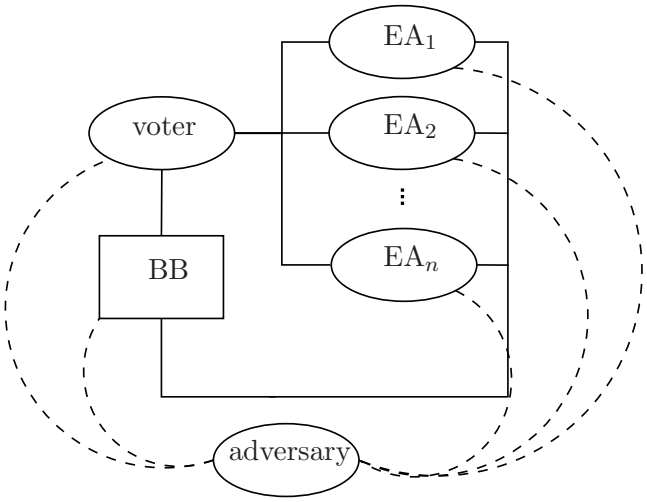

Figure 5.1.: Adversary communication model

5.1. Setting

In order to define our setting, we consider the components of a generic electronic voting system in the presence of an adversary (see Figure 5.1). Such a system consists of voters, several election authorities (EAs), a public bulletin board (BB), and an adversary. The voters are registered by the election authorities and subsequently cast ballots which are processed by (possibly different) election authorities. The bulletin board is used by the voters and the election authorities in order to post messages for reasons of verifiability. We assume that the election authorities communicate via the bulletin board. Thus, in our setting, the following communication channels do exist, and are represented by solid lines in Figure 5.1:

- from the voter and each election authority to the bulletin board
- between the voter and each election authority

The communication occurring over any of these channels may employ a range of cryptographic primitives such as encryption or blind signatures (see Section 2.2). Besides affecting the existing communication channels, the adversary can possibly also create new communication channels (represented by dashed lines in Figure 5.1) to existing entities. Note that, even if the adversary has none of the capabilities considered below, he learns the information posted to the bulletin board as it is assumed to be public knowledge (see Section 2.2.7).

We restrict ourselves to protocol level in the following and, therefore, we do not consider implementation aspects such as corrupted software developers or administrators.[1]

[1]For the same reason, we do not consider side channel attacks, for example those exploiting electromagnetic radiation emanating from voting machines, see the Tempest discussion [Pie09].

5.2. Adversary capabilities

We consider two different categories of adversary capabilities: communication abilities and cryptographic abilities. For the former, we further distinguish between the adversary's abilities concerning existing communication channels, and his ability to create new channels. This leads to the following categorization of adversary capabilities:

I. Existing communication channels

II. New communication channels

III. Cryptography

We consider each of them more thoroughly in the following.

5.2.1. Capabilities concerning existing communication channels

We distinguish the following adversary capabilities regarding the ways in which the adversary can affect existing communication channels:

Ia. The adversary is able to **detect channel usage**.

Ib. The adversary is able to **determine the sender** of a message.

Ic. The adversary is able to **eavesdrop** on the communication channels.

Id. The adversary is able to **block** communication channels and thus suppress messages that are sent via these channels.

Ie. The adversary is able to **inject** messages into the communication channels.

If. The adversary is able to **modify** messages sent over the communication channels.

An untappable channel provides perfect privacy [JCJ05] and thus protects against an adversary with any of the above capabilities. An anonymous channel protects against an adversary with capability Ib, but is still subject to attacks by an adversary with any of the capabilities Ia and Ic-f. Thus, when analyzing voting schemes in light of the adversary capabilities, Ib and Ia-f are not considered for channels which are assumed to be anonymous or untappable, respectively.

5.2.2. Capabilities concerning new communication channels

For the second category, we consider the following adversary capabilities:

IIa. The **voter** can send messages to the **adversary**.

IIb. An **election authority** can send messages to the **adversary**.

IIc. The **adversary** can send messages to a **voter**.

IId. The **adversary** can send messages to an **election authority**.

IIe. The **adversary** can post messages to the **bulletin board**.

By repeated use of powers IIa-d, the adversary establishes one-way or two-way communications with groups of voters and/or groups of election authorities. Scenarios IIb and IId can refer both to different authorities (for example registration authority or tallying authority) and to different members of the same authority in a distributed setting (for example a tallying authority divided into several tellers).

Scenarios IIa and IIb model voters or, respectively, election authorities who cooperate with the adversary by leaking secrets, whereas IIc and IId model an adversary who coerces election authorities or voters, respectively (this is considered more thoroughly in the next paragraph). The difference between Ic and IIa, respectively IIb, is that for Ic, the adversary can know all information sent via the affected channel, while for the other two variants he is restricted to the information provided to him by the collaborating party, i.e. the voter or the election authority, respectively.[2] Capability IIe models an adversary who can corrupt the bulletin board by posting unauthorized messages.

Receipt-freeness and coercion-resistance

The scenarios IIa and IIc are inspired by [KT09] and aim at modeling receipt-freeness and coercion-resistance, respectively: scenario IIa models a voter who cooperates with the adversary by leaking secrets (for example receipts proving his vote). Scenario IIc models an adversary who is trying to coerce the voter, for example by furnishing the voter with voting material in order to cast a specific (or a random) vote. Combining IIa and IIc models interaction between voter and adversary and covers simulation, randomization and forced-abstention attacks (cf. Section 2.1.6 and [JCJ05]). This scenario corresponds to the two-way communication channel considered in [KT09]. Similarly, IIb and IId model the case that an election authority cooperates with the adversary or, respectively, is coerced by the adversary.

5.2.3. Cryptographic capabilities

For the third category, we do not assume that cryptography works perfectly as opposed to the standard Dolev-Yao attacker model [DY83]:

IIIa. The adversary is able to break any cryptography which provides only computational security.

As noted above, it makes sense to consider the case that the adversary can break cryptography in order to identify breaches of privacy that may occur, for example, at a time when cryptographic algorithms have become insecure. Thus, even if voter and ballot or ballot and vote cannot be linked at present, in the long term this may

[2] This information, however, has not necessarily been sent elsewhere before.

become feasible, for example because cryptographic schemes providing only computational security have become insecure.[3] A voting scheme using cryptographic algorithms which provide information-theoretic security is secure against an adversary with capability IIIa.

5.3. Attacks on privacy

So far in this chapter we have defined a set of adversary capabilities which are independent of the security properties considered in Chapter 4. In Chapter 6 we will analyze to what extent an adversary with different capabilities can affect the level of privacy and verifiability provided by different voting protocols. Therefore, in preparation for Chapter 6, we now consider how the adversary can use these capabilities to attack privacy or verifiability. Note that the following considerations are preliminary: more precise statements regarding the relation between the adversary capabilities and possible attack scenarios require focusing on a specific voting protocol; we will do so in Chapter 6.

We start by considering the adversary capabilities which are relevant for attacks on voter privacy, and subsequently consider the capabilities which can be used to attack verifiability in Section 5.4. Each time we go through the different categories of adversary capabilities as defined in Sections 5.2.1 to 5.2.3.

5.3.1. Capabilities concerning existing communication channels

If the adversary is able to detect usage of the channel from the voter to the voting system (Ia) and, additionally, can determine the sender of a message (Ib), he will most certainly be able to decide whether a certain voter cast a ballot. Undecidable voter abstention (A.1, see Section 4.3) is lost in this case (supposed that this privacy level had been provided before).

If the adversary can determine the sender of a message (Ib) and, at the same time, eavesdrop on the channel which is used by the voter to cast his ballot (Ic), the adversary can link the voter and his ballot. This implies that unlinkability of voter and ballot (UL.1a) is lost, although the link is not provable (UL.2a), unless the voter has signed his ballot. Note that this attack may, however, not necessarily degrade the privacy level provided, for example in a voting system which posts ballots next to the names of voters who cast them, thereby publishing the link between the voter and his ballot.

As we will see in Section 5.4, the remaining capabilities of category I can mostly be exploited to compromise accuracy and eligibility.

[3] Long-term security in electronic voting and long-term privacy in particular has been addressed for example in [VH04], [VK06] and [GKM+06].

5.3.2. Capabilities concerning new communication channels

A channel from the voter to the adversary (IIa) can be used by the voter to disclose his ballot or even his voting decision to the adversary, in which case either unlinkability of voter and ballot (UL.1a) or even unlinkability of voter and vote (UL.1) is compromised. If the adversary obtains sensitive information (such as private keys) from corrupted election authorities (IIb), this information may reveal the link between ballot and vote (recall that the ballot is the encrypted or otherwise concealed vote, cf. Section 4.1). In this case unlinkability of ballot and vote (UL.1b) is lost, and if the link between the voter and his ballot is public, then voter and vote can be linked (i.e. UL.1 is lost). Note that this attack is particularly dangerous since the according link may be revealed for *all* voters at the same time. An adversary with capability IIc can provide the voter with a predetermined ballot to be cast. Thus, voter and vote can obviously be linked (no UL.1). Moreover, as the adversary acts as the voter in this case, the voter is excluded from the election. As we will see in Section 5.4, the remaining capabilities of category II (i.e. IId and IIe) can rather be exploited to compromise eligibility.

5.3.3. Cryptographic capabilities

If the ballot is an encryption of the vote (which holds for most voting schemes), an adversary who can break cryptography (IIIa) is able to link ballot and vote. Unlinkability of ballot and vote (UL.1b) is compromised in this case, which may lead to a total loss of privacy in case the link between voter and ballot is public. Note that the threat posed by an adversary with capability IIIa is far more dangerous for privacy than most of the capabilities we considered so far (besides IIb): the attacks can be established on a massive scale, i.e. for all voters at the same time.

5.4. Attacks on verifiability

Unlike with privacy, verifiability is a requirement for which attack scenarios cannot be defined straightforwardly. To understand this, let us recall what verifiability comprises according to Section 4.4: while universal verifiability allows the public to verify that the integrity of the collection of cast votes (AV) as well as eligibility (EV) and uniqueness (QV) have been maintained, individual verifiability allows each voter to verify the correctness of ballot preparation and the integrity of his individual vote or ballot (IV). Thus, verifiability aims at proving that accuracy, eligibility and uniqueness have been met, and thus helps to detect attacks aimed at these properties. Consequently, verifiability is compromised if a violation of any of these properties remains undetected. In the following we thus consider specific attacks on accuracy, eligibility and uniqueness which are enabled by the adversary capabilities defined in Section 5.2.

5.4.1. Capabilities concerning existing communication channels

As explained in Section 5.3, the capabilities Ia-c can be exploited to compromise privacy. An adversary limited to such abilities cannot actively interfere with the voting system and, therefore, cannot compromise verifiability.

An adversary able to block the channel from the voter to the voting system (Id) can prevent the cast ballot from being received by the voting system. This attack may be recognized by the voter due to outer individual verifiability (IV.2) and also claimed if an according chance of objection (CO.2) is provided. Otherwise, the integrity of the individual vote is compromised since a legitimately cast ballot is not captured by the voting system (and therefore lost). If the adversary injects his own ballot into the communication channel from any voter to the voting system (Ie), he may seize this voter's right to vote. Should the voter not have cast his ballot yet, he is deprived of this possibility, which compromises eligibility. The voter may be able to recognize the fraud due to outer individual verifiability (IV.2), and also be able to claim it if an according chance of objection (CO.2) is provided. It is, however, unlikely for a voter who has not voted yet to verify whether someone has cast a ballot in his place (cf. [Adi08] and Section 6.1.2). If the voter has already cast his ballot and the adversary, in addition to injecting messages, has also the capability to block this channel (Id), he may substitute this voter's ballot with his own illegal one, thus infringing both accuracy (i.e. integrity of the individual vote) and eligibility. Again, the voter may recognize (IV.2) and claim this (CO.2). An adversary equipped with capability If is able to modify ballots that are being sent to the voting system, thus compromising accuracy. Such attacks can be detected by the voter if outer individual verifiability (IV.2) is ensured, and reported if an according chance of objection (CO.2) is provided. If the option of multiple voting is provided, the voter can also recast his vote.

5.4.2. Capabilities concerning new communication channels

As explained in Section 5.3, the capabilities IIa-c can mostly be used to compromise privacy. If limited to capability IIa or IIb, the adversary can merely obtain messages from the voter (IIa) or an election authority (IIb), which is not sufficient to compromise verifiability. Similarly, only privacy is affected by an adversary sending messages to a voter (IIc) in terms of providing this voter with a predetermined ballot.

Capability IId allows the adversary to send messages to election authorities. This can be exploited in registration phase by forcing the registration authority to add the adversary to the voter list, thus compromising eligibility. Listing ineligible voters may be noticed if unconditional eligibility verifiability (EV.1) is provided; in case only conditional eligibility verifiability (EV.2) is provided, an election authority must be trusted for the verification. An adversary capable of sending messages to the bulletin board (IIe) can post unauthorized ballots which may be counted by the voting system. If this attack happens in voting phase, it affects eligibility, and may

be detected by eligibility verifiability (EV).[4] If the adversary mounts this attack in tallying phase, then integrity of the set of all votes is as well compromised, which may be detected by accuracy verifiability (AV). Note that, if the adversary is an eligible voter, this attack affects uniqueness as well, and may be detected by uniqueness verifiability (QV).

5.4.3. Cryptographic capabilities

An adversary able to break cryptography (IIIa) can mount attacks on privacy as explained in Section 5.3. In a voting scheme which uses electronic signatures to authenticate voters, the adversary can use this capability to forge a voter's signature. This way an unauthorized ballot is authenticated, which compromises eligibility.

5.5. Summary

In Section 5.2 of this chapter we provided several adversary capabilities, divided into different categories related to communication and cryptography. These capabilities can be used as building blocks for defining a fine-tuned adversary model for specific election scenarios. In Section 5.3 and 5.4 we assessed how the adversary capabilities defined in Section 5.2 can be used to mount attacks on privacy and verifiability, respectively. Overall, it turned out that attacks on privacy are usually *passive* (e.g. eavesdropping, obtaining information from corrupted voters or election authorities), while attacks on verifiability (i.e. undetected attacks on accuracy, eligibility and uniqueness) require the adversary to *actively* interfere with the voting system (e.g. by modifying sent messages or injecting new messages). Table 5.1 provides an overview of the results. We will reconsider the attack types enabled by the different adversary capabilities at the end of Chapter 6.

[4] Note that integrity of the set of all votes is not affected in this case since this collection is not complete until the voting phase has ended, cf. Section 4.4.

Table 5.1.: Adversary capabilities affecting the security requirements

	privacy	verifiability		
		accuracy	eligibility	uniqueness
Ia+b	X			
Ib+c	X			
Id		X		
Ie			X	
If		X		
IIa	X			
IIb	X			
IIc	X			
IId			X	
IIe		X	X	X
IIIa	X		X	

6. Application

In Chapters 4 and 5, we have

1. introduced an (un)linkability model for voting which captures privacy as well as verifiability,
2. compiled different levels of privacy and verifiability, referring to our (un)linkability model, and
3. provided a list of different adversary capabilities that can be employed to attack privacy and verifiability.

Together, these three components form our taxonomy for privacy and verifiability in electronic voting. In this chapter we demonstrate the applicability of the taxonomy by using it to analyze the security of several state-of-the-art voting schemes.

Chapter overview

We apply the taxonomy to Helios 1.0 [Adi08] in Section 6.1, Helios 2.0 [AdMPQ09] in Section 6.2, and Prêt à Voter [CRS05] in Section 6.3. After giving a brief description of the respective scheme, we first classify the basic level of privacy and verifiability provided, and subsequently consider attacks on privacy and verifiability which can be mounted by an adversary with different capabilities. We use the notation introduced in Chapters 4 and 5. In particular, we abstract from implementation details and express each voting protocol in terms of the setting described in Section 5.1. The results of our analysis are discussed in Section 6.4.

An earlier version of Section 6.1 and 6.2 has been published as [7], while Section 6.3 has been published in [5].

6.1. Helios 1.0

6.1.1. Description

Helios 1.0 is a remote electronic voting system [Adi08] which has been designed for elections where the risk of coercion can be considered low, as for example universities and local clubs. Helios 1.0 has a single trusted component, the Helios server, and uses a public bulletin board. Since there is no direct communication between the voter and the bulletin board, the latter can be considered part of the Helios server.

In registration phase, voters obtain an email with their user name and the randomly generated election-specific password. This email also contains the Internet

address of the virtual voting booth provided by the Helios server as well as a hash of the election parameters. Upon entering the Internet address, all parameters and templates required for preparing the ballot are downloaded. Ballot preparation happens offline and is separated from ballot casting: anyone can generate and audit ballots; voters are authenticated only at ballot casting time.

After the user has made his choices and finished ballot preparation by sealing the ballot, the voting system commits to the encrypted vote by displaying a hash of the ciphertext. Next, the correct preparation of the ballot can either be audited, or the ballot can be cast after the voter has been authenticated (**Benaloh challenge**, see [Ben07]). If the user chooses to audit the ballot, the ciphertext and the randomness used for encryption is displayed, which allows for checking that the vote was correctly transformed into the ballot.[1] The voter can either run his own verification code to ensure that the encryption was correct, or he can use the Ballot Encryption Verification program provided. If the voter chooses to cast the ballot, he is authenticated and his ballot is recorded and posted to the bulletin board next to the voter name. The voter obtains a confirmation email containing his encrypted vote and its hash.

In tallying phase the ballots are processed by a mixnet (see Section 2.2.6). Proofs of correct shuffling and correct decryption are provided using the method proposed in [SK95] and published on the bulletin board. After all proofs have been generated and the result has been tallied, the Helios server deletes the permutation, randomness, and secret key for that election.

6.1.2. Analysis

Basic level of privacy and verifiability

The hashed encrypted vote is published next to the voter name on the bulletin board, and the encrypted vote is visible as well. This establishes a provable[2] link between voter and ballot as anyone can verify the link on the bulletin board. Thus, if the adversary is restricted to public information, he can provably link voter and ballot, but cannot link ballot and vote, i.e. we have UL.1b, but no UL.1a and no UL.2a (see the first row of Table 6.1). Voter abstention is decidable and provable (no A.1, no A.2) as the bulletin board shows which voters have cast a vote by publishing the hashed encrypted vote next to their name.

The correct processing of the cast votes is continuously verifiable by the public (AV.1) due to the proofs of correct mixing and tallying. Eligibility is verifiable since Helios 1.0 publishes a voters' register containing the names of all eligible voters [Adi08, Section 4.2]. Thus, anyone can check, without having to trust anyone, that

[1] If the vote is cast hereafter, a different random value is used for encryption, thus producing a different ciphertext.

[2] We assume that all public information is provable. The contents of the bulletin board are assumed to be signed by an election authority.

ballots were cast only by voters listed in the voters' register and that each voter cast at most one vote (EV.1, QV.1).[3]

Helios 1.0 allows the voter to verify that his hashed encrypted vote is published next to his name on the bulletin board (linkability of voter and ballot). Thus, outer individual verifiability (IV.2) is provided. As the voter can check that the prepared ballot contains the correct vote, inner individual verifiability of the uncast ballot is provided (IV.1 (uncast)).[4] A failure of this check can be claimed (CO.1) as the according verification program is public. Note that this check can be performed by anyone, thus providing universal verifiability of correct ballot preparation. If the value published does not match the receipt which the voter obtained, the voter can claim this by showing the confirmation email. However, as this email is not signed by any election authority, it does not prove anything. Thus, no chance of objection is given (no CO.2).

The levels of verifiability provided by Helios 1.0 are summarized in the second row of Table 6.1.

Table 6.1.: Levels of privacy and verifiability provided by Helios 1.0

privacy	UL.1b, no A.1, no A.2, no UL.1a, no UL.2a
verifiability	AV.1, EV.1, QV.1, IV.1 (uncast), IV.2, CO.1, no CO.2
Ia	no additional power
Ib + Ic	no additional power
Ic	no additional power
Id	IV.2, but no CO.2 → voter excluded
Ie	IV.2, but no CO.2 → voter excluded
If	IV.2, but no CO.2 → voter excluded
IIa	no UL.1b → no UL.1
IIb	no UL.1b → no UL.1
IIc	no UL.1, voter excluded
IId	eligibility compromised, detected by EV.1
IIe	voter impersonated (i.e. excluded)
IIIa	eligibility compromised; no UL.2, no UL.1b → no UL.1

[3] We assume that publishing a voters' register which contains voter names is sufficient to establish unconditional eligibility and uniqueness as listing ineligible voters would be noticed with high probability.

[4] In the following, inner individual verifiability referring to ballots which are not cast is denoted by IV.1 (uncast), see Section 4.4.2.

Privacy and verifiability in the presence of an adversary

Now we consider how the different adversary capabilities introduced in Section 5.2 can be employed to establish either undesired linkability, i.e. a loss of privacy, or undesired unlinkability, i.e. a loss of verifiability. We also state whether the attacks can be detected and claimed by the voter.

Capabilities concerning existing communication channels. There is only one existing communication channel, namely between the voter and the Helios server. The ability to detect channel usage (Ia) does not add any power to the adversary as the fact which voter cast a vote is public knowledge anyway. If the adversary can eavesdrop on the communication channel from the voter to the Helios server (Ic) and, at the same time, determine the sender of a message (Ib), he can link the voter and his ballot (no UL.1a). This, however, does not add any power to the adversary as this link is public. Unlinkability of ballot and vote (UL.1b) is provided in this scenario as the randomness used for encrypting the vote never leaves the voting terminal.

The adversary can use capability Id to block the channel from the voter to the Helios server and, thus, prevent this voter's ballot from being listed in the set of received ballots. The voter can recognize this (IV.2), but cannot claim it (no CO.2): the confirmation email sent to the voter upon vote casting is not signed and, thus, does not constitute a valid receipt which could be used to prove the fraud. Also, if the adversary is blocking the channel between the voter and the Helios server, the voter will will most likely not obtain this email. Thus, the voter is excluded from the election.

If the adversary can inject messages into the communication channel from the voter to the Helios server (Ie) before this voter has cast his vote, he can inject his own ballot, thus excluding that voter from the election. As already noted, the voter recognizes this (IV.2), but has no means to claim this due to the unsigned confirmation email (no CO.2). As multiple voting is not provided, the voter cannot escape this attack by just recasting his vote.

An adversary equipped with capability If is able to modify ballots that are being sent to the Helios server. Such attacks can be detected by the voter due to IV.2; however, they cannot be reported (no CO.2) due to the deficient receipt. Here as well, the voter cannot recast his vote as multiple voting is not provided.

Capabilities concerning new communication channels. If the voter gives away his ballot information (for example by using the "Coerce Me!" button provided for voter education [Adi08], adversary capability IIa), the adversary can link ballot and vote (no UL.1b). As the link between voter and ballot is public (no UL.1a), voter and vote can be linked (no UL.1).

If the election server leaks the private decryption key (IIb), ballot and vote can be linked (no UL.1b), which again implies that voter and vote can be linked (no UL.1).

An adversary with capability IIc can provide the voter with a predetermined ballot to be cast, thus linking voter and vote (no UL.1) and excluding the voter from the election.

If equipped with capability IId, the adversary can force the Helios server to add his name to the voter list in registration phase and thus compromise eligibility. However, listing ineligible voters is noticed with high probability due to EV.1.

If the adversary tries to post unauthorized votes to the bulletin board (scenario IIe), he either has to ensure that his name has been entered in the list of eligible voters (see IId), or he has to use the name of an authorized voter who is abstaining. While in [Adi08] it is claimed that impersonating abstaining voters is detected by means of individual verifiability, we argue that it is not realistic to assume that an abstaining voter will audit the bulletin board to see whether someone tried to impersonate him.

Cryptographic capabilities. An adversary who is able to break the encryption scheme (IIIa) can link each ballot to the contained vote (no UL.1b). As the encrypted vote is posted next to the voter name on the bulletin board, the adversary can thus link each voter to his vote (no UL.1). The link is provable as anyone can verify the decryption (no UL.2b implies no UL.2 due to no UL.2a).

An adversary able to break the signature scheme used for signing the voter's registration data (IIIa) can issue fake registration material to voters. Any voter affected by this attack will have his vote refused by the election server in voting phase. Upon showing the signed receipt, however, the voter is probably granted access to the voting system, even though he may not be eligible. Thus, eligibility is compromised in this case.

The levels of privacy and verifiability provided by Helios 1.0 depending on the different adversary capabilities are summarized in Table 6.1. In this table, each row shows which levels of privacy or verifiability are (not) provided depending on the adversary capabilities assumed. If several attacks are feasible, these have been unified in the table.

6.2. Helios 2.0

6.2.1. Description

Helios 2.0 was used in the 2009 presidential election at the Université catholique de Louvain (UCL) in Belgium [AdMPQ09]. It differs from Helios 1.0 mainly by providing modular authentication based on existing UCL credentials, publishing voter aliases instead of voter names, using homomorphic encryption instead of a mixnet for anonymizing the votes, and employing a distributed tallying authority. Table 6.2 shows the main differences between Helios 1.0 and 2.0.

Helios 2.0 comprises an election server, a registration authority and a distributed tallying authority. Like for Helios 1.0, a public bulletin board is used, which is

Table 6.2.: Main differences between Helios 1.0 and 2.0

	Helios 1.0	Helios 2.0
voter authentication	user name + password	credentials
ballot posted next to	voter name	voter alias
anonymization of votes	mixnet	homomorphic encryption
tallying authority	centralized	distributed

assumed to be part of the election server in the following. The ballot is composed of an encryption of a yes/no vote for each candidate and a zero-knowledge proof of the validity of the contained plaintexts (see Section 2.2.3). In registration phase, voters use their UCL credentials to register and obtain their alias[5] and the election-specific password in a pdf file signed by the registration authority. Ballot preparation is separated from ballot casting; both are carried out as for Helios 1.0, with one difference: multiple voting is allowed. Verification programs provided by third parties can be used by the voters to verify the proper encryption of their ballot. Each voter obtains a receipt on having voted, i.e. an email which is signed by the election server and contains the hash of his encrypted vote. This receipt is also posted to the bulletin board next to the voter alias. Tallying the votes[6] comprises verifying the zero-knowledge proofs included in each ballot and jointly decrypting the encrypted sum of the votes. The votes are tallied offline. Each teller publishes his decryption share and a zero-knowledge proof of correct decryption.

6.2.2. Analysis

Basic level of privacy and verifiability

The hashed encrypted vote is published next to a voter alias on the bulletin board. A list containing the encrypted vote associated to each voter alias can also be downloaded for audit. This establishes a link between voter alias and ballot. The link between the voter alias and the voter name is only known to the registration authority (and, of course, to the voter). If the adversary is restricted to public information, Helios 2.0 thus provides undecidable voter abstention (A.1), unlinkability of voter and ballot (UL.1a), and unlinkability of ballot and vote (UL.1b) (see the first row of Table 6.3). This implies that A.2, UL.1b and UL.2b are provided as well (see Section 4.3).

Since the decryption shares held by the tellers are published together with a zero-knowledge proof of correct decryption, the correct processing of the cast votes is

[5] For the UCL election, this was the letters "ER" followed by six digits.

[6] In the UCL election, a sophisticated vote weighting according to the voter category was carried out before tallying. We do not consider this as it is not relevant to our analysis. For details refer to [AdMPQ09].

continuously verifiable by the public (AV.1). Helios 2.0 publishes a voters' register containing the aliases of all eligible voters. Hence, anyone can check that ballots were cast only under aliases listed in the voters' register. Eligibility is thus verifiable under the assumption that the registration authority did not issue voter aliases to persons not authorized to vote (EV.2), and uniqueness is verifiable under the assumption that the registration authority did not issue multiple aliases to single voters (QV.2).

Helios 2.0 allows the voter to verify that his hashed encrypted vote is published next to his alias on the bulletin board and thus provides outer individual verifiability (IV.2). As the voter can check that the prepared ballot contains the correct vote, inner individual verifiability of the uncast ballot is provided (IV.1 (uncast)). Due to the verification programs provided by independent third parties, a failed check on ballot preparation can be publicly claimed (CO.1). If the value published does not match the receipt which the voter obtained, the voter can claim this by showing the receipt which was signed by the election authority (CO.2). However, if the adversary manages to seize the receipt which the voter needs to prove a fraud (either by corrupting the registration authority, scenario IIb, or by blocking the communication channels, scenario Id), the chance of objection is lost.

The levels of verifiability provided by Helios 2.0 are summarized in the second row of Table 6.3.

Privacy and verifiability in the presence of an adversary

Now we consider how the different adversary capabilities introduced in Section 5.2 can be employed to establish either undesired linkability, i.e. a loss of privacy, or undesired unlinkability, i.e. a loss of verifiability. We also state whether the attacks can be detected and claimed by the voter.

Capabilities concerning existing communication channels. The following communication channels do exist:

1. between the registration authority and the voter, and
2. between the voter and the election server.

The communication channel from the tellers to the election server is not considered as tallying happens offline (the tellers only publish their decryption shares, and robustness is achieved by having backups of the keys).

First we consider the communication channel from the registration authority to the voter. This channel is used to provide the voter with his voting credentials (i.e. voter alias and password). By detecting channel usage (Ia) and identifying the sender of the registration request (Ib), the adversary knows that a certain voter registered for the election, but does not learn his alias. However, this does not mean that this voter will also cast a vote and, thus, does not affect privacy. Identifying the sender of the registration request (Ib) and eavesdropping on this channel when the alias is sent (Ic) provides the link between a voter and his alias. Thus, upon visiting the

Table 6.3.: Levels of privacy and verifiability provided by Helios 2.0

privacy	(A.1, UL.1a, UL.1b) → (A.2, UL.2a, UL.2b)
verifiability	AV.1, EV.2, QV.2, IV.1 (uncast), IV.2, CO.1, CO.2
Ia	no additional power
Ia + Ib	A.2, no A.1
Ib + Ic	A.2, UL.2a, no A.1, no UL.1a
Id	IV.2, no CO.2 → voter excluded
Ie	salvageable due to multiple voting
If	IV.2, CO.2
IIa	A.2, UL.2a, no A.1, no UL.2b, no UL.1a, no UL.1b → no UL.1
IIb	
reg. auth.	A.2, UL.2a, no A.1, no UL.1a
reg. + tall. auth.	A.2, UL.2a, no A.1, no UL.2b, no UL.1a, no UL.1b → no UL.1
IIc	no UL.1, voter excluded
IIe + Ic	IV.2, CO.2
IIe + IIb	voter impersonated (i.e. excluded)
IIe + IId	eligibility compromised, no voter harmed
IIIa	no UL.1b, no UL.2b

bulletin board at the end of the voting phase, voter abstention is decidable (no A.1), yet not provable (A.2). Also, the adversary learns the link between the voter and his ballot (no UL.1a), although he cannot prove it (UL.2a). The adversary can use capability Id to block the channel between the registration authority and the voter. This prevents the affected voter from obtaining his credentials and, thus, from voting. He cannot claim this as the signed confirmation email is sent over the same, blocked channel. Injecting messages into this channel (Ie) in order to supply the voter with fake credentials requires the signature of the registration authority and, thus, does not help the adversary unless the registration authority is corrupted. However, the adversary could send an unsigned pdf file to the voter and hope that the voter will not realize that the signature of the registration authority is missing. This could, in effect, exclude the voter from the election as he would cast his ballot using invalid credentials. Modifying valid credentials that are being sent over the affected channel (If) does not help the adversary as this attack is recognized by the voter due to the signature provided.

Now we consider the communication channel between the voter and the election server. This channel is used by the voter to cast a ballot under his alias. If the adversary detects channel usage and identifies the sender (Ia and Ib), he knows that this voter participated in the election. Thus, voter abstention is decidable, yet not provable (A.2, no A.1). If the adversary is able to eavesdrop on this channel (Ic) and additionally can identify the sender (Ib), he can link the voter to his alias. As the link between the alias and the ballot is public, this establishes a link between the voter and his ballot (no UL.1a). Still, if no party is corrupt, unlinkability of voter and vote is provided (due to UL.1b) as the randomness used for encrypting the vote never leaves the voting terminal. Blocking this channel (Id) prevents the ballot from being received by the election server. The voter recognizes this attack by visiting the bulletin board (IV.2). However, as the adversary is blocking the channel between the voter and the election server, the voter will most likely not obtain the receipt on having voted and, thus, cannot object (no CO.2).

The adversary can use capability Ie to inject a ballot into the channel between voter and election server. If this happens after the voter cast a ballot, the voter can object by showing his signed receipt on the original ballot. If this happens before the voter cast a ballot, the voter can complain by pointing out that he did not receive a receipt on this ballot.[7] In any case, he can recast his vote as multiple voting is allowed. If the adversary can only modify ballots that are being sent to the bulletin board (If), the voter recognizes this (IV.2) and is able to complain by showing his receipt (CO.2).

Capabilities concerning new communication channels. If the voter (IIa) or the registration authority (IIb) reveals the link between voter alias and voter name, then voter abstention is decidable (no A.1) and voter and ballot can be linked (no UL.1a),

[7] It is questionable whether such a complaint would be successful as the confirmation emails are supposed to provide a positive proof, not a negative one (by their absence).

although both is not provable (A.2, UL.2a). If, additionally, the voter reveals the randomness used for encryption (IIa), ballot and vote can be linked (no UL.1b, which implies no UL.1 due to no UL.1a). The link is provable as it can be verified using the information that has been published on the bulletin board (no UL.2b). If both registration and tallying authority are corrupt (scenario IIb for all authorities), voter and vote can be linked (no UL.1): the registration authority leaks the link between voter name and alias, which makes voter abstention decidable (no A.1) and establishes a link between voter and ballot (no UL.1a), and the tallying authority leaks the private decryption key, which establishes a link between ballot and vote (no UL.1b). Only the link between ballot and vote is provable as it can be verified using the public information provided (no UL.2b). Note that, for the tallying authority to be corrupt, it suffices if enough tellers are corrupt.

An adversary with capability IIc can provide the voter with a predetermined ballot to be cast, thus linking voter and vote (no UL.1) and excluding the voter from the election. If the adversary tries to post unauthorized ballots to the bulletin board (scenario IIe), he has to use a valid alias. There are two possibilities to accomplish this:

1. cooperate with a corrupt registration authority, or
2. use the alias of an abstaining voter.

If the adversary cooperates with a corrupt registration authority, he can either obtain an alias from it (scenario IIb) or provide the registration authority with an alias which is to be validated (scenario IId). If the registration authority provides the adversary with an alias of an existing voter, then this voter is excluded from the election; in case the alias does not belong to any other voter, then no voter is harmed. To use the alias of an abstaining voter, the adversary must either corrupt the registration authority in order to obtain the alias (which refers to IIb) or eavesdrop on the communication channel from the registration authority to the voter (Ic). Using the alias of an abstaining voter is detected by this voter if he visits the bulletin board (IV.2); however, this is not a realistic assumption as already noted in Section 6.1.2. The voter can claim that his vote was stolen as the signed hash of the encrypted vote is missing on the bulletin board (CO.2). However, this chance of objection is lost if a corrupt election server has signed the hash of the adversary's ballot (IIb).

Cryptographic capabilities. As the link between the voter alias and the voter name is only known to the registration authority (and to the voter), unlinkability of voter and vote holds even if the encryption scheme is broken. In that case, only the link between the ballot and the vote is provably revealed (no UL.1b, no UL.2b).

The levels of privacy and verifiability provided by Helios 2.0 depending on the different adversary capabilities are summarized in Table 6.3. In this table, each row shows which levels of privacy or verifiability are (not) provided depending on the adversary capabilities assumed. If several attacks are feasible, these have been unified in the table.

6.3. Prêt à Voter

6.3.1. Description

Prêt à Voter [CRS05] is an electronic voting system that uses paper ballot forms which are scanned. The voter retains part of the ballot as his encrypted receipt. The scheme was originally developed by Ryan [Rya05] and since then extended many times [CRS05, RS06b, LR08, Rya08]. For our analysis we refer to the version [CRS05] which uses decryption mixnets.

The participants are voters, a vote scanning device (VSD), an election authority, and k tellers.[8] Prior to the election, the election authority generates[9] a large number of ballot forms consisting of two columns: while the left column contains a candidate list determined by a cyclic offset from the base candidate ordering, the right column holds a random value at the bottom, the *onion*, which cryptographically buries the information necessary for reconstructing the candidate ordering on the left column.

Prêt à Voter allows for pre-election auditing by revealing the construction of selected ballot forms. Thus, anyone can compute the onion as well as the offset for the candidate ordering and thereby verify that the ballot form was prepared correctly. Each voter can also cast a dummy vote for a specific candidate. The ballot is thereupon decrypted by the tellers, and the voter can verify that the decrypted vote matches the one he intended to cast.

To cast the actual vote, the voter registers at the polling station and randomly selects a ballot form. In the polling booth the voter marks the ballot with an X in the right column next to the selected candidate (see Figure 6.1), removes the left column showing the candidate ordering and shreds it. The right column is fed into the VSD and subsequently retained by the voter as a receipt. Note that the VSD does not learn the voter's decision.

Once the election has closed, the VSD transmits the ballots to the bulletin board. Each teller performs an anonymizing mix and decryption by subsequently operating on the onions. Proper mixing is verifiable by randomized partial checking [JJR02].

6.3.2. Analysis

Basic level of privacy and verifiability

The voter casts his vote in a voting booth which establishes an untappable channel between the voter and the VSD [XS06]. We assume that the adversary cannot enter the voting booth, although he may be physically present at the polling station. Thus, the adversary can spot which voter cast a vote, i.e. voter abstention is decidable (no A.1). Still, he cannot prove this to anyone who is not present, which gives us unprovable abstention (A.2). The ballots which are input to the voting system do not contain any personal information of the voter (UL.1a). Also, individual ballots

[8] In terms of our model, EA_1 is the election authority and EA_2, ..., EA_{k+1} are the tellers.

[9] There have to be significantly more ballot forms than the amount of eligible voters due to the audit process which will be described later.

candidate B	
candidate C	
candidate D	X
candidate A	
	hfY92w7k

Figure 6.1.: Marked ballot form in Prêt à Voter

cannot be linked to the contained votes (UL.1b) due to the mixing. If restricted to public information, Prêt à Voter thus provides unlinkability of voter and ballot (UL.1a) and unlinkability of ballot and vote (UL.1b) (see the first row of Table 6.4).

The correct processing of the ballots in the tallying phase can be publicly verified by randomized partial checking [JJR02]. This establishes (probabilistic) linkability of the set of received ballots and the set of all votes (AV.1). Eligibility and uniqueness verifiability are not provided as no voters' register is published and the voters are not associated with the ballots cast (no EV, no QV). The election officials checking voter eligibility and uniqueness at the polling station must be fully trusted not to authorize ineligible persons for voting.

The voter can visit the bulletin board to check that his receipt is correctly posted and hence correctly entered into the tallying process. This establishes linkability of voter and ballot, i.e. outer individual verifiability (IV.2). If the value published does not match the receipt which the voter obtained, the voter can claim this by showing the receipt (CO.2). However, the voter does not obtain any proof that the random onion belongs to the candidate order in the left column and will, thus, be decrypted to the vote he intended to cast. Hence, inner individual verifiability of the cast ballot is not provided.

Pre-election auditing, i.e. revealing the construction of selected ballot forms, establishes linkability of the ballot form and the candidate ordering and allows anyone to verify correct ballot preparation. Upon casting a dummy vote, the ballot is decrypted by the tellers, and the voter can verify that the decrypted vote matches the one he intended to cast (IV.1 of the uncast ballot). This establishes a link between the (dummy) ballot and the (dummy) vote and assures the voter that his actual ballot will contain the correct vote as well. As this auditing process is public, failed checks can be claimed (CO.1).

The levels of verifiability provided by Prêt à Voter are summarized in the second row of Table 6.4.

Table 6.4.: Levels of privacy and verifiability provided by Prêt à Voter

privacy	A.2, UL.1a, UL.1b, no A.1
verifiability	AV.1, IV.1 (uncast), IV.2, CO.1, CO.2, no EV, no QV
Ia	no additional power
Ib	no additional power
Ic	UL.2a, no UL.1a
Id	IV.2, CO.2
Id + IIa	IV.2, no CO.2 → voter excluded
Id + Ie	eligibility compromised, no voter harmed
If	IV.2, CO.2
If + IIa	IV.2, no CO.2 → voter excluded
IIa	UL.2a, no UL.1a
IIb	no UL.1b, no UL.2b
IIa + IIb + IIc	UL.2a, no UL.1a, no UL.1b → no UL.1
IId	no UL.1b, no UL.2b
IIe	eligibility compromised, no voter harmed
IIIa	no UL.1b, no UL.2b

Privacy and verifiability in the presence of an adversary

Now we consider how the different adversary capabilities introduced in Section 5.2 can be employed to establish either undesired linkability, i.e. a loss of privacy, or undesired unlinkability, i.e. a loss of verifiability. We also state whether the attacks can be detected and claimed by the voter.

Capabilities concerning existing communication channels. The only function of the VSD is to transmit the information on the ballot to the bulletin board. We consider this to be done by the voter directly. Thus, in our model, voter and VSD are equal. Also, there is no remote communication between the voter and any of the election authorities as voter authentication is established at the polling station. Thus, we have two existing communication channels:

1. from the voter to the bulletin board, and
2. from the tellers to the bulletin board.[10]

First, we consider the communication channel from the voter to the bulletin board. Capabilities Ia and Ib do not add any power to the adversary as he can be present at the polling station anyway, thus knowing which voter cast a vote. Using capability Ic, the adversary learns the link between the voter and his ballot (no UL.1a). However, he cannot prove this link to anyone (UL.2a).

Blocking the channel from the voter to the bulletin board (Id) is detected as the voter can check the bulletin board for his vote and additionally show his receipt to prove that he cast a vote (CO.2). However, this possibility of recovery is lost if the voter gives away his receipt (IIa). Equipped with capability Ie, the adversary is able to inject ballots that are posted to the bulletin board. Due to the anonymity provided by the voting booth, cast ballots are not associated with the voters who cast them. Thus, no valid vote is lost if an adversary injects ballots. This attack compromises eligibility, but can be detected if the number of participating voters is compared to the total number of received ballots. However, this comparison does not help if the adversary can block the channel at the same time (Id), thus suppressing as many cast ballots as he injected.

An adversary with capability If is able to modify ballots sent to the bulletin board. As for Id, such attacks can be detected by the voter and reported (CO.2) unless he gives away his receipt (IIa).

Now we consider the communication channel from the tellers to the bulletin board. Capabilities Ia and Ib are not relevant as the adversary is supposed to know who the tellers are (public information). Similarly, Ic does not add any power to the adversary as the messages sent are published anyway.

Blocking the channels (Id) is detected (CO.2) due to missing ballots as long as the adversary cannot inject messages (Ie) and vice versa. Modifications to the ballots

[10] The election authority generating the ballot forms does not access the bulletin board and is therefore not considered here.

that are being tallied (If) are detected with high probability due to randomized partial checking (AV.1).

Capabilities concerning new communication channels. If the adversary obtains a receipt from the voter (IIa), he can establish a link between the voter and his ballot (no UL.1a). This link is not provable (UL.2a) unless the third party which wants to obtain the proof can spot which voter gave his receipt to the adversary.

Using capability IIb, the link between the ballot and the vote can be established (no UL.1b): either the election authority reveals the association between the candidate ordering and the onion for each ballot, or each teller reveals his private key. The link between ballot and vote is provable in this case (no UL.2b) as the published data can be used to verify the values revealed.

Equipped with capability IIc, the adversary can furnish the voter with a marked ballot before he enters the polling station (provided that the adversary managed to get a ballot form, for example from the election authority who generated them, IIb) and coerce him to hand back a new, unmarked ballot (IIa), thus proving that he cast the ballot provided by the adversary. As the unmarked ballot can thereupon be used in like manner by the adversary, this attack is referred to as "chain voting" [RP05]. Voter and ballot can be linked in this case as well as voter and vote (no UL.1a, no UL.1b). Still, the link is not provable (UL.2a) unless the third party which wants to obtain the proof knows which voter was coerced.

If the adversary can send messages to an election authority (IId) prior to the election, he can furnish EA_1 with the secret values needed for generating each of the ballot forms. Thus, the adversary knows the link between each ballot and each vote, i.e. unlinkability of voter and ballot (UL.1b) is lost. The link between ballot and vote is provable in this case (no UL.2b) as the published data can be used to verify that the predetermined values have been used for generating the ballot forms.

If equipped with capability IIe, the adversary can compromise eligibility by sending ballots to the bulletin board as for Ie. The difference between injecting a ballot in the existing communication channel from voter to bulletin board (Ie) and creating a new channel to the bulletin board (IIe) is that in the latter case, the injected ballot is not associated with a specific voter. However, as Prêt à Voter does not associate cast ballots with the voters who cast them, capability IIe is already implied by Ie.

Cryptographic capabilities. If the adversary can break the pre-image resistance of the hash function (IIIa), he can trace back votes through the mixnet as follows:[11] based on the position of the chosen candidate in step i, the adversary guesses the position in step $i + 1$, computes the offset for step $i + 1$ and verifies the guess by computing the onion for that step. This establishes a link between ballot and vote (no UL.1b). The link is provable as anyone can verify it using the data published on the bulletin board (no UL.2b).

[11] Note that the mixnet is traversed from step $2k$ to step 0, using two key pairs per teller due to randomized partial checking.

If the adversary can break the encryption scheme (IIIa), the ballot transformation is revealed and the adversary learns the link between each ballot and the corresponding vote. Thus, unlinkability of ballot and vote is lost (no UL.1b), and the link is provable as it can be verified on the basis of the public information provided (no UL.2b).

The levels of privacy and verifiability provided by Prêt à Voter with respect to different adversary capabilities are summarized in Table 6.4. In this table, each row shows which levels of privacy or verifiability are (not) provided depending on the adversary capabilities assumed. If several attacks are feasible, these have been unified in the table.

6.4. Discussion

So far, this chapter has shown how our taxonomy for privacy and verifiability in voting can be used to analyze the security of voting schemes. To conclude the application of our taxonomy, we summarize and elaborate on the results and consider differences as well as similarities between the protocols under analysis.

Applying the taxonomy. We have seen how the taxonomy provides a unified approach to assess the security of voting schemes. Thus, different voting schemes can be compared in an intuitive, informal, yet precise way. By revealing the strengths and weaknesses of the respective scheme, its suitability for election scenarios with different priorities becomes apparent. If a specific adversary model has been determined for an election that is to be carried out, the assumptions made by the relevant protocols are to be compared with this adversary model in order to reveal incompatibilities. For example, a protocol assuming a trusted registration authority cannot be used in an election scenario for which an adversary capable of corrupting all election authorities is assumed.

Comparing the protocols. Our analysis shows that, although Helios 1.0 and 2.0 are similar voting schemes (for example, both use the Benaloh challenge in voting phase), they provide different levels of privacy and verifiability:

1. Helios 1.0 does not provide the voter with a chance of objection (CO), while Helios 2.0 does so by means of the signed confirmation emails.

2. Helios 1.0 provides eligibility and uniqueness verifiability without the need for trust (EV.1, QV.1), while for Helios 2.0, the registration authority must be trusted (EV.2, QV.2).

The first difference demonstrates that any receipt the voter is provided with is useless if its probative value is insufficient (for example an unsigned email or ordinary paper used for paper audit trail). The second difference originates in the fact that

Helios 1.0 publishes a voters' register with voter names, while Helios 2.0 uses voter aliases. Enhanced eligibility and uniqueness verifiability, however, come at a price: publishing the ballots next to the voter names provides a link between voter and ballot (no UL.1a). Thus, privacy is compromised if the link between the ballot and the vote is revealed, for example by cryptanalysis. The use of voter aliases provides a second layer of security here (cf. [AdMPQ09]), but impairs eligibility verifiability at the same time: it cannot be publicly verified whether each alias corresponds to an eligible voter. Thus, the use of voter aliases is preferable if the priority is set on undecidable voter abstention and unlinkability of voter and vote, whereas using voter names on the bulletin board enhances eligibility and uniqueness verifiability. Viewed more generally, this also shows that there is a trade-off between undecidable voter abstention and verifying eligibility and uniqueness.

Although the tallying phase is quite different for Helios 1.0 and 2.0, both protocols provide proofs on its correct implementation and, thus, both offer continuous accuracy verifiability. The level of individual verifiability is the same for both Helios 1.0 and 2.0 as the same mechanisms are used to establish it (Benaloh cast-or-audit protocol [Ben07] for inner individual verifiability; and publishing the ballot on the bulletin board next to the voter name or alias for outer individual verifiability).

Assessing the adversary capabilities. We now reconsider the types of attacks enabled by the different adversary capabilities in light of the results gained from the voting schemes analyzed hitherto. In general, the capabilities of category I are not fatal. Passive attacks of this category (Ia-c) either do not add any power to the adversary at all, or help to establish a link between voter and ballot (no UL.1a) which, though, is not provable (UL.2a). Active attacks of this category (Id-f) aim at suppressing (Id), adding (Ie) or modifying ballots (If). As already noted in Section 5.4, adding ballots is an attack on eligibility. Modifying ballots can usually be countered by the voter showing his receipt (CO.2), which emphasizes the importance of providing the voter with a fair chance of objection. However, blocking the channel between the voter and the election server nullifies this advantage as the receipt is suppressed as well. Here, a significant advantage of Prêt à Voter (and, basically, any poll-site voting scheme providing paper receipts) becomes evident: blocking a remote communication channel cannot prevent the voter from obtaining his receipt.

The capabilities of categories II and III are much more severe for two reasons: they can be used to (provably) reveal the link between the ballot and the vote, thus establishing a link between voter and vote and breaching voter privacy. Moreover, using capability IIb (corrupt election authority) or IIIa (breaking cryptography), this can be established on a massive scale, i.e. for all voters at the same time. An exception is Helios 2.0 which is, at least partly, safe against a total loss of voter privacy due to the second layer of security established by the use of voter aliases as explained above.

Reconsidering verifiability. Each of the protocols we have analyzed provides universal verifiability of correct ballot preparation: for Helios, anyone can generate ballots and verify that the ballot was created correctly. Prêt à Voter offers pre-election auditing of selected ballot forms by revealing their construction.[12] In both cases, inner individual verifiability of the uncast ballot is not limited to the voter, but rather extended to any interested party. This indicates a paradigm shift: universal verifiability (in terms of accuracy verifiability) seems to be no longer restricted to the tallying phase, but is rather already incorporated in the voting or pre-voting phase. This should be kept in mind when designing future voting systems.

Another feature is common to all the protocols under analysis: inner individual verifiability is provided only for *uncast* ballots. This approach of indirect verifiability allows the voter to be assured that his vote will be counted as intended without providing him with a receipt that could be used to prove his actual vote. While individual verifiability is still widely understood as the ability for the voter to check the correct form of his *cast* ballot rather than verifying *uncast* ballots, the indirect form provided for example by Helios or Prêt à Voter is much better suitable for reconciling verifiability and voter privacy.

[12] Note however that, to meet the level of verifiability provided by Helios, the ballot forms used for auditing Prêt à Voter have to be selected truly at random (cf. [CRS05]).

Part II.

Long-Term Verifiability: Legal Issues and Technical Implications

7. Introduction

In Part I we have, among other issues, taken a closer look at verifiability in voting. We have seen that each voter should have the possibility to check that his vote was properly taken into account, and anyone should be able to verify that all legitimately cast votes have been counted correctly. These verifications are usually thought of as being carried out *during* or *shortly after* the election. However, legal regulations apply for example to political elections, requiring the proper conduct of the election to be provable *even years after* the election was carried out. Therefore, in Part II we turn to long-term verifiability and consider the legal issues and technical implications of keeping election records beyond the tallying phase.

In this part of the thesis we do not consider voting machines since these are used in polling stations and, thus, are more close to classical paper-based voting. We rather focus on remote electronic voting as the underlying problem, i.e. which data should be retained and how this should be accomplished, is more challenging and, therefore, more interesting in this case.

Chapter overview

This chapter sets the stage for the following considerations. Section 7.1 provides background information on long-term retention of election data. Related work is presented in Section 7.2. In Section 7.3 we explain the methodology used in the following two chapters.

7.1. Background

Secure long-term retention of relevant documents is an important issue in the public (as well as the private) sector. The correct implementation of administrative processes must be verifiable and provable for years or even decades. Strict regulations are imposed here, and this applies in particular to elections as they embody democratic decision-making: relevant documents such as the ballots or the voters' register must be retained for a specific period of time in order to allow for a recount in case the election is challenged. In Germany, this holds for parliamentary elections as well as works council elections. Regarding Elections for the Federal Parliament (Bundestag), § 2 (2, 4) of the Law on the Scrutiny of Elections (Wahlprüfungsgesetz, WPrüfG[1]) specifies that any eligible voter, any Returning Officer and the President of the Bundestag may file an appeal within a term of two months after the

[1] English version available at `http://www.bundeswahlleiter.de/en/europawahlen/rechtsgrundlagen/wahlpruefungsgesetz.html`.

election day; the President of the Bundestag may file an objection even after this period has expired. Therefore, most of the election documents are retained for four years, which corresponds to the legislative period of the German Bundestag. This holds for other election types as well: election documents are usually retained for the term of office of the elected body. Overall, the legislative period of the elected body ranges from two years for associations [Ges04] to six years for elections for the governing boards of social security institutions (see § 58 (2) of the German Social Security Code IV (Sozialgesetzbuch, SGB IV)). The retention period may be extended if scrutiny procedures are pending. Thus, it should be assumed that election data must be retained for up to ten years. Such legal retention obligations apply not only to common paper-based elections, but also to their electronic equivalent. But contrary to the case of paper-based elections, general legal regulations on retention of remote electronic election data have not been issued so far, and there are no according specifications or guidelines.

In Germany, there have been several pilot applications of remote electronic voting in nationwide societies. The German Informatics Society (Gesellschaft für Informatik, GI) has been electing its executive committee over the Internet since 2004, while still retaining the option for postal voting. To this end, the GI has developed a catalog of requirements for online elections in non-governmental organizations [Ges05, GKM+06]. The German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) adopted online elections for the review boards in 2007. Both GI and DFG have adopted their own regulations for online elections which comprise also regulations on the retention of election data: the evaluation records of the election are supposed to be retained for the term of office of the elected body, i.e. two and four years, respectively [Ges04, Deu06]. The evaluation records are, however, not specified in the regulations.

At present it is common practice to implement a hybrid form of retention: relevant election data is retained electronically and, at the same time, parts of it are printed and retained as a hard copy (see for example [Rii02, Deu06]). However, proper electronic retention eliminates the need for retaining hard copies in parallel. Moreover, printing electronic data always involves a loss of information [RS06a]. Nevertheless, retaining electronic data requires a different approach than the paper-based variant—whereas secure storage of paper documents is achieved by locking them in a safe once and for all, several challenges have to be faced when retaining electronic documents over a long period of time: electronic data can easily be changed, therefore issues like integrity and authenticity must be addressed. Moreover, it is well known that the suitability of many cryptographic algorithms decreases with time. Furthermore, due to hardware and software obsolescence, difficulties in terms of readability emerge. Thus, long-term retention of electronic data truly is a long-term task. In the following chapters we will also see that a major challenge specific to the retention of election documents is to maintain voter privacy.

7.2. Related work

We consider related work to comprise

- previous work concerning long-term retention in general,
- previous work concerning long-term verifiability in electronic voting, and
- the significance of legal requirements in electronic voting.

7.2.1. Long-term retention in general

The overall aspects of preserving digital data in the long term have been treated in textbooks like [BRSS06] and [Gla07]. Secure long-term retention of electronic documents has also been addressed by many research projects and working groups. InterPARES (International Research on Permanent Authentic Records in Electronic Systems)[2] is a major international research initiative which aims at developing the knowledge necessary to provide policies, strategies and standards ensuring the longevity and authenticity of digital material. The long-term preservation of electronically signed documents has also been addressed by the European Telecommunications Standards Institute (ETSI) [ETS08, ETS06]. The Long-Term Archive and Notary Services (LTANS)[3] working group brings forward the standardization in this area by defining requirements, protocols and data structures for the secure usage of archive and notary services.

In Germany, NESTOR[4] (Network of Expertise in Long-Term Storage of Digital Resources) is a competence network concerned with long-term preservation and accessibility of digital documents. The DOMEA[5] concept (in German: "Dokumenten-Management und elektronische Archivierung") defines requirements for document management and electronic archiving in public administration. Conclusive and secure long-term retention of electronically signed documents has also been addressed by the project ArchiSig[6] and its follow-up project TransiDoc[7]. Recently, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) developed a Technical Directive [Bun09] which regulates trustworthy long-term retention for German government agencies. Based on the Evidence Record Syntax (ERS) standard [GBP07] and the results of the ArchiSig and ArchiSafe [ZLH08] projects, the Directive addresses long-term integrity and authenticity. In [8], the approach of [Bun09] has been refined and extended by also considering confidentiality and availability.

[2] http://www.interpares.org/
[3] http://www.ietf.org/html.charters/ltans-charter.html
[4] http://www.langzeitarchivierung.de/eng/index.htm
[5] http://www.verwaltung-innovativ.de/cln_110/nn_685150/DE/Organisation/domea_konzept/domea_konzept_node.html?_nnn=true
[6] http://www.archisig.de/english/index.html
[7] http://www.transidoc.de/website-transidoc/index-en.html

7.2.2. Long-term verifiability in electronic voting

Although plenty of research has been conducted into long-term preservation in general, retention and long-term verifiability in electronic voting has not been studied thoroughly yet. The importance of appropriate record keeping for secure electronic voting has already been recognized by the Council of Europe, who recommends that "any data retained after the election or referendum period shall be stored securely" [Cou05, Standard No. 75]. And furthermore,

> "the e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required" [Cou05, Standard No. 99],

which is specified as follows:

> "The information kept in the electronic ballot box must be securely saved for as long as this is necessary to permit any recount or legal challenge or for the period after the election required by the electoral process in the member state in question." [Cou05, Standard No. 163]

Concrete measures are not specified and regarded as a matter for national legislature.

The Common Criteria Protection Profile [VV08] defines a basic set of security requirements for online voting systems. Although requirements for the post-election phase are not addressed, the importance of long-term integrity and privacy has been recognized:

> "The server-sided TOE [Target of Evaluation] ensures that after the tallying including the determination of the election result, the election data, the election result and, if required, the audit records or further data are stored in a way that they are protected against manipulations. This protection is effective outside the TOE's scope of control and outside the election server. Subsequent forgeries or fraudulent manipulations are detectable." [VV08, Objective No. 161]

Thus, it is required that integrity protection remains effective even beyond the control of the voting system. But before protective measures can be considered, the question which data should be retained must first be answered. A naive approach would be to simply retain *any* data occurring during the online election. This approach falls short for several reasons:

1. The data generated during the election (on the basis of the voting protocol used) may be insufficient or inappropriate to meet legal requirements on retention of election documents. We will see in the following chapters that retention issues have to be considered already when designing and implementing an electronic voting protocol.

2. The principle of data minimization must be considered: according to §6 (1) of the EU Directive[8] 95/46/EC, personal data must only be collected for specified, explicit and legitimate purposes, and must not be excessive in relation to these purposes. Personal data is any information relating to an identified or identifiable natural person (§ 2 (a) of the EU Directive 95/46/EC). As we will see in the following chapter, personal data occurs for example in the voters' register or on the forms with supporting signatures for nominated candidates.

3. The records retained must not reveal any voter's preference. In particular, it must not be possible to compromise voter privacy by combining certain records which, though, may not be a threat to privacy individually. Therefore, the data occurring during the election must be carefully checked as to not allow conclusions to be drawn about the voter's choice at some point later.

A one-to-one mapping from the documentation of a paper-based election at the polling station to keeping records of a remote electronic election is not possible due to their differing implementation. Thus, other ways of identifying the according documents in an online election must be found, and provisions must be established to ensure their security and longevity.

7.2.3. Legal requirements

If the results of high-stakes elections shall become legally binding, legal requirements must be considered. It is commonly accepted that parliamentary elections have to be free, equal and secret. The principles of freedom and secrecy are also enshrined in the Additional Protocol to the European Convention on Human Rights [Cou03] and are thus supposed to be reflected by national electoral law of the European countries. According to [MGKQ03], the principles of universal and direct elections belong to the European electoral heritage. Together, these form the five basic principles of electoral law according to German Constitutional Law. [MGKQ03, VH04, GKM+06] have interpreted the five basic principles of electoral law in terms of online voting. In a similar way, the Council of Europe has considered legal standards for e-voting by deriving general requirements from the principles of universal, equal, free and secret suffrage [Cou05, Standards No. 1–19].

[MGKQ03] emphasizes the importance of transparency and public scrutiny: verification procedures for the tallying hardware and software are postulated, and it is claimed that the possibility of recount must be given. In Germany, a judgment of the Federal Constitutional Court emphasized the importance of both verifiability and legal compliance of electronic voting systems: in March 2009, the use of specific electronic voting machines in the 2005 Federal Elections for the German Bundestag was ruled unconstitutional [Fed09b]. The reason for this decision was that the voting machines in use failed to provide a sufficient level of verifiability. In particular, the

[8] English version available at `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995D0466:EN:HTML`.

judgment claimed that the voter must be able to verify that his vote was recorded as intended without having detailed knowledge of computer technology. Although the judgment refers to voting machines, which are not considered in the following, it still reflects the fact that law and technology go hand in hand in electronic voting, and close collaboration between computer scientists and jurists is a precondition for establishing secure and legally binding electronic elections.

7.3. Methodology

The methodology used in the following chapters is referred to as KORA ("Konkretisierung rechtlicher Anforderungen", Implementation of Legal Requirements) [HPR92]. KORA is an approved method to bridge the gap between law and technology by translating abstract legal norms into concrete technical measures, and can be used whenever a certain (existing or new) technology has to be (re)designed such that it complies with law. In a four-stage process, legal requirements are substantiated into technical implementation proposals:

1. **Legal requirements.** At the first stage, legal requirements are derived from fundamental legal norms such as constitutional law and its specifications in statute law. These legal requirements provide a starting point for the evaluation and the design of information technology (IT) systems. Usually, the legal requirements refer to the social aspects affected by the information technology under consideration, for example human communication [HPR92].

2. **Legal criteria.** In order to assess whether the considered IT system meets the legal requirements specified at stage 1, these requirements have to be broken down into legal criteria. These criteria characterize solutions which meet the legal requirements, yet they do not not refer to a concrete technical or organizational approach.

3. **Implementation requirements.** Next, technical implementation requirements are derived from the legal criteria established at stage 2. These implementation requirements abstract from the technical features of the IT system. They can refer, for example, to aspects of the system architecture or its functionality. If an existing IT system is to be redesigned using KORA, then the requirements at this stage can also be obtained by abstracting from existing technical features.

4. **Implementation proposals.** At the last stage technical implementation proposals are developed, taking into account the implementation requirements identified at stage 3. The implementation proposals refer to technical specifications or features of the IT system, and constitute measures that are to be taken from a legal point of view.

In the following we use KORA to answer both parts of our research question for Part II of this thesis (see Section 1.2):

- In Chapter 8 we use KORA to identify the records which should be retained after a remote electronic election has been carried out.
- In Chapter 9 we identify constraints to the record keeping, and use KORA to derive according protective measures.

In both cases we take German Constitutional Law and existing electoral laws to be our starting point.

8. Identifying the records to be kept

This chapter sets out to identify the documents which have to be retained after a remote electronic election on a parliamentary level has been carried out. We use the method KORA (see Section 7.3) to derive implementation proposals from legal requirements. As such requirements have not yet been specified for online elections, we take the present legal framework on conventional paper-based elections as a basis. This approach is reasonable since electronic voting should be at least as secure as conventional paper-based voting [BBG07, DSJ06]. More specifically, we run through the four stages provided for by KORA as follows:

1. **Legal requirements.** First of all, we identify the relevant legal requirements laid down in German Constitutional Law and Federal Electoral Law. To this end, we ascertain the reasons why election documents need to be retained.

2. **Legal criteria.** In order to obtain legal criteria, we take advantage of the fact that legal retention obligations for paper-based elections already exist. Therefore, we compile the retention obligations for paper-based parliamentary elections as specified by the Federal Electoral Regulations. Next, we consider the background of these obligations (i.e. the purpose of keeping each individual record), relating to the legal requirements identified at the previous stage. Since the Federal Electoral Regulations are meant to specify the Federal Electoral Law, this approach is consistent with KORA.

3. **Implementation requirements.** As the retention obligations specified by the Federal Electoral Regulations are very explicit and bound to the scenario of paper-based voting, they cannot be transferred to the scenario of online elections directly. Therefore, we abstract from the retention purposes identified at the previous stage in order to obtain general implementation requirements for keeping election records.

4. **Implementation proposals.** Finally we interpret the implementation requirements for the scenario of remote online elections and derive implementation proposals by identifying the records which shall be retained in order to meet the implementation requirements specified at stage 3.

Note that in this chapter we only address the question *which* records should at least be kept; the questions *how* this should be established and whether there are records which must *not* be retained are considered in Chapter 9. Earlier versions of this chapter have been published as [13] and [1].

Chapter overview

The structure of this chapter corresponds to the four stages provided for by KORA as specified above: in Section 8.1 we identify the legal requirements which apply to keeping records of parliamentary elections. In Section 8.2 legal criteria are derived by compiling the retention obligations laid down in current German law on conventional paper-based elections and analyzing the retention purposes in relation to the legal requirements identified in Section 8.1. In Section 8.3 we derive implementation requirements from the retention purposes identified in Section 8.2. In Section 8.4 we specify the records to be retained in order to meet the implementation requirements found in Section 8.3. Section 8.5 summarizes and discusses the results.

8.1. Legal requirements

The primary reason for retaining election records is to prepare for scrutiny proceedings: according to § 2 (2, 4) WPrüfG, any eligible voter, each Land Returning Officer, the Federal Returning Officer and the President of the Bundestag may challenge the election within a period of two months after the poll; the President of the Bundestag may challenge the election even after this period has expired (§ 2 (4) WPrüfG). Hence, the proper conduct of the election must be provable and thus conclusively documented. But what does the proper conduct of an election comprise?

First of all, the election has been conducted properly if the basic principles of electoral law have been followed (cf. Section 7.2.3). These principles are of prime importance and are thus laid down in German Constitutional Law (Grundgesetz, GG[1]) and also stated at the beginning of the German Federal Electoral Law (Bundeswahlgesetz, BWG[2]): according to § 38 GG and § 1 (1) BWG, the members of the German Bundestag are elected in universal, direct, free, equal and secret elections by the Germans who have the right to vote. In the following we explain briefly what the five basic principles of electoral law mean. Similar interpretations have been provided, for example, by Mitrou et al. [MGKQ03].

1. An election is **universal** if it is guaranteed that any eligible voter can participate and cast his vote. The right to vote may not be denied because of political, economic or social reasons [Sch90].

2. The principle of **direct** elections postulates that the voters alone determine the composition of the parliament [Sch90]. Nobody may influence the outcome of the election after the voting phase has terminated. Furthermore, a voter cannot transfer his right to vote to someone else who then votes on his behalf (§ 14 (4) BWG). However, auxiliary persons may help disabled voters (§ 33 (2) BWG).

[1]English version available at `http://www.iuscomp.org/gla/statutes/GG.htm`.
[2]English version available at `http://www.iuscomp.org/gla/statutes/BWG.htm`.

3. **Free** elections exclude the possibility that voters are influenced unlawfully by others or even coerced to vote in a particular way. This applies also to the period after the votes have been cast: any possibility to check a ballot cast by a particular voter must be excluded. Furthermore, voters must not be influenced by intermediate results of the election [Sch90].

4. All votes cast by eligible voters have **equal** influence on the election results. This principle applies also to the eligible candidates in the sense that equal opportunities for all candidates should be ensured [Sch90].

5. Finally, the principle of **secret** elections postulates that the voter's decision must be kept secret. It must not be possible to associate a vote with the voter who cast it (this is also known as voter privacy or unlinkability, cf. Chapter 4). Secrecy of the vote is a precondition for unrestricted freedom of vote [Sch90].

In addition to provable compliance with the five basic principles of electoral law, another legal requirement must be provably met: according to § 31 BWG, Federal Elections for the German Parliament must be conducted **in public**. The principle of public elections can also be derived from German Constitutional Law: according to § 20 (2) GG, "all state authority is derived from the people. It shall be exercised by the people through elections and other votes and through specific legislative, executive, and judicial bodies." As the voter confers the state authority to the elected representatives, he shall maintain confidence in his successful participation [BR09]. Thus, all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception [Fed09b]. In conventional paper-based elections taking place at polling stations, the principle of public elections is implemented by allowing the interested public to be present during the poll. This kind of physical observation is not achievable for remote electronic elections as the voting system is based on information technology and the underlying procedures are implemented by computers. Thus, compliance with the principle of public elections is a particular challenge in remote electronic voting.

So far, we have identified the following legal requirements:

The proper conduct of the election must be verifiable. This comprises verifiable compliance with the five basic principles of electoral law, i.e.

I. the principle of **universality**,

II. the principle of **directness**,

III. the principle of **freedom**,

IV. the principle of **equality**,

V. the principle of **secrecy**,

and, additionally, verifiable compliance with

VI. the principle of **public elections**.

Note the difference between investigating *how* the respective principle is complied with (i.e. which measures are taken to satisfy it) and investigating *how it can be documented that* this principle has been complied with. We attend to the second task in the following. However, both questions are related with respect to the principle of public elections: publishing selected parts of the records that are kept supports the principle of public elections by establishing transparency, and at the same time documents that this principle has been complied with.

8.2. Legal criteria

As observed in Section 8.1, the legal requirements for keeping records of parliamentary elections comprise documenting compliance with the basic principles of electoral law, and documenting compliance with (and thereby also satisfying) the principle of public elections. In order to further specify these legal requirements according to KORA, we take advantage of the fact that legal retention obligations for paper-based elections already exist. Therefore, in this section we analyze the retention obligations laid down in present German electoral law on Federal Elections. At first, in Section 8.2.1 we ascertain which documents have to be retained for which period of time. Then, in Section 8.2.2, we identify the concrete purpose of each individual retention obligation, relating to the legal requirements identified in Section 8.1. We refer to the Federal Electoral Regulations in the following, which are a specification of the Federal Electoral Law. Therefore, our analysis is consistent with KORA.

8.2.1. Retention obligations for paper-based elections

Federal Elections for the German Bundestag are held every four years. They are subject to the German Federal Electoral Law and specified by the according Federal Electoral Regulations (Bundeswahlordnung, BWO). The federal territory is subdivided into 299 constituencies, each of which comprises several polling districts. In each polling district an Electoral Board including an Electoral Officer is appointed (§ 6 BWO). Furthermore, each constituency appoints a Constituency Returning Officer (§ 3 BWO). The Land Returning Officers and the Federal Returning Officer are appointed for an indeterminate period (§ 1, § 2 BWO).

The voters' register must be closed the day before the election at the latest. Closure of the register is certified by completing annex 8 of the BWO. Polling cards may be issued to voters registered in the voters' register upon application (§ 25 (1) BWO).[3] A notice is placed in the voters' register next to the name of each voter who applied for a polling card. The polling card issued may thereafter be used for absentee voting or for voting in a different polling district of the same constituency. If the polling

[3] Until the end of 2008, voters could only apply for a polling card if they declared to be outside of their polling district on election day or unable to go to the polling station due to physical or other reasons. This was amended on December 3, 2008 (cf. Federal Law Gazette I, p. 2378). At present, the application for a polling card does not have to be substantiated.

card is used for absentee voting, the voter must sign an affidavit on the polling card, thus certifying that he has voted personally.

The Electoral Officer opens the poll by informing the members of the Electoral Board about their duty of impartiality and discretion (§ 53 (1) BWO). Before the voting phase begins, the Electoral Officer amends the voters' register by placing marks beside the name of voters who have been issued a polling card after the closure of the voters' register (§ 53 (2) BWO). Finally, the Electoral Officer checks that the ballot box is empty and locks or seals it (§ 53 (3) BWO).

According to § 72 BWO, the clerk in each polling district shall compile an election record pursuant to the model provided in annex 29 of the BWO. The election record documents the polling procedure and the determination of the election results. Furthermore, the election record contains decisions on the following issues:

- admission or exclusion of voters whose voting right was questionable (§ 56 (7) BWO)
- validity and content of questionable ballots (§ 69 (6) BWO)
- validity or legal ownership of questionable polling cards (§ 59 BWO)

The ballots and the polling cards which correspond to the latter two items are enclosed in the election record. The completed election record must be approved and signed by each member of the Electoral Board. It is handed over to the local authority of the commune immediately, whence it is forwarded to the Constituency Returning Officer (§ 72 (3, 4) BWO). All authorities in charge have to ensure that the election records including the annexes are protected against unauthorized access (§ 72 (4) BWO). Separate election records are compiled for absentee voting according to annex 31 of the BWO (§ 75 (5) BWO), and must as well be protected against unauthorized access (§ 75 (6, 7) BWO).

After the poll has been closed, the Electoral Board shall establish the election result in the polling district (§ 67 BWO). Hereafter the ballots are collected and the pile of ballots as well as the pile of received polling cards is sealed by the Electoral Officer and handed over to the local authority of the commune. Each authority in charge must protect these documents against unauthorized access (§ 73 (1, 2) BWO). The absentee voting documents are treated in like manner (§ 77 (7) BWO).

According to § 89 (1) BWO, the following documents must be retained and protected against unauthorized access:

- voters' register
- polling card register
- register of polling cards which have been declared invalid according to § 28 (8) BWO (affecting voters whose names have been canceled from the voters' register)

- register of voters that shall vote before a moving Electoral Board according to § 29 (1) BWO
- forms with supporting signatures for nominated candidates
- voter's notices which have been collected

While the voter's notices have to be discarded immediately to ensure data protection and voter privacy (§ 90 (1) BWO), all other documents listed have to be retained for at least six months after the election (§ 90 (2) BWO). If electoral scrutiny proceedings are pending, further retention may be ordered by the Federal Returning Officer (§ 90 (2) BWO). According to § 89 (2, 3) BWO, information on these documents may only be provided to official authorities and may only be used for election statistics, scrutiny procedures or in case an election fraud according to § 107 and § 108 of the German Criminal Code (Strafgesetzbuch, StGB[4]) is suspected.

All other election documents, i.e.

- ballots,
- absentee voting documents (polling cards and ballots), and
- election records

must be protected against unauthorized access (§ 73 (2), § 75 (7), § 72 (4) BWO) and may be discarded 60 days before a new German Bundestag is elected (§ 90 (3) BWO).

8.2.2. Purposes of the retention obligations

In the following we refer to the documents which have to be retained according to Section 8.2.1 and consider the specific purpose of their retention, relating to the legal requirements identified in Section 8.1. We start with the election documents which, according to § 90 (3) BWO, have to be retained for almost the whole election period and therefore are of special importance.

Each **election record** sets out that the election has been duly performed. The record documents that the members of the Electoral Board have been instructed on the proper conduct of the election and informed about their duties and responsibilities, in particular discretion and impartiality. If the Electoral Board could unduly influence the election results this would violate the principle of **equal** elections [Wil02]. Moreover, discretion of the election staff supports **freedom and secrecy** of the vote.

If any changes to the voters' register are required (for example due to belatedly issued polling cards which require an according mark to be set beside the name of the affected voters), these must be documented in the election record. While authorized

[4]English version available at `http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html`.

corrections to the voters' register during preparation phase are still possible, the voters' register must be closed before the election starts. This prevents illegal changes to the voters' register and hence may be viewed as supporting **universal** elections in the sense that no eligible voters are denied the right to vote, and no ineligible persons are permitted to vote. Any special incidents such as turning away voters in accordance with § 56 (6) BWO (for example because they are not registered in the voters' register and do not possess a polling card) must be thoroughly documented in the election record. This accounts for the fact that no eligible voter has been excluded from the election and thus supports the principle of **universal** elections.

The record also accounts for the fact that proper surroundings for vote casting have been established: the tables which are used for vote casting are supposed to be equipped with shields to protect voter privacy (§ 50 BWO) and hence support **secrecy and freedom** of the vote. The ballot box must be in a proper condition and empty before the voting phase starts, which aims at fulfilling the principle of **universal** elections in terms of excluding illegal ballots. Also, the ballot box must be locked or sealed before the voting phase begins, and it must not be opened again until the poll has been closed (§ 53 (3) BWO). This provides evidence that no ballots could have been taken out as long as the ballot box was locked or, respectively, the seal was unbroken. Obtaining intermediate results which could influence voters is thereby prevented, which supports **free** elections. Each of these provisions is confirmed by the election record.

Moreover, the election record accounts for proper vote casting: the Electoral Board must take care and also confirm in writing that the voters have been unobserved while voting and that they folded the ballot paper after having completed it. These measures clearly aim at **secret and free** elections. The poll must be closed at 6 p.m., and only voters who are in line at that time are entitled to cast their ballots. Closing the poll in due time while allowing the present voters to cast their ballots aims at ensuring that voters who were present on time are not excluded from the poll, thus supporting **universal** elections.

Furthermore, the correct evaluation of the election documents and determination of the election results can be verified on the basis of the election record: the poll, including the tallying of the votes, must be conducted in public (see also § 54 BWO).[5] This is important with respect to the principle of **public** elections. For conventional paper-based elections this condition is met by allowing anyone to be present in the polling room as long as polling is not disrupted (§ 31 BWG, § 54 BWO).

The election record also documents that ballots have been counted by two members of the Electoral Board independently. In case there are doubts about the values written down in the election record, the **ballots** allow for retallying and hence verifying the correctness of the announced election results. Ascertaining that all ballots have been counted correctly and having the ballots counted by two members of the Electoral Board independently supports **universality and equality**.

[5]Note that the poll is opened by the Electoral Officer by taking the actions as explained in Section 8.2.1 and, thus, is not limited to the period of vote casting.

The **voters' register** allows for verifying the voting rights. It is retained to make this verification possible even after the election, for example in case the election is challenged because of alleged participation of persons who were not eligible to vote. This contributes to **universal** elections in terms of ensuring that only persons who have the legal right to vote are permitted to participate in the election. According to § 14 (1) BWO, the voters' register contains the first and last name of the voter as well as his date of birth and mailing address. When a voter casts his ballot, this is acknowledged by placing a mark beside his name in the voters' register (§ 56 (4) BWO). Hence, the total of voters who have cast a ballot can be determined by these marks after the election has ended. Thus, the voters' register can be used to check that this value matches the one written down in the election record and, if required for verification, also the number of ballots cast. Note that, unless required for ascertaining voter eligibility, the Electoral Board may not announce personal data of the voter in such a way that these could be learned by anyone present (§ 56 (4) BWO).

The **polling card register** contains the names of voters who have been issued a polling card for absentee voting or for voting in a different electoral district. This register should match the voters' register in the sense that each voter who is in the polling card register should have a corresponding mark beside his name in the voters' register. This way it can be checked that a voter who has obtained a polling card could not have voted twice. Since polling cards are first and foremost used for absentee voting, this review may contribute to excluding the possibility that someone has cast a ballot in person and an absentee ballot at the same time: if multiple voting channels are provided, it must be ensured that only one vote per voter is accounted. Mutual exclusion of voting in person and absentee voting as well as checking the acknowledgments of voting provides for **equality** in terms of giving each voter equal influence on the election result. Furthermore, by comparing the **polling cards** received during the election with the **register of polling cards which have been declared invalid**, it can be verified that only valid polling cards have been used for voting. This contributes to **universal** elections in terms of ensuring that only persons who have the legal right to vote are permitted to participate in the election. In case of absentee voting, the affidavit which has to be signed by the voter to certify that the vote was cast personally aims at ensuring **free and direct** elections.

The **forms with supporting signatures for nominated candidates** testify to sufficient support for the candidates by the general public. These may be used as a justification for nomination of the candidates if challenged. At the same time, they guarantee equal opportunities for all candidates and hence support the principle of **equal** elections.

8.3. Implementation requirements

In Section 8.2 we have identified the legal criteria for keeping election records by answering the following question:

> What is the purpose of retaining this specific record, and which legal requirement is this purpose related to?

For example, one purpose of retaining the election record is to document that the physical ballot box did not contain any illegal ballot papers before the polls were opened, which supports the principle of universal elections. In order to obtain implementation proposals for remote electronic voting, we have to translate these legal criteria into implementation requirements that are independent of whether the election is implemented on paper or electronically. Therefore, the question to be answered next is:

> Which (general) implementation requirements can be derived from the legal criteria?

We identify the implementation requirements by investigating which conditions must be demonstrably satisfied and thus conclusively documented. Referring to our last example, the corresponding implementation requirement is to account for the fact that the ballot box has been empty before the voting phase started. This requirement is independent of either paper-based or electronic implemenation of the election: the ballot box could be both physical or electronic.

The implementation requirements apply to parliamentary elections in general, irrespective of whether the election is carried out electronically or in a conventional, paper-based way. What makes the difference between the two scenarios is *how* these implementation requirements are met and *which data* must be retained in order to prove that they have been met. While the latter is addressed in Section 8.4, the former issue depends on the voting system used, and is not considered in the following.

In Section 8.1 we have learned that retention of election data aims at proving the proper conduct of the election, which comprises verifiable compliance with the five basic principles of electoral law and the principle of public elections. The proper conduct has to be documented for all three phases of an election: preparation, voting, and evaluation. Therefore, we take a sequential approach in the following: we structure the implementation requirements derived from the retention purposes according to the election phase they refer to, i.e. preparation phase (Section 8.3.1), voting phase (Section 8.3.2), and evaluation phase (Section 8.3.3), and interpret the implementation requirements within the scenario of remote electronic elections.

8.3.1. Preparation phase

As shown in Section 8.2.2, documenting the correct preparation of the election amounts to proving that the following implementation requirements have been satisfied:

Prep1: Trustworthy entities

Prep1.1 The trustworthiness of the election staff has been ascertained.

Prep1.2 The trustworthiness of the voting system has been ascertained.

Prep2: Proper installation and surroundings

Prep2.1 The ballot box has been empty before the voting phase started.

Prep2.2 The voter had the chance to complete the ballot unobserved.

Prep3: Closure of the voters' register

Prep4: Justified nomination of candidates

Prep1.1 In an online election, not only the integrity and trustworthiness of the Electoral Board should be ascertained. Several people are involved in setting up and maintaining the voting system, for example software engineers and system administrators. Appropriate measures such as background and reference checking should be applied and documented, and compliance with due diligence procedures should be verified.

Prep1.2 In a conventional paper-based election, official authorities such as the Electoral Board and the Returning Officers are the only entities who handle the ballots. However, even passive components such as the ballot box or the tables in the polling station have to conform with certain specifications (cf. § 51, § 52 BWO).[6] As these components are merely passive, this amounts to installing them properly (see Prep2). By contrast, an electronic voting system is not only implemented and run by humans, but rather contains components which actively process the ballots. Therefore, checking on the trustworthiness of the election staff is not sufficient. Due performance of any component involved in receiving, processing and tallying the ballots must be ascertained. An approved way to establish this is to evaluate the voting system using, for example, the Common Criteria standard [Vol08]. An evaluation of the voting system according to a high Evaluation Assurance Level (EAL) should be mandatory for parliamentary elections.[7]

Prep2.1 In a conventional paper-based election, the Electoral Board verifies that the ballot box has been empty before the voting phase started (this can also be verified by the public), and documents this fact in the election record. In the scenario of online elections, the ballot box is electronic. As for the physical ballot box, it must be documented that its electronic equivalent has been empty before the election started—unless a voting

[6] In a paper-based election, the "voting system" consists of the tools and devices used, e.g. the ballot box.

[7] The existing Protection Profile for electronic voting systems [VV08] requires a rather low evaluation depth (EAL2+) which is not sufficient for parliamentary elections [VG08].

protocol is used which requires the ballot box to be initialized with dummy votes (see for example [ACvdG07, AR08], although these protocols have been designed for poll-site electronic voting using paper ballots, which is not considered here).

Prep2.2 In a conventional paper-based election, votes are cast in a controlled environment: voter privacy is established physically by means of the privacy shields which the tables in the polling station are equipped with, and voting in private is enforced by the Electoral Board and documented in the election record. Moreover, this can be publicly verified by being present in the polling room. In a remote electronic election, the Electoral Board has no influence on the surroundings in which voters cast their vote, thus this documentation requirement cannot be transferred directly to remote electronic elections. We take this matter up in Section 8.3.2 (Vote3).

Prep3 Like in a conventional paper-based election, it must be documented that the electronic voters' register in an online election has been closed before the voting phase started, and that it has not been modified hereafter.

Prep4 Justified nomination of candidates must be provable also in an online election. The collection of supporting signatures may still be accomplished using pen and paper. An electronic variant may be applicable in the case that electronic signatures are available to the public, for example if electronic Citizen Cards have been issued.[8]

8.3.2. Voting phase

As shown in Section 8.2.2, documentation of proper voting amounts to proving that the following implementation requirements have been met:

Vote1: Special incidents

Vote2: Different voting channels

Vote3: Secrecy of the vote

Vote3.1 The content of the ballot was protected against unauthorized inspection from the time the ballot was completed until the end of the voting phase.

Vote3.2 If the vote has been cast in an uncontrolled environment, the voter has affirmed having voted personally.

Vote4: Proper termination of the poll

Vote5: Public conduct of the poll

[8] The upcoming German Identity Card, which is to be introduced in November 2010, will support qualified electronic signatures according to the German Signature Law. For details refer to `http://www.bmi.bund.de/cln_174/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html`.

Vote1 In a conventional paper-based election, any special incidents that occurred during the poll (such as turning away ineligible voters) must be documented by the Electoral Board, and can be observed by being present in the polling room. System monitoring is an appropriate means to document any special incidents in an online election, and can also be used to document the correct execution of the voting software during the whole election, i.e. preparation, voting and tallying.

Vote2 Any voting system must provide secure procedures to exclude the possibility of having more than one vote per voter accounted, and these procedures have to be documented. If multiple voting via one or more voting channels[9] is permitted, policies are required to determine which vote is to be counted. This may be determined by a predefined priority mode of voting (e.g. voting in person with a paper ballot) or by the time the ballot was cast (i.e. the latest vote counts). This policy is to be published at least several days before the election in order to inform the voters.

Vote3.1 For paper-based elections which take place at the polling station, the Electoral Board must take care and also document in writing that polling happens unobserved, and that the votes contained in the ballot box have not been revealed as long as the voting phase has not terminated. The scenario of remote electronic voting does not allow unobserved polling to be enforced by any supervisory authority as voters complete their ballot by means of an arbitrary computer. Therefore, the voter himself must take care not to be observed when casting his vote. Concealing the content of the ballot can be established by several means, for example by encrypting the votes using a threshold encryption scheme and providing multiple talliers who jointly decrypt the encrypted votes after the voting phase has terminated (see Section 2.2.2). However, the voting platform used by the voter might be compromised by malicious software which records the vote before it is encrypted. It is obviously beyond the power of the Electoral Board to check the voter's private computer for malware. There are, however, several measures to mitigate this threat: before casting his vote, the voter should be informed on the duty to take appropriate measures in order to keep his voting client free from malware. There could as well be supervised public terminals for voters who are not sufficiently confident in securing their home computers.

Vote3.2 As the scenario of voting at home in a remote electronic election is similar to absentee voting due to the uncontrolled environment, the voter shall as well be required to electronically sign an affidavit certifying that the vote was cast personally. If electronic signatures are not available to

[9] For example, in the 2007 Estonian parliamentary elections, voters could change their electronic vote either by voting again electronically or by voting with a ballot paper (§ 44 (6) of the Riigikogu Election Act, available at `http://www.vvk.ee/public/dok/RKseadus_eng.pdf`).

the voter, he should at least be required to confirm having voted personally.

Vote4 Proper termination of the poll is a challenge for remote electronic elections: while it must not be possible for the voter to start filling out the ballot after the polls have closed, it must still be ensured that votes which are pending can enter the ballot box. This is in general referred to as the "last call problem" and discussed for example in [MHR04]. Secure procedures for intermediate storage must be provided to solve this problem, and their application has to be documented. Deadlines regarding the period between closing the polls and closing the ballot box must be determined and published. If a voter has started to fill out the ballot and the voting phase is about to end, he shall be informed about the time remaining until the ballot box is closed.

Vote5 As already noted in Section 8.1, the public conduct of an online election cannot be implemented by physical observation. Therefore, other means to establish a public poll have to be found. We elaborate on this issue in Section 8.4.

8.3.3. Evaluation phase

As shown in Section 8.2.2, documenting the correct evaluation of the election outcome amounts to proving that the following implementation requirements have been satisfied:

Eval1: Repeated, independent tallying

Eval2: Public conduct of the tally

Eval1 In a conventional paper-based election, the ballots have to be counted by two members of the Electoral Board independently. This can be publicly verified and is also documented in the election record. For remote electronic elections, requiring different members of the Electoral Board to tally the ballots does not add any significant value if the same tallying routine is used for both runs.[10] It is preferable to have third parties (for example election observers and official scrutiny authorities) perform a recount using a different tallying routine and checking whether the same result as for the original routine is obtained. If this is not possible (for example because tallying requires using secret keys that would have to be disclosed), the ballots should be recounted using a tallying routine that has been written in a different programming language than the original routine (cf. [AdMPQ09]). Due to universal verifiability (see Sections 2.1.7 and 4.4), retallying should also be open to the public. This is

[10] However, the approach of using two or more separate individuals or entities operating together (commonly referred to as "dual control") is an important method to enhance the security of an online voting system. It should be adhered to where appropriate, for example when opening the poll or tallying is initiated by the Electoral Board.

addressed below (Eval2). Note that remote electronic elections usually do not provide the possibility of a manual recount.

Eval2 Whereas the public scrutiny required for small-scale non-political elections (for example in societies) is limited [BR09], electing a parliament should offer a high level of transparency to the voters and must allow for comprehensive assessment by election observers. The tallying process should be made transparent by providing to the public a means to verify that the ballots were correctly transformed into the election result. If applicable, a certified (possibly third-party) routine should be provided to recount the votes and verify the election result. Voters could even be invited to implement their own routines for a recount, provided that the according specification is published and followed. Such an approach, however, requires a policy which states how to handle discrepancies between the official election result and the result calculated by self-made tallying routines.

8.4. Implementation proposals

Finally we give implementation proposals by determining the documents which have to be retained in order to meet the implementation requirements identified in Section 8.3. We follow the structure of Section 8.3. Here we only recommend *which* records shall be retained, the question *how* this should be established is considered in Chapter 9. We also specify whether the respective record shall be published (in order to satisfy the principle of public elections) or whether it is confidential (since it contains sensitive information). This decision is made according to the following policies:

P1 If a record retained contains personal information of voters or other persons involved, it shall be confidential. Personal information may include for example the name, address or date of birth, as well as the fact whether a voter participated in the election.

P2 If a record is retained in order to demonstrate compliance with conditions that can be publicly verified in a conventional paper-based elections, it shall be published. If possible, the public shall additionally be provided with a means to actively verify the respective condition instead of merely acknowledging the record retained.

8.4.1. Preparation phase

Prep1: Trustworthy entities

Prep1.1 Non-disclosure agreements as well as contracts requiring involved staff to provide due diligence shall be retained. These records are confidential as they contain personal information of the respective persons (P1).

Prep1.2 The evaluation report setting out that the voting system conforms to certain security requirements shall be retained. This record is public as voters can verify the according condition (i.e. conformance of components such as the ballot box or the tables in the polling station with given specifications) in conventional paper-based elections (P2).
Comments. The evaluation report has to be specified depending on the evaluation standard used. In Common Criteria, the Evaluation Technical Report, which is produced by the evaluator and submitted to an evaluation authority, documents in detail the overall verdict and its justification [CEM09]. The Certification Report summarizes the results and contains the certificate. The Certification Report is public, whereas the Evaluation Technical Report usually is confidential. For parliamentary elections, we recommend that the Evaluation Technical Report should be published as well. It must at least be open to election observers.

Prep2: Proper installation and surroundings

Prep2.1 A document certifying that the ballot box was empty before the voting phase started shall be retained. This record is public as voters can verify the according condition in conventional paper-based elections (P2).

Prep2.2 Not applicable.
Comments. As mentioned before, when allowing the voter to cast his vote from an arbitrary computer, unobserved polling cannot be enforced, nor can it be documented by any supervisory authority. The voter has to take care of this on his own account.

Prep3: Closure of the voters' register

The version of the voters' register which was used to determine voter eligibility shall be retained. This record is confidential as it contains personal information of voters (P1), compare to its equivalent in conventional paper-based elections (§ 89 (1) BWO). The number of eligible voters shall be publicly announced (cf. § 78 BWO).

Prep4: Justified nomination of candidates

The collection of supporting signatures for candidate nominations shall be retained. This record is confidential as it contains personal information of the nominated candidates and the supporting voters (P1), compare to its equivalent in conventional paper-based elections (§ 34 (4) and § 39 (3) BWO). The nominated candidates shall be publicly announced (§ 38, § 43 (1) BWO).

8.4.2. Voting phase

Vote1: Special incidents

The log files produced by the voting system shall be retained. This record is public as voters can observe special incidents that occurred during the poll in conventional paper-based elections (P2).

Vote2: Different voting channels

i. A record of all voters who have cast a vote shall be retained. This record is confidential as it contains personal information of voters (P1), compare to the amended voters' register in conventional paper-based elections (§ 56 (4) and § 89 (1) BWO). The number of participating voters shall be publicly announced (§ 78 BWO).

ii. If multiple voting channels are offered, a document providing evidence of the channel used by each voter shall be retained. This record is confidential as it contains personal information of voters (P1), compare to the polling card register in conventional paper-based elections (§ 89 (1) BWO).

Vote3: Secrecy of the vote

Vote3.1 A document setting out how the voting system ensures the secrecy of the vote from the time the ballot is completed until the end of the voting phase must be retained. This record is public as voters can verify the according condition (i.e. folded ballots and a sealed or locked ballot box) in conventional paper-based elections (P2).
Comments. This may also be established by setting out that the voting system does not allow for ballots to be opened before the voting phase has ended, for example on the basis of the evaluation report retained according to Prep1.2 (see Section 8.4.1).

Vote3.2 A declaration of having voted personally made by each voter shall be retained. If electronic signatures are available, the voter shall sign an according affidavit. This record is confidential as it contains personal information of voters (P1), compare to its equivalent (the polling cards) in conventional paper-based elections (§ 75 (7) BWO).

Vote4: Proper termination of the poll

i. A document providing evidence of the timely termination of the poll shall be retained. It may be part of the log files retained according to Vote1. This record is public as the according condition can be publicly verified in a conventional paper-based election (P2).

ii. A document providing evidence that voters have been notified about the upcoming end of the voting phase shall be retained. It may be part of the

log files retained according to Vote1. This record is public as the according condition can be publicly verified in a conventional paper-based election (P2).

Vote5: Public conduct of the poll

The log files produced by the voting system shall be retained (cf. Vote1). This record is public as voters can observe the polling procedure in conventional paper-based elections as well (P2).
Comments. The public conduct of an online election cannot be implemented by physical observation (see also Eval2, Section 8.3.3). Publishing log files is a substitute for physical observation and, thus, helps to establish a public poll. Note that source code is protected by copyright according to § 2 and § 69a of the German Copyright Act (Urheberrechtsgesetz, UrhG). Thus, if the voting system has been implemented using proprietary software, the source code shall be considered a trade secret. The source code shall, however, be open at least to election observers. If the election is challenged, the judge may also decide on an inspection of the source code within the election scrutiny proceedings.

8.4.3. Evaluation phase

Eval1: Repeated, independent tallying

A document containing the election results established on the basis of an independent recount shall be retained. This record is public as the corresponding procedure in paper-based elections (i.e. ballot counting by two members of the Electoral Board) is public as well (P2).
Comments. The recount should either be performed by a third party, or, if this is not possible (for example because of secret keys required for tallying), using a tallying routine that has been written in a different programming language than the original one (cf. [AdMPQ09]).

Eval2: Public conduct of the tally

i. The set of ballots received by the voting system shall be retained. This record is public as anyone may be present when the ballot boxes are opened and the ballots are disclosed in a conventional paper-based election (P2).

ii. A document setting out that the received ballots have been correctly processed and tallied shall be retained. This record is public as anyone may be present during tallying in a conventional paper-based election (P2).
Comments. The ballots received by the voting system are the basis for establishing the election result. Therefore, having transformed these ballots correctly into the corresponding votes shall be publicly verifiable. The according record may comprise, for example, zero-knowledge proofs of correct decryption or proofs of correct mixing (see Section 2.2.3), and it

shall be published as the tallying process cannot be physically observed. It is preferable to provide the public with a means to actively verify the tallying process or parts of it (for instance by publishing the secret key of the teller after the poll has ended, see [2]).[11] However, this depends on the voting system and may not be applicable (for example in a voting system using homomorphic encryption with distributed tellers, cf. Section 2.2.5).

iii. The number of valid and invalid votes shall be documented as well as the the election results (i.e. number of votes for the different parties and candidates). This record is public as this data is published for conventional paper-based elections as well (P2), see § 79 (1) BWO.

8.5. Summary

Legally binding remote electronic voting presupposes that the proper conduct of the election is verifiable for several years. This requires appropriate record keeping. While the retention obligations for paper-based elections are governed by electoral law, according specifications for electronic voting have not yet been issued.

We have used KORA (see Section 7.3) to derive the records to be kept for online elections from relevant legal requirements. This involved abstracting from existing retention obligations laid down in German Electoral Law in order to identify the implementation requirements that must be met to provide evidence of the proper conduct of the election. These implementation requirements were interpreted within the scenario of remote electronic voting. Finally, we have derived implementation proposals, thus recommending which records should be kept in order to meet the implementation requirements. Due to our approach, these recommendations are based upon legal obligations regarding conventional paper-based elections and, therefore, their consideration is an important step on the way toward legally binding online elections for the German Bundestag. We have also recommended which of the respective records should be published in order to satisfy the principle of public elections, and which of them should be kept confidential. An obvious way to implement our recommendations regarding publication of specific data is to post them to a public bulletin board (see Section 2.2.7).

In particular, we have seen that retaining merely data generated by the protocol (such as the ballots or proofs of correct tallying) does not suffice to meet legal retention requirements. It is necessary to keep further records, for example in order to document trustworthiness and proper installation of the voting system. In the following chapter we identify any constraints in terms of both the quantity and the quality of the data retained.

[11] Cf. the concept of constructive universal verifiability introduced in [Pie06].

9. Identifying constraints and proposing protective measures

In Section 8.1 we learned that the primary objective of retaining election data is to conclusively document the proper conduct of the election, and in the remainder of Chapter 8 we identified the records which must be kept to this end. In particular, we have seen that documenting the proper conduct of the election means documenting that the basic principles of electoral law and the principle of public elections have been complied with during each phase of the election.

Now that we have established which records should be kept as a minimum, we need to investigate whether there is also an upper limit to the records kept: the election records not only have to document that the basic principles of electoral law have been satisfied while the election was carried out; the records *themselves* also have to be consistent with these principles. Moreover, we have to ascertain whether additional relevant principles or rights could be infringed by the data retained, and whether ensuring conclusiveness of the records requires special measures to be applied.

In this chapter we therefore identify any constraints to the record keeping in terms of both the quantity and the quality of the data retained. As in Chapter 8, we start from legal requirements and use KORA (see Section 7.3) to derive appropriate implementation proposals. In particular, we investigate whether the records could infringe the basic principles of electoral law or any other fundamental constitutional rights, and analyze the way in which the record keeping should be accomplished in order to preserve the probative value of the data retained.

As already noted in Section 7.2.1, measures to protect the security and longevity of electronic records have been developed and established within several projects and working groups. These measures are mostly generic and, thus, can basically also be applied in order to securely retain electronic election data. However, merely applying these measures to any data occurring during the election is not sufficient since specific challenges posed by the scenario of electronic voting, such as maintaining voter privacy in the long term, have to be addressed.

This chapter is based on joint work with Zoi Opitz-Talidou; an earlier version has been published as [3] (in German).

Chapter overview

The structure of this chapter corresponds to the four stages provided for by KORA: In Section 9.1 we identify the legal requirements regarding secure and conclusive retention of election data. Section 9.2 translates these legal requirements into le-

gal criteria. In Section 9.3 we derive technical implementation requirements from the legal criteria identified in Section 9.2. Implementation proposals fulfilling these implementation requirements are made in Section 9.4. Section 9.5 summarizes the chapter.

9.1. Legal requirements

As already stated in Section 8.1, the primary reason for retaining election records is to prepare for scrutiny proceedings (§ 81 BWO). Recall that, according to § 2 (2, 4) WPrüfG, any eligible voter, each Land Returning Officer, the Federal Returning Officer and the President of the Bundestag may challenge the election within a period of two months after the poll; the President of the Bundestag may challenge the election even after this period has expired (§ 2 (4) WPrüfG). Evidence is collected according to § 7 (2) WPrüfG and requires measures to preserve the probative value of the records retained: they can only be used as evidence of the proper conduct of the election if they have **sufficient probative value**.

However, considering the matter of conclusiveness alone is not sufficient: the election records kept are only admissible as evidence if they do not infringe the basic principles of electoral law (cf. Section 7.2.3). In the following we therefore go through these principles and analyze whether they may be interfered with by the election records kept.

The principle of universality postulates that any eligible voter can participate in the election and thereby execute his right to vote (cf. Section 8.1). This principle relates to the quality of the access to the election provided to the voters and therefore restricts to the voting phase. The principle of universal elections is thus not affected by the election records that are kept *after* the election has been carried out.

The principle of directness postulates that the voters alone determine the election result, and that nobody may influence the outcome of the election once the polls have closed (cf. Section 8.1). However, illegal ballots could possibly be injected even after the voting phase has terminated. Still, the principle of directness is not considered to be affected by the occurrence of illegal ballots—forgeries rather affect the principle of equality as explained below [Wil02, Kar05]. The principle of direct elections merely excludes the possibility of having an electoral college determine the election result. Therefore, this principle is not affected by the election records kept.

The principle of equality requires all votes cast by eligible voters to have equal influence on the election results (cf. Section 8.1). Having ineligible voters cast illegal ballots which affect the election result is considered to infringe the principle of equality [Wil02, Kar05], and such an infringement can possibly occur even after the tallying phase has terminated and the retention period has commenced: illegal ballots could be added to the legitimately cast votes after the end of the election,

and a different election result than the one established before could be claimed. In such a case the correct election result would have to be indisputably ascertainable since otherwise the principle of equal elections would be infringed. Therefore, the election result which has been established on the basis of the legitimately cast votes must be unequivocally evident from the records kept.

The principle of freedom postulates that voters can freely express their intention and must not be influenced unlawfully by others or even coerced to vote in a particular way (cf. Section 8.1). This applies also to the period after the votes have been cast: it must not be possible to ascertain a voter's voting decision. If the voter fears that his decision becomes public in the future, his freedom of vote is limited. Thus, the principle of free elections can be infringed even after the election has been carried out, and is therefore essentially affected by the records retained.

The principle of secrecy postulates that the voter's decision must be kept secret, i.e. that it must not be possible to associate a vote with the voter who cast it (cf. Section 8.1). This principle is closely related to the principle of freedom since secrecy of the vote is a precondition for unrestricted freedom of vote [Sch90]. The secrecy of the vote has to be maintained beyond the end of the election in order to ensure unrestricted freedom of vote.[1] Thus, the principle of secret elections is as well affected by the records retained and must be considered in the following.

The principle of public elections postulates that all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception [Fed09b]. Keeping election records *supports* this principle rather than conflicting with it since publishing selected parts of the records kept helps to establish public elections (cf. Section 8.1). Recall that, with respect to retention of election data, the principle of public elections is of a different kind than the other five principles: while compliance with the five principles is *documented* by the records kept, the principle of public elections is also *satisfied* by means of the retention provisions. In order to *comply with* this principle, the records kept must be made available to the public in an appropriate way. At the same time, this means that the principle of public elections can only be *infringed* by the election records if data under retention is withheld from the public without good cause. We have already recommended which of the records should be published in order to satisfy the principle of public elections (see Section 8.4). Therefore, this principle does not have to be considered any more in the following.

In summary, we have thus figured out that the principles of secret, free and equal elections can be interfered with by the records kept. Additionally, we have to take

[1] To date there is no consensus on how long one's voting decision should be kept secret. It has been claimed that, at least for Federal Elections, the secrecy of the vote should hold forever [Wil02]; however, it may also be sufficient to maintain the secrecy of the vote for the voter's lifetime (P. Richter, personal communication).

into account the constitutional right to **informational self-determination**, which is derived from § 2 (1) GG. It postulates that everyone shall personally decide on the disclosure and use of his personal data [Fed83]. This fundamental right may only be restricted in view of public interest, and it must not be restricted further than necessary. It also encompasses protection against unlimited collection and storage of personal data. Informational self-determination can be infringed by the election records kept since they contain personal data of voters and candidates, and must therefore be taken into account.

We have thus identified the following legal requirements:

I. The **probative value** of the records providing evidence of the proper conduct of the election must be sufficient, and it must be preserved throughout the retention period.

II. The principle of **equal elections** must not be infringed, i.e. the election result established on the basis of the legitimately cast votes must be clearly and unequivocally evident from the records kept.

III. The principles of **free and secret elections** must not be infringed, i.e. the records kept must not reveal any voter's voting decision.

IV. The fundamental right to **informational self-determination** must be preserved, i.e. personal data of voters or other persons involved must be protected against unauthorized access, and must not be used for any purpose other than specified by electoral law.

The principles of free and secret elections have been considered in a single requirement since they are closely interrelated. The next step is to derive legal criteria from the legal requirements we have just identified.

9.2. Legal criteria

The following legal criteria can be derived from the legal requirements identified in the previous section:

1. First of all, the requirement of preserving the probative value of the records retained (I) requires the information contained in the records to be readable by humans. To this end, hardware to access the data as well as software to interpret and visualize it must be available and trustworthy [RFDJ07].

2. Any records must be retained in a way that ensures their tamper-resistance. This legal criterion is derived from two requirements: to preserve the probative value of the records kept (I), and to establish unequivocal evidence on the election results in order to prevent the principle of equal elections from being infringed (II). It has to be ensured that the records cannot be maliciously or accidentally altered or deleted [RFDJK07]. Thus, there must be a means

to detect whether a document has been altered or deleted, and the archiving system must provide methods to prevent undue modifications and to retrieve documents in their original condition.

3. The records retained must be authentic, and there must be ways to verify their authenticity [RFDJ07]. This criterion follows from the requirement to preserve the probative value of the records kept (I) and the requirement to establish unequivocal evidence of the election results (II). In order to allow for verification of authenticity, the issuer of a document which is part of the records retained must be ascertainable—as long as this does not affect voter privacy. Obviously, this criterion cannot be fulfilled independently of the criterion which is derived from the legal requirements of secrecy and freedom (see 5. below).

4. In order to be able to use the records as evidence in a lawsuit, they must be presentable to the court [FD06]. To this end, it must be possible to provide the records on a portable data carrier, or to transmit the records electronically. This criterion can be derived from the requirement to ensure a sufficient probative value of the records retained (I), since the probative value can only be assessed by the court if the records are presentable to the judges.

5. From the legal requirements of secrecy and freedom (III) it can be derived that any possibility to check a ballot cast by a particular voter must be excluded, which holds even *after* the election has been carried out: the records retained must not allow for establishing a link between any voter and his vote, thereby revealing the voter's voting decision.

6. From the requirement to preserve the right to informational self-determination (IV) it can be derived that data protection provisions must be adhered to if the records kept contain personal data, which holds for some of the election records (e.g. the voters' register or the collection of supporting signatures for candidate nominations, cf. Section 8.4.1, Prep3, Prep4). The data protection provisions are regulated by the Federal Data Protection Law (Bundesdatenschutzgesetz, BDSG). According to § 9 BDSG, appropriate technical and organizational measures must be taken to protect personal data. Data protection also encompasses purpose specification: while it is legitimate to store personal data within the scope of election documentation, it has to be ensured that the data retained is not used for any purpose other than specified by electoral law.

9.3. Implementation requirements

In the following we derive technical implementation requirements from the legal criteria identified in Section 9.2.

1. The first implementation requirement is to ensure the **readability** of the records retained. To this end, standardized, generally accepted and widespread data

formats should be used [BRSS06]: this increases the probability that appropriate software is available and, thus, helps to avoid later format conversion. Since election records have a retention period of up to ten years (see Section 7.1), transformations during the retention period can be prevented if appropriate data formats are used from the beginning, that is, already when implementing the voting system.

2. The second implementation requirement is to ensure the **integrity** of the records retained (cf. [VV08, Objective No. 161]). According to the corresponding legal criterion, modifications shall not only be recognized, but rather have to be prevented. Also, any compilation of interrelated documents must be preserved in its entirety, i.e. the **completeness** of relevant documents must be ascertainable [RS06a].

3. The third implementation requirement is to ascertain the **authenticity** of the records retained. While paper records can be signed by hand of their issuer and subsequently retained as such, establishing and preserving authenticity of electronic documents requires special measures. While providing for authenticity of the cast votes, voter privacy must still be ensured (see 5., implementation requirement of privacy).

4. The fourth implementation requirement is to ensure the **negotiability** of the records. The according legal criterion requires that the records can be transferred electronically or physically via a portable data storage device. To this end, protective measures to fulfill the implementation requirements should preferably apply to the record itself instead of applying via the storage medium or the archiving system (cf. [VV08, Objective No. 161]): document-related protective measures are capable of protecting the retained documents directly, irrespective of the storage medium and the archiving system which is used [RFDJ07].

5. The fifth implementation requirement is to maintain voter **privacy** beyond the end of the election. If the voting system produces separate records which, when combined, may compromise voter privacy, these records must not be retained to the extent that voter and vote can be linked. Since remote electronic voting requires electronic procedures to authenticate voters before they cast a ballot, voter authentication data has to be present in the system at some point in time. This data might be existent even beyond the end of the election and eventually can be used to ascertain the voter's voting decision *afterward*. Here we assume that the election records are stored centrally, i.e. we do not consider the possibility of storing the records in a distributed way (this is addressed for example in [8]).

6. The sixth implementation requirement is to ensure **confidentiality** of personal data. Any confidential information stored must be protected against unauthorized access. Moreover, the **purpose specification** must be adhered to—the

data retained must not be used for any purpose other than specified by electoral law: according to § 89 (2, 3) BWO, information contained in

- the voters' register
- the polling card register
- the register of polling cards which have been declared invalid according to § 28 (8) BWO (affecting voters whose names have been canceled from the voters' register)
- the register of voters that shall vote before a moving Electoral Board according to § 29 (1) BWO
- the forms with supporting signatures for nominated candidates

may only be provided to official authorities and may only be used for election statistics, scrutiny procedures or in case an election fraud according to § 107 and § 108 StGB is suspected. These specifications must be adhered to.

9.4. Implementation proposals

In the following we make implementation proposals for each of the implementation requirements listed in Section 9.3. First we explain methods appropriate to fulfill each requirement, then we make concrete recommendations for the scenario of online elections, referring to the records that have to be kept according to Section 8.4. We assume the existence of a public bulletin board (see Section 2.2.7).

1. To ensure **readability** of the records retained, standardized and persistent data formats shall be used. These are, for example, PDF/A [Intc] and XML [BPSM+08] (see also [Bun06, M 4.170]). The latter is human-readable as well as machine-readable and particularly suitable for structured data sets which need to be easy to parse in different programming languages (see Section 8.4.3, Eval1). Therefore we recommend to use XML for the record of ballots and the voters' register (cf. [Adi08]). XML signatures [ERS02] should be used to sign these records as they are tailored to XML documents and provide for strong flexibility (see 3., implementation proposals for authenticity).

Recommendations on readability

R1.1 Structured data sets such as the ballots (see Section 8.4.3, Eval2) or the voters' register (see Section 8.4.1, Prep3) should be generated and retained in XML format.

R1.2 If records retained in XML format have to be signed (see 3., implementation proposals for authenticity), XML signatures should be used.

R1.3 Self-contained documents that are not directly related to a specific election such as the agreements and contracts according to Prep1.1 (see Section 8.4.1) and the evaluation report (see Section 8.4.1, Prep1.2) should be retained in PDF/A format.

2. Qualified timestamps [HS91] are an approved method to demonstrate the **integrity** of electronic records. They can prove that a document existed in a certain form at a specific point in time and, thus, provide the possibility to recognize alterations to the document [KOV07]. However, the fact that timestamps can be used to establish the chronological order of incoming messages must not be exploited to compromise voter privacy. We take this up when making according implementation proposals for privacy (see 5.).

   Qualified timestamps are issued by a Certificate Service Provider who, according to § 2 of the Signature Law (Signaturgesetz, SigG), must conform to specific legal requirements. In order to minimize the number of qualified timestamps required, one may use Merkle's hash trees [Mer80] as standardized in [GBP07]. However, timestamps can only prove that a document has not changed since a specific point in time. Unauthorized modification can be prevented by retaining the records on non-rewritable storage media kept in a secure location. Both approaches shall be combined; additionally, redundant safekeeping increases the security and availability of the records kept.

Recommendations on integrity

R2.1 The voters' register shall be provided with a qualified timestamp before the election starts (see Section 8.4.1, Prep3). This documents conclusively the state of the voters' register in which it was referred to for checking eligibility during the polling phase. It also allows for setting marks to indicate that a voter has already cast his vote or that he has used a specific voting channel.

R2.2 The ballot box shall be provided with a qualified timestamp at the very beginning of the voting phase in order to prove that it was in a correct state then (see Section 8.4.1, Prep2.1).

R2.3 When the voting phase has ended and pending votes have been resolved (i.e. either cast or canceled), the contents of the ballot box should be provided with a qualified timestamp. This provides evidence of the timely termination of the poll (see Section 8.4.2, Vote4).

R2.4 Any of the records retained according to Section 8.4 should be kept on non-rewritable, portable storage media and stored in a secure location accessible by authorized persons only. A duplicate of each record shall be kept in like manner, but in a different place.

3. The method of choice in order to provide for **authenticity** is to use electronic signatures: an electronic signature ensures that the originator of a signed document can be identified. At the same time, signing a document can prove that it has not been modified thereafter. Thus, electronic signatures establish authenticity and demonstrate integrity. However, electronic signatures must not be used in a way which would cause voter privacy to be compromised. We will consider this when proposing according measures for maintaining privacy (see 5.).

   According to § 371a and § 437 of the German Code of Civil Procedure (Zivilprozessordnung, ZPO), authenticity of electronic documents is assumed if they are provided with a qualified electronic signature as only these have a probative value which equals those of signatures by hand. Thus, only qualified electronic signatures should be used for conclusive retention. According to § 6 (1) SigG and § 17 of the Signature Ordinance (Signaturverordnung, SigV), preserving qualified electronic signatures requires renewing them before the security suitability of the employed algorithms and parameters expires, and providing the renewed signature with a qualified timestamp. According to annex 1 Section I (2) SigV, the algorithms and parameters shall be suitable for at least six years. Moreover, the verification data must be available for the whole retention period [BPRS02]. According to § 14 (3) SigV, qualified certificates shall be valid for no more than five years from the date of issuance.

Recommendations on authenticity

R3.1 We recommend to provide the individual votes with signatures in order to prove their authenticity. However, this should not be accomplished after the end of the election, but rather be provided for by the voting protocol. Otherwise, alleged alterations during the poll cannot be disproved.[2]

Due to voter privacy, the cleartext vote must obviously not be signed by the voter himself. An approved method to achieve authenticity of the votes (and to confirm the voter's eligibility at the same time) is having the votes signed by a validating authority, see for example the voting protocols [OMA+99] or [2]. Blind signatures can be used here in order to conceal the vote from the validation authority (see Section 2.2.4). However, this depends on the voting protocol used.

R3.2 If signing the votes is not provided for, the ballots shall be signed. There are two possibilities to establish this: either the voter signs the individual ballot before he casts it, or the collection of received ballots is signed

[2] Note that an archiving system cannot make up for negligence in the preparation of documents. For example, the integrity of a document which was created without appropriate safeguards cannot be verified for the time before this document was entered into the archiving system [RFDJ07].

by an election authority.[3] The first approach presupposes that electronic signatures are available to the voters, and has been used for example in the Estonian voting system [Est05]. However, this approach has the disadvantage that upon publishing the signed ballots, voter privacy may be compromised in the long term if the encryption scheme becomes insecure. Contrary to the option of voter signatures, having an election authority sign the set of received ballots after the voting phase has terminated (see Section 8.4.3, Eval2) shall be mandatory as this provides a proof of integrity and completeness at the same time (see R3.4e).

R3.3 The evaluation report should be signed by the certification authority (see Section 8.4.1, Prep1.2).

R3.4 The following documents shall be signed by an election authority:

a) the voters' register (see Section 8.4.1, Prep3)

b) the list of nominated candidates including the supporting signatures (see Section 8.4.1, Prep4)

c) the records on participating voters and voting channels used (see Section 8.4.2, Vote2)

d) the log files of the voting system (see Section 8.4.2, Vote1 and Vote5)

e) the set of received ballots[4] (see Section 8.4.3, Eval2)

f) the documents on the correct processing and tallying of the received ballots (see Section 8.4.3, Eval2)

g) the records containing the number of valid and invalid votes and the election results (see Section 8.4.3, Eval2)

h) the results of the recount (see Section 8.4.3, Eval1)

Note that voter privacy must be respected in any case (see 5., implementation proposals for privacy).

R3.5 Timely signature renewal must be taken care of for any signatures issued along these recommendations. This applies also to any signatures issued in terms of the contracts according to Prep1.1, the forms with supporting signatures for nominated candidates according to Prep4, or the affidavits according to Vote3.2 (see Sections 8.4.1 and 8.4.2).

[3] In the following, an election authority denotes the Electoral Officer or any other authorized party provided by the respective voting scheme.

[4] We recommend having the ballots received in each polling district signed by the Electoral Officer. Additionally, the overall record containing several sets of ballots from the individual polling districts should be signed by the Constituency Returning Officer. Thus, the integrity, authenticity and completeness of the respective record can be proven. This approach can be continued by having the Land Returning Officer sign the record containing the ballots of the constituencies, and having the Federal Returning Officer sign the record containing the ballots received in the lands.

4. **Negotiability** is achieved by combining several approved measures: using widespread or standardized data formats supports negotiability since it increases the probability that the records can be accessed without any difficulty [RFDJ07] (see also the implementation proposals for readability). Keeping the records on non-rewritable, portable storage media allows the records to be collected and presented to the court (see also the implementation proposals for integrity). Document-related protective measures such as signatures and timestamps can be verified by anyone. They apply directly to the records kept, and therefore remain effective irrespective of the storage medium and the archiving system which is used [RFDJ07]. Thus, negotiability is achieved by taking appropriate measures which are used primarily to meet the other legal criteria. Therefore, we do not provide specific recommendations here.

5. **Privacy** is preserved by restricting the volume or the characteristics[5] of the records in an appropriate way. In particular, it must not be possible to compromise voter privacy by combining different records which, though, may not be a threat to privacy individually. In Chapter 4 we have learned that privacy can be established by either unlinkability of voter and ballot, or unlinkability of ballot and contained vote (see Section 4.2). It follows that, in order to establish long-term privacy, it must not be possible to reconstruct both links at the same time from the records kept (or data otherwise remaining from the election). We give an example to illustrate the issue: imagine a voting system which produces a table listing ballots alongside the names of the voters who have cast them (as is the case for the schemes proposed for instance in [AdMPQ09, JCJ05]). This table should be retained according to recommendation Eval2 i. (see Section 8.4.3). If the private key which was used to extract the votes from the ballots is retained as well (for instance due to verifiability), then anyone who is able to access the records kept may compromise voter privacy.

   Restricting access to the records (see implementation proposals for confidentiality) is not sufficient in this case: a crucial issue for maintaining privacy is protection of private keys. For example in the 2007 Estonian parliamentary elections, a core requirement for ensuring voter privacy was to prevent anyone from gaining access to both the electronically signed votes and the private key used for decrypting the encrypted votes [Est05]. Secure key management (i.e. secure generation, delivery, backup, usage, and deletion of keys, see also [Bun06, M 2.46]) is a general requirement which applies to any voting system (cf. [VV08, Objective No. 193]). We focus on the aspect which is affected by record keeping, namely secure deletion of private keys (cf. [Est05]).

   The Estonian voting system shows another feature which may affect voter privacy: in order to prevent vote-buying, it allows for multiple voting, i.e. overwriting a vote cast electronically by either a new electronic vote or a traditional

[5] Here, the characteristics are meant to refer to cryptographic attributes such as electronic signatures or timestamps.

vote on paper. This approach requires procedures to recognize a voter who has already cast an electronic vote in order to be able to cancel this vote. This is accomplished by storing the encrypted votes including the voter's signature which is later on used to identify the affected ballots. The signatures are separated from the encrypted ballots before the votes are counted. However, retaining encrypted votes which have been signed by the voters may compromise voter privacy in the long term when the encryption scheme has become insecure (cf. R3.2) and, of course, in case the private decryption key is disclosed, as stated above. Therefore, the signed encrypted votes should not be retained, but rather deleted as soon as the election result has been verified and the period for contesting the election has expired (cf. § 2 (2, 4) WPrüfG).

Finally, specific election results may allow inference on the voting decision of individual voters with absolute or extremely high certainty: imagine an election where solely one voter uses a specific voting channel (e.g. one single absentee vote). In this case, retaining the list of participating voters and voting channels used (cf. R3.4c) as well as the election result per voting channel (cf. R3.4g) would reveal that voter's voting decision. This can be prevented by either organizational (e.g. separation of duty) or technical means (e.g. encryption).

Recommendations on privacy

R5.1 After the election has terminated, authentication data referring to the identity of the voter (i.e. information used for authenticating the voter and checking eligibility, such as the voter's electronic signature, cf. R3.2) must no longer be linkable to ballot data containing the vote (e.g. in encrypted form).

R5.2 Any private keys used to extract the votes from the ballots shall be permanently deleted after the election results have been established and verified (for instance by checking proofs of correct tallying) and the two-month period for contesting the election has expired (cf. § 2 (2, 4) WPrüfG). If the private keys have previously been distributed among several trustees (secret sharing, cf. Section 2.2.2), according deletion policies must be enforced for each trustee.

R5.3 Any residual information linking the voter to his vote or allowing conclusions to be drawn about the voter's choice (for example the secret permutations used by mixnets and the randomization values used by a reencryption mixnet) must be destroyed after the vote has been cast (cf. [VV08, Objectives No. 162 and 192]). This holds also for residual information stored on the voting device which has been used to cast the vote (for example the random value used for blinding the vote in order to obtain a blind signature, cf. [OMA+99]). If deletion cannot be accomplished automatically by the voting system, the voter must be informed how to delete such traces.

R5.4 Ballots should not be provided with timestamps upon entering the electronic ballot box as conclusions regarding the chronological order of the votes cast can be drawn from this (see Section 8.4.3, Eval2; cf. [VV08, Objectives No. 162 and 192]).

R5.5 If the election result allows conclusions to be drawn about the voting decision of individual voters (with absolute or extremely high certainty), the relevant records must be kept secret. Appropriate measures are separation of duty or encryption. These measures should be applied to those records listed in R3.4 which are affected depending on the individual election scenario.

6. The requirement of **confidentiality** and **purpose specification** can be fulfilled by access control and encryption (cf. the annex to § 9 (1) BDSG). Implementing access control in the archiving system helps to achieve confidentiality during the retention period. The respective records shall be retained in such a way that any user can inspect the documents he is authorized to see. For example, the user can only access the voters' register in the role of the Electoral Board. A drawback of this approach is that access control ceases to be effective if the protected document is collected from the archive, for example because it has to be presented to the court (see also the implementation proposals for negotiability).

   To protect the confidential document directly, it can also be encrypted. In this case, the decryption key has to be retained as well and must be protected against unauthorized access. Since the retention period most probably does not exceed ten years (see Section 7.1), reencryption can be avoided if the keylength is chosen appropriately from the beginning, i.e. in such a way as to remain secure for the whole retention period. This can be established, for example, on the basis of the ECRYPT recommendations.[6] However, it should be monitored whether weaknesses of the used encryption scheme have been found in the meantime, so that the affected records can be reencrypted if required.

Recommendations on confidentiality and purpose specification

R6.1 The persons who may challenge the election according to § 2 (2) WPrüfG (i.e. the eligible voters, each Land Returning Officer, the Federal Returning Officer and the President of the Bundestag) shall have access to those retention records which are public (see policy P2, Section 8.4) for the period in which the election may be challenged by the respective person (see § 2 (4) WPrüfG). We recommend using a bulletin board to this end.

R6.2 The confidential retention records (see policy P1, Section 8.4) shall only be accessible to designated election authorities and official election ob-

[6] The ECRYPT Yearly Report on Algorithms and Key Lengths is available at `http://www.ecrypt.eu.org/ecrypt1/`.

servers. This applies to the records listed under Prep1.1, Prep3, Prep4, Vote2, Vote3.2 in Section 8.4, and can be established using either encryption or role-based access control within the archiving system.

R6.3 Anyone who has access to election records containing personal data must be informed on his duty not to use this data for any purpose other than specified by electoral law, i.e. election statistics, scrutiny procedures or in case an election fraud according to § 107 and § 108 StGB is suspected (cf. § 89 (2, 3) BWO).

9.5. Summary

This chapter considered the constraints which apply to election records kept. Starting from legal requirements and using KORA (see Section 7.3), we have derived legal criteria and, as a next step, requirements for implementing the retention of online election data. Then we proposed concrete recommendations on how to meet the implementation requirements, referring to the records that have to be kept according to Section 8.4. We have seen that some of these measures (such as signing the votes, see R3.1) affect the voting protocol directly and, thus, should be considered already when designing and implementing an electronic voting scheme.

We have considered the constraints which apply to the records kept *after* the election. However, in order to comply with the implementation requirement of confidentiality, the respective records must, first of all, not be published *during* the election, for example on public bulletin boards (see Section 2.2.7). Still, this is often disregarded by current voting protocols; we will consider such an example in the following chapter when we apply our findings to a state-of-the-art online voting scheme.

When publishing election data, it should also be considered that even encrypted data can lose its confidentiality in the long term if the cryptographic algorithms which have been used become insecure. Thus, anyone can copy the information published via the bulletin board and simply wait until the encryption system is broken in the future. This may also compromise voter privacy in the long term if, for example, encrypted votes are published next to the voters' names.

Thus, if sensitive data is published negligently (or even well-intentioned and showing awareness of the issue of verifiability), this may compromise confidentiality or even privacy, though the latter may eventually be affected only in the long term. Overall, verifiability is desirable only as far as privacy is not affected, and should never allow for disclosing a voter's voting decision (cf. [Pie08, Section 10.3] for a different view).

10. Application

In this chapter we apply our results regarding secure and conclusive retention of election data, which we established in Chapter 8 and 9, to the voting scheme [JCJ05] proposed by Juels, Catalano, and Jakobsson (JCJ). This protocol was the first one to offer coercion-resistance: a voter cannot prove how he voted, and he cannot be forced to abstain from voting, to cast a random vote, or to vote in a particular way (see Sections 2.1.6 and 3.1). As we suppose that coercion-resistance is a mandatory requirement for an online voting scheme to be used in parliamentary elections (compare the legal requirement of free elections, see Section 8.1), we have selected the JCJ scheme to demonstrate the applicability of our retention concepts established for Federal Elections for the German Bundestag.

After the JCJ scheme was published in 2005, several proposals for improvements followed [Smi05, WAB07, AFT07], of which only the last one preserved coercion-resistance. However, as the improvements in [AFT07] only pertain to efficiency, they are not relevant to our approach, and we stick to the original scheme [JCJ05]. We investigate which records must be kept in order to meet the retention requirements specified in Section 8.4, and which measures should be applied according to the recommendations made in Section 9.4. An earlier version of this chapter has been published in [15].

Chapter overview

First we describe the JCJ protocol in Section 10.1. In Section 10.2 we investigate the records to be kept and the protective measures to be applied. The results are discussed in Section 10.3.

10.1. Description of the JCJ scheme

The intuition behind the JCJ scheme [JCJ05] is the following: a potential adversary does not learn whether the coerced voter complied with his demand. In effect, the adversary thus has no possibility to coerce the voter. The voter's identity remains hidden during vote-casting, and validity of the ballots is verified by blind comparison against the voters' register. To this end, secret anonymous credentials are distributed among the voters in registration phase. These credentials serve two purposes: they are used to authenticate the voters, and mark a freely cast vote. If a voter wants the vote he is about to cast to be accounted, he includes his valid credential; if not (due to coercion), he attaches an invalid credential. The coercer is not able to distinguish invalid credentials from valid ones and hence cannot know if the voter has complied

with his demand. Since multiple voting is allowed, the voter can hereafter cast a valid vote. In the end only the latest vote with a valid credential is accounted in the tallying process.

In the following we explain the three phases of the protocol (i.e. registration, voting, and tallying phase) more thoroughly. The participants are voters, a registration authority, and a distributed tallying authority. The registration authority is assumed to be trustworthy; in particular, it must not leak credentials to an adversary [JCJ05]. For encryption, a modified version of ElGamal (see Section 2.2.1) is used throughout; for details refer to [JCJ05]. Prior to the election, the key pair $(SK_{\mathcal{T}}, PK_{\mathcal{T}})$ of the tallying authority $\mathcal{T}$ is generated. Let $\mathcal{E}_{PK_{\mathcal{T}}}(m)$ denote an encryption of message m using the public key $PK_{\mathcal{T}}$.

Registration. Each eligible voter v_i receives a unique valid credential σ_i from the registration authority over an untappable channel. An encrypted version $S_i = \mathcal{E}_{PK_{\mathcal{T}}}(\sigma_i)$ of each credential is published on the bulletin board. At the end of the registration phase, the voters' register L contains all valid encrypted credentials alongside the plaintext names of registered voters, and is signed by the registration authority.

Voting. The registration authority publishes an integrity-protected candidate list $C = \{c_1, c_2, \ldots, c_{nC}\}$ where each entry c_i identifies a possible choice (that is, a candidate or party). Using an anonymous channel, voter v_i posts his ballot to the bulletin board. Each ballot consists of the following components:

1. $\mathcal{E}_{PK_{\mathcal{T}}}(c_j)$, an encryption of the chosen candidate, hereafter referred to as the encrypted vote
2. $\mathcal{E}_{PK_{\mathcal{T}}}(\sigma_i)$, an encryption of the voter's credential
3. a non-interactive zero-knowledge proof (see Section 2.2.3) on $c_j \in C$, proving that the vote is cast for a valid candidate
4. a non-interactive zero-knowledge proof of knowledge of σ_i and c_j

Voter v_i encrypts his valid credential σ_i if he wants his vote to be accounted, otherwise he encrypts a fake credential $\tilde{\sigma}_i$. The proof that c_j indeed marks a valid candidate is necessary since casting write-in votes allows for coercion: the adversary could force the voter to cast a vote containing a predetermined character string, and subsequently verify whether the voter complied with his demand by checking the bulletin board for this specific string. Knowledge of σ_i and c_j must be proven to prevent replay attacks performed by simply reencrypting votes that have already been cast.

Tallying.

1. **Proof checking.** Let B_0 denote the list of all encrypted credentials that have been used for ballot casting. The tallying authority first checks that all proofs included in each ballot are correct. Ballots containing invalid proofs are discarded. For the remaining ballots, let A_1 denote the list of encrypted votes and B_1 the list of encrypted credentials.

2. **Duplicate removal.** The tallying authority removes ballots with credential duplicates via pairwise plaintext equality tests (see Section 2.2.3). Only the latest credentials in B_1 are kept, resulting in a weeded list B_2. The ciphertexts in A_1 which correspond to duplicate credentials (i.e. those with the same indices) are also removed, resulting in a weeded list A_2. Now there is no more than one vote per given credential.

3. **Mixing.** The list of encrypted votes as well as the list of encrypted credentials is processed by a reencryption mixnet (see Section 2.2.6) using the same, secret permutation. The list of encrypted credentials contained in L is processed through a reencryption mixnet as well, but using a different permutation. Let A'_2, B'_2 and L' denote the mixed lists.

4. **Validity checking.** The credentials in B'_2 are compared with the ones in L' via pairwise plaintext equality test, eliminating those which do not correspond to valid credentials in L'. The corresponding invalid votes in A'_2 are eliminated as well. Let A_3 and B_3 denote the final lists. These now correspond to authentic ballots cast freely by eligible voters with at most one vote per voter.

5. **Vote counting.** The encrypted votes in A_3 are jointly decrypted and tallied. The tallying authority publishes a proof of correct decryption.

10.2. Records to be kept

We now investigate which records should be kept according to the implementation proposals specified in Section 8.4, and which constraints and protective measures should apply to these records according to the recommendations given in Section 9.4. We follow the structure of Section 8.4.

10.2.1. Preparation phase

Prep1: Trustworthy entities

Prep1.1 The agreements and contracts documenting trustworthiness of staff members, in particular registration and tallying authority, should be retained in PDF/A format (see Section 9.4, R1.3). These records are confidential as they contain personal information of the respective persons, and should therefore only be accessible to designated election authorities (see Section 9.4, R6.2).

Prep1.2 The evaluation report should be signed by the certification authority (see Section 9.4, R3.3) and retained.

Prep2: Proper installation and surroundings

Prep2.1 The JCJ scheme does not explicitly provide for a ballot box; the ballots are cast by posting them to the bulletin board (see Section 10.1). Therefore, documenting that the ballot box was empty before the voting phase started amounts to documenting that the bulletin board did not contain any ballots at that time. A copy of the contents of the bulletin board provided with a qualified timestamp issued at the beginning of the voting phase (see Section 9.4, R2.2) should therefore be retained.

Prep2.2 Not applicable (see Section 8.4.1).

Prep3: Closure of the voters' register

The voters' register L lists the names of the eligible voters and contains their valid, encrypted credentials. It should be provided with a qualified timestamp before the election starts (see Section 9.4, R2.1). The number of eligible voters is determined by $|L|$, the length of list L. Since this list is a structured data set, it should be generated and retained in XML format (see Section 9.4, R1.1), and signed by the registration authority using XML signatures (see Section 9.4, R1.2, R3.4a). This record is confidential as it contains personal information of voters, and should therefore only be accessible to designated election authorities (see Section 9.4, R6.2).

Prep4: Justified nomination of candidates

The candidate list C contains unique identifiers for the candidates and should be retained since the identifiers are required to determine the election result from the encrypted votes in list A_3. If C does not list the names of the candidates, a document assigning the candidate identifiers to their names has to be retained as well as the collection of supporting signatures for candidate nominations. Each of these documents should be signed by the registration authority (see Section 9.4, R3.4b). The collection of supporting signatures for candidate nominations is confidential as it contains personal information of the nominated candidates and the supporting voters, and should therefore only be accessible to designated election authorities (see Section 9.4, R6.2).

10.2.2. Voting phase

Vote1: Special incidents

The log files of the system should be signed by an election authority (see Section 9.4, R3.4d) and subsequently retained.

Vote2: Different voting channels

i. List B_3 in conjunction with the voters' register L provides a record of all voters who have cast a vote under a valid credential: B_3 contains all valid encrypted credentials that have been used for ballot casting, and L contains the names of eligible voters alongside their valid, encrypted credentials. Using plaintext equality tests, the names of voters who have participated in the election using valid credentials can be figured out, as well as their number. The resulting record should be signed by the tallying authority and retained (see Section 9.4, R3.4c); it must be ensured that it remains confidential as coercion-resistance would otherwise be compromised (see also Section 9.4, R6.2). The number of voters who have only cast ballots using invalid credentials cannot be determined: $|B_2| - |B_3|$ yields the number of ballots cast under invalid credentials; however, this number may be greater than the number of voters who cast these ballots due to the possibility of one voter using different invalid credentials. If the total number of voters must be ascertainable, then the JCJ protocol has to be adapted, for example by using predefined invalid credentials as proposed in [MHEA08].

ii. Using plaintext equality tests as mentioned above, the names of voters who have participated in the remote electronic election and used valid credentials can be figured out, thus documenting the voters who cast an online vote. The resulting record should be signed by the tallying authority and retained (see Section 9.4, R3.4c) in a way such that its confidentiality is ensured (see Section 9.4, R6.2).

Vote3: Secrecy of the vote

Vote3.1 Documenting that the content of the ballot was protected against unauthorized inspection from the time the ballot was completed until the end of the voting phase can be achieved by demonstrating that the key pair $(SK_{\mathcal{T}}, PK_{\mathcal{T}})$ has been generated securely (i.e. by a trusted third party or using a secure key-generation protocol, see [JCJ05]). According documents should be retained. The certified trustworthiness of the tallying authority (see Section 10.2.1, Prep1.1) completes this record.

Vote3.2 The JCJ protocol is not designed for providing voter declarations of having voted personally. Such declarations could be introduced as another part of the ballot (besides encrypted vote and zero-knowledge proofs), but have to be anonymous in order to preserve coercion-resistance. Ballots of voters who have not provided this declaration could then be sorted out in tallying phase.

Vote4: Proper termination of the poll

i. Timely termination of the poll is documented by retaining the log files (see Vote1, Vote5). Additionally, a copy of the contents of the bulletin

board which has been provided with a qualified timestamp issued at the end of the voting phase should be retained (see Section 9.4, R2.3).

ii. Having notified voters about the upcoming end of the voting phase is documented by retaining the log files (see Vote1, Vote5).

Vote5: Public conduct of the poll

The log files of the system should be signed by an election authority (see Section 9.4, R3.4d) and subsequently retained.

10.2.3. Evaluation phase

Eval1: Repeated, independent tallying

Since having the ballots recounted by an independent third party is not possible due to the secret keys required, the ballots should be recounted using a different tallying routine. Note that recounting the votes requires running through all five phases according to Section 10.1. The results should be signed by the tallying authority and retained (see Section 9.4, R3.4h).

Eval2: Public conduct of the tally

i. A validating authority confirming authenticity of the votes by signing them is not provided by the JCJ protocol. Therefore, recommendation R3.1 (see Section 9.4) cannot be applied. According to R3.2, the ballots should thus be signed. As this cannot be provided by the voters themselves (recall that coercion-resistance requires their identity to remain hidden during the election process), the collection of received ballots should be signed by the tallying authority and retained (see Section 9.4, R3.4e). The total N of received ballots[1] is determined by this record. The ballots are a structured data set and, thus, should be generated and retained in XML format (see Section 9.4, R1.1). XML signatures should be used to sign the received ballots (see Section 9.4, R1.2).

ii. The proofs of correct decryption should be signed by the tallying authority and retained (see Section 9.4, R3.4f).

iii. The election result and the number of valid and invalid ballots should be documented, signed by the tallying authority, and subsequently retained (see Section 9.4, R3.4g). Note that a ballot[2] can be invalid due to one or more of the following reasons:

[1] Note that this value includes multiple ballots cast by voters under both valid and invalid credentials.

[2] As mentioned in Section 10.1, for the JCJ scheme to remain coercion-resistant, it is excluded that voters cast write-in votes, which means that they vote for candidates that are not listed in C. This implies that voters cannot cast invalid *votes*, that is, ballots which have been invalidated by an illegal vote and not by using an invalid credential or providing invalid proofs.

- it contains an invalid proof (this holds for $N - |B_1|$ ballots, see stage 1 of the tallying phase)
- it has been cast under a valid credential which was *later on* reused to vote, thus invalidating the previously cast ballot (this holds for $|B_1| - |B_2|$ ballots, see stage 2 of the tallying phase)
- it was cast under an invalid credential (this holds for $|B_2| - |B_3|$ ballots, see stage 4 of the tallying phase)

Thus, there are $N - |B_3|$ invalid ballots. Note that documenting the retrieval of the election result includes retaining ballots that have been declared invalid. Thus, ballots that have been sorted out due to invalid proofs, duplicate credentials or invalid credentials (see stage 1-3 of the tallying phase) must not be discarded, but rather retained and just eliminated from the tally. The proofs of knowledge of the tallied votes should be kept as well. List B_3 contains the valid, unique credentials under which votes have been cast; it should be retained as it must be verifiable that only eligible voters (i.e. those listed in the voters' register L) have cast a ballot.

Other measures to be taken with regard to privacy

In accordance with our recommendation R5.4 (see Section 9.4), the JCJ scheme does not timestamp the ballots, but rather refers to the order in which the ballots were posted to the bulletin board for determining the order of the received ballots. The secret key of the tallying authority should be securely retained for two months (i.e. the period in which the election may be challenged by the public, cf. § 2 (2, 4) WPrüfG) and permanently deleted hereafter in order to protect voter privacy (see Section 9.4, R5.2). Since the tallying authority is distributed (see Section 10.1), according deletion policies must be enforced for each trustee. Any residual information linking the voter to his vote must be deleted (see Section 9.4, R5.3): the voter must permanently delete any local copies of the credential which he obtained from the registration authority, and the mixnet must permanently delete the secret permutations used for the mixing procedures in tallying phase, as well as the randomization values used to reencrypt the messages. In the unlikely event that the election result allows inference on the voting decision of individual voters, according measures must be applied to protect voter privacy (see Section 9.4, R5.5).

After the election has terminated, authentication data referring to the identity of the voter must no longer be linkable to ballot data containing the vote (see Section 9.4, R5.1). This is not fulfilled by the JCJ scheme: the protocol provides for publishing the list L of encrypted credentials alongside the voter names on the bulletin board. The list of all received ballots, consisting of encrypted vote, encrypted credential and zero-knowledge proofs, is published as well (see Section 10.1). Hence, via L, the voter is linked to the encrypted credential, and, via the ballot, the encrypted credential used for vote-casting is linked to the encrypted vote. It follows

that, should the encryption scheme be broken in the long term, voter and vote can be linked. In Section 10.3 we propose how to improve the protocol in this regard.

Other measures to be taken with regard to integrity, authenticity, and confidentiality

Any of the records retained should be kept on non-rewritable, portable storage media and stored in a secure location; a duplicate of each record shall be kept in a different place (see Section 9.4, R2.4). The records which are public should be posted to the bulletin board for at least two months after the poll (see Section 9.4, R6.1). The confidential records should only be accessible to election authorities and official election observers. Therefore, these records should be protected by either encrypting them or by implementing access control within the archiving system (see Section 9.4, R6.2). Moreover, anyone who has access to election records containing personal data must be informed on his duty not to use this data for any purpose other than specified by electoral law (cf. § 89 (2, 3) BWO), i.e. election statistics, scrutiny procedures or in case an election fraud according to § 107 and § 108 StGB is suspected (see Section 9.4, R6.3). Timely signature renewal must be taken care of for any signatures issued (see Section 9.4, R3.5).

10.3. Discussion

In this chapter we investigated which of the data occurring in an online election based on the protocol [JCJ05] must be retained according to the implementation proposals given in Chapter 8, and how the protective measures derived in Chapter 9 can be applied to the protocol. We have seen that

- retaining *no more than* the data generated by the protocol is not sufficient to meet legal retention requirements. For example, secure generation of the key pair $(SK_{\mathcal{T}}, PK_{\mathcal{T}})$ must be documented;
- retaining records generated by the protocol *in their original condition* lacks sufficient probative value. For example, according to the protocol, no record besides the voters' register L is to be signed by an election authority. Thus, additional protective measures as proposed in Section 9.4 have to be taken; and
- retaining *any* data occurring during the online election is even dangerous since this may compromise voter privacy. For example, the randomization values and the permutation used by the reencryption mixnet could be exploited to reconstruct the mixing of the ballots in tallying phase.

In order to maintain voter privacy in the long term, we propose that the valid encrypted credentials should not be published alongside the voters' plaintext names (cf. Section 8.4.2, Vote3). We recommend to detach the two parts of list L and

scramble them already in the registration phase in order to hide the relation between the voter and the encrypted credential. Alternatively, the plaintext names of voters should not be published at all (cf. Section 8.4.1, Prep3, and Section 9.4, R6.2): the voter can see the anonymized list of encrypted credentials published on the bulletin board; additionally, he can be assured by obtaining a proof from the registrars that the encryption of his credential is valid and contained in this list. However, this approach cannot save receipt-freeness and coercion-resistance in the long term as the adversary learns the valid credentials if the encryption is broken and, thus, can tell whether he has obtained a valid or a fake credential from the coerced voter.

11. Conclusions and future work

Chapter overview

This chapter concludes the thesis at hand by providing a summary for each Part I and II, recapitulating the contributions made, and considering future work.

Part I: A Taxonomy for Privacy and Verifiability in Electronic Voting

The first part of this thesis aimed at answering the following research question:

> Which levels of privacy and verifiability are conceivable in electronic voting, and how are both properties related?

We addressed this question by first reviewing existing definitions of privacy and verifiability and considering related work in Chapter 3. In Chapter 4, we provided an intuitive model which captures both privacy and verifiability and allows to express both properties in terms of (un)linkability, thus clarifying the relation between the two. Also in Chapter 4, we introduced different levels of privacy and verifiability. Our research question was thus answered in Chapter 4. In Chapter 5 we considered different adversary capabilities and how they can be exploited to mount attacks on privacy and verifiability. The adversary capabilities constitute building blocks which can be combined in order to obtain the desired adversary model. Together, these three components (i.e. the (un)linkability model, the privacy and verifiability levels, and the adversary capabilities) establish our taxonomy for privacy and verifiability in electronic voting. The taxonomy can be used for analyzing the security of existing voting schemes, which we have done in Chapter 6, thus demonstrating the applicability of the taxonomy. Our analysis showed that, depending on the adversary capabilities assumed, different levels of privacy and verifiability and, thus, different forms of (un)linkability are provided.

The value of the (un)linkability model lies in the unification of seemingly different properties under a common terminology, enabling a clear visual representation of privacy and verifiability. Moreover, the model allows to define precisely the notions cast-as-intended, counted-as-cast, recorded-as-cast and counted-as-recorded, which are not accurate by themselves. The levels of privacy and verifiability demonstrate the different facets of both properties. Together with the (un)linkability model, they contribute to a deeper understanding of privacy and verifiability and their correlation in electronic voting. Moreover, the compilation of the different levels of privacy and verifiability allows to select appropriate levels for different types of elections, and the adversary capabilities enable designing voting systems for particular environments, where the stakes of the election determine what kind of adversary model should be

assumed. Consequently, the question arises which privacy and verifiability levels and what adversary models are suitable for which election type. However, answering this question is beyond the scope of this thesis as it involves a long process of decision-making.

When investigating the levels of privacy in Section 4.3, we did not consider probabilistic privacy [DPP07]: even if an adversary cannot link voter and vote with absolute certainty, it is still not desirable that there is a high probability that a voter cast a specific vote. The suitability of this approach for voting is limited as the outcome of an election is directly related to the probabilities of voters having voted in a certain way [Pie08]. However, it may still be considered future work to extend the taxonomy by the concept of probabilistic privacy. Similarly, one could define sublevels of universal verifiability depending on whether verification is probabilistic or not:

> **Absolute accuracy verifiability.** There is a proof of the correct processing of the ballots in tallying phase, i.e. absolute assurance is provided.
>
> **Probabilistic accuracy verifiability.** There is evidence of the correct processing of the ballots in tallying phase, i.e. probabilistic assurance with a certain probability $p < 1$ is provided.

Such a differentiation would allow for a classification of the techniques employed to achieve verifiability. We consider this to be future work.

Part II: Long-Term Verifiability: Legal Issues and Technical Implications

The second part of this thesis aimed at answering the following research question:

> Which records of a remote electronic election should be retained, and which protective measures should be applied?

We addressed this question by first providing background information on long-term retention of election data, presenting related work, and explaining the methodology in Chapter 7. In Chapter 8, we answered the first part of our research question by identifying the records to be retained after an online election has been carried out. To this end, we abstracted from legal retention obligations on paper-based elections and derived retention requirements for online elections using an approved method named KORA. In Chapter 9, we identified any constraints which apply to the record keeping, and used KORA to derive according technical measures for secure and conclusive retention of electronic election data, thus answering the second part of our research question. In Chapter 10 we applied our results to [JCJ05], a state-of-the-art voting scheme. We investigated which of the data generated by (or in addition to) the protocol must be retained in order to meet the requirements identified in Chapter 8, and which measures should be applied according to the recommendations made in Chapter 9. We also proposed how to improve the protocol with respect to long-term voter privacy.

Establishing Internet voting in parliamentary elections presupposes that its technical implementation meets certain legal requirements, and conclusive retention of election data is one of them. Thus, our work contributes to laying the basis for legally binding online voting on a parliamentary level in Germany. As electoral law in Europe is rather consistent, other countries may benefit from this as well. Furthermore, our work is valuable for developing legally compliant electronic voting systems as the need for record keeping should be considered already when designing and implementing a remote electronic voting protocol.

In Chapter 8 we have seen that, in an online election, it is not possible to fully comply with the legal principles of secrecy and freedom of vote. This is due to the fact that the scenario of remote electronic voting does not allow unobserved polling to be enforced by any supervisory authority. Moreover, as the poll cannot be physically observed, it is particularly challenging to establish and to document the public conduct of an online election. Both disadvantages apply also to absentee voting, a voting channel which is well-established in Germany. It was introduced in the 1957 Federal Election and has ever since become widely used. Between 1990 and 2009, the absentee voter turnout (i.e. the number of absentee voters divided by the total number of participating voters) increased from 9.4% to 21.4% [Bun] (see also Table 11.1).

Table 11.1.: Absentee voter turnout in Federal Elections since 1990 [Bun]

1990	1994	1998	2002	2005	2009
9.4%	13.4%	16.0%	18.0%	18.7%	21.4%

The option of absentee voting was introduced in order to strengthen the universality of elections at the expense of secrecy and public conduct [BR09]. Online voting happens in uncontrolled environments as well and is therefore comparable to absentee voting. In both scenarios, secrecy in terms of unobserved polling must be taken care of by the voter himself. With regard to the principle of public elections, however, remote electronic voting has an advantage over absentee voting by offering a different kind of transparency which cannot be established even in a conventional paper-based election: anyone can verify that the ballots have been correctly processed and tallied, usually on the basis of mathematical proofs. These are less intuitive, but provide much stronger evidence of the proper conduct of the election than simply observing the Electoral Board counting the votes manually. Although such verification methods are not understandable to the general public, they can substantially help experts to verify that the election has been duly performed.

Contrary to that, the Federal Constitutional Court has judged that *each citizen* must be able to comprehend the essential steps of the election without having expert knowledge (see [Fed09a], margin number 109). However, this judgment refers to voting in the controlled environment of polling stations using voting machines.

Therefore, it does not fully apply to remote electronic voting in uncontrolled environments as the public conduct is traded off for universality in this case. In fact, the Court's press release states that "all essential steps of an election are subject to the possibility of public scrutiny unless other constitutional interests justify an exception" [Fed09b]. Introducing remote electronic voting as an additional voting channel in parliamentary elections accommodates voters' needs in a mobile society and provides an opportunity to increase voter turnout, which is a constitutional interest. It is, however, highly desirable to provide easily comprehensible verification methods in order to reach as many people as possible. The question how to reconcile verifiability and usability is, in fact, a major open problem in electronic voting.

Acronyms

BDSG	Bundesdatenschutzgesetz (Federal Data Protection Law)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BWG	Bundeswahlgesetz (Federal Electoral Law)
BWO	Bundeswahlordnung (Federal Electoral Regulations)
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DFG	Deutsche Forschungsgemeinschaft (German Research Foundation)
DOMEA	Dokumenten-Management und elektronische Archivierung (Document Management and Electronic Archiving)
ERS	Evidence Record Syntax
GG	Grundgesetz (German Constitutional Law)
GI	Gesellschaft für Informatik (German Informatics Society)
InterPARES	International Research on Permanent Authentic Records in Electronic Systems
KORA	Konkretisierung rechtlicher Anforderungen (Implementation of Legal Requirements)
NESTOR	Network of Expertise in Long-Term Storage of Digital Resources
SGB	Sozialgesetzbuch (Social Security Code)
SigG	Signaturgesetz (Signature Law)
SigV	Signaturverordnung (Signature Ordinance)
StGB	Strafgesetzbuch (German Criminal Code)
UrhG	Urheberrechtsgesetz (German Copyright Act)
WPruefG	Wahlprüfungsgesetz (Law on the Scrutiny of Elections)

Bibliography

[ACvdG07] Roberto Araújo, Ricardo Felipe Custódio, and Jeroen van de Graaf. A Verifiable Voting Protocol based on Farnel, 2007. IAVoSS Workshop on Trustworthy Elections (WOTE 2007).

[Adi06] Ben Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2006.

[Adi08] Ben Adida. Helios: Web-based Open-Audit Voting. In *SS'08: Proceedings of the 17th conference on Security symposium*, pages 335–348, Berkeley, CA, USA, 2008. USENIX Association.

[AdMPQ09] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios. In David Jefferson, Joseph Lorenzo Hall, and Tal Moran, editors, *EVT/WOTE '09: Proceedings of the Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*. USENIX Association, 2009.

[AFT07] Roberto Araújo, Sébastien Foulle, and Jacques Traoré. A practical and secure coercion-resistant scheme for remote elections. In David Chaum, Miroslaw Kutylowski, Ronald L. Rivest, and Peter Y. A. Ryan, editors, *Frontiers of Electronic Voting*, volume 07311 of *Dagstuhl Seminar Proceedings*. Internationales Begegnungs- und Forschungszentrum fuer Informatik (IBFI), Schloss Dagstuhl, Germany, 2007.

[AN06] Ben Adida and C. Andrew Neff. Ballot Casting Assurance. In *EVT '06: Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop*, Berkeley, CA, USA, 2006. USENIX Association. `http://www.usenix.org/events/evt06/tech/full_papers/adida/adida.pdf`.

[AR08] Roberto Araújo and Peter Y. A. Ryan. Improving the farnel voting scheme. In Krimmer and Grimm [KG08], pages 169–184.

[BBG07] Earl Barr, Matt Bishop, and Mark Gondree. Fixing Federal E-Voting Standards. *Communications of the ACM*, 50(3):19–24, 2007.

[Ben87] Josh Daniel Cohen Benaloh. *Verifiable Secret-Ballot Elections*. PhD thesis, Yale University, New Haven, CT, USA, 1987.

[Ben06] Josh Benaloh. Simple Verifiable Elections. In *EVT '06: Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop*, Berkeley, CA, USA, 2006. USENIX Association. `http://www.usenix.org/event/evt06/tech/full_papers/benaloh/benaloh.pdf`.

[Ben07] Josh Benaloh. Ballot Casting Assurance via Voter-Initiated Poll Station Auditing. In *EVT '07: Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop*, pages 14–14, Berkeley, CA, USA, 2007. USENIX Association. `http://www.usenix.org/event/evt07/tech/full_papers/benaloh/benaloh.pdf`.

[BFP+01] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, and Guillaume Poupard. Practical Multi-Candidate Election System. In *PODC '01: Proceedings of the twentieth annual ACM symposium on Principles of distributed computing*, pages 274–283, New York, NY, USA, 2001. ACM.

[BM03] Mike Burmester and Emmanouil Magkos. *Towards Secure and Practical e-Elections in the New Era*, volume 7 of *Advances in Information Security*, chapter 5. Kluwer Academic Publishers, 2003.

[BMQR07] Jens-Matthias Bohli, Jörn Müller-Quade, and Stefan Röhrich. Bingo Voting: Secure and Coercion-Free Voting Using a Trusted Random Number Generator. In Ammar Alkassar and Melanie Volkamer, editors, *VOTE-ID*, volume 4896 of *Lecture Notes in Computer Science*, pages 111–124. Springer, 2007.

[Bon98] Dan Boneh. The Decision Diffie-Hellman Problem. In Joe Buhler, editor, *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer, 1998.

[BPRS02] Ralf Brandner, Ulrich Pordesch, Alexander Roßnagel, and Joachim Schachermayer. Langzeitsicherung qualifizierter elektronischer Signaturen. *DuD – Datenschutz und Datensicherheit*, 26(2), 2002.

[BPSM+08] Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, and François Yergeau. *Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation*. W3C, 1 edition, November 2008.

[BR09] Johannes Buchmann and Alexander Roßnagel. Das Bundesverfassungsgericht und Telemedienwahlen. Zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu elektronischen Wahlgeräten für die Durchführung von "Internetwahlen" in nicht-politischen Bereichen. *Kommunikation und Recht (K&R)*, 12(9), 2009.

[BRSS06] Uwe M. Borghoff, Peter Rödig, Jan Scheffczyk, and Lothar Schmitz. *Long-Term Preservation of Digital Documents: Principles and Practices*. Springer, Secaucus, NJ, USA, 2006.

[BT94] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *STOC '94: Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 544–553, New York, NY, USA, 1994. ACM.

[Bun] Bundeswahlleiter. Wahl zum 17. Deutschen Bundestag am 27. September 2009. Ergebnisse der repräsentativen Wahlstatistik. Available at `http://www.bundeswahlleiter.de/de/bundestagswahlen/BTW_BUND_09/veroeffentlichungen/statement.pdf`.

[Bun06] Bundesamt für Sicherheit in der Informationstechnik. *IT–Grundschutz–Kataloge: Maßnahmen: Maßnahmenkatalog M4 Hardware und Software*, 2006. Available in German at `http://www.bsi.de/gshb/`; outdated English version available at `https://www.bsi.bund.de/cln_174/ContentBSI/EN/Topics/ITGrundschutz/itgrundschutz.html`.

[Bun09] Bundesamt für Sicherheit in der Informationstechnik. Vertrauenswürdige elektronische Langzeitspeicherung. Technische Richtlinie 03125 (BSI-TR-03125), 2009. Version 1.0.

[CCC+08] David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, and Alan T. Sherman. Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. In *EVT '08: Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop*, pages 1–13, Berkeley, CA, USA, 2008. USENIX Association.

[CCp09a] Common Methodology for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 3. CCMB-2009-07-001, July 2009. `http://www.commoncriteriaportal.org/thecc.html`.

[CCp09b] Common Methodology for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 3. CCMB-2009-07-002, July 2009. `http://www.commoncriteriaportal.org/thecc.html`.

[CCp09c] Common Methodology for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 3. CCMB-2009-07-003, July 2009. `http://www.commoncriteriaportal.org/thecc.html`.

[CEM09] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3. CCMB-2009-07-004, July 2009. `http://www.commoncriteriaportal.org/thecc.html`.

[Cet07] Orhan Cetinkaya. *Verifiability and Receipt-freeness in Cryptographic Voting Systems*. PhD thesis, Middle East Technical University, 2007.

[CF85] Josh D. Cohen and Michael J. Fischer. A Robust and Verifiable Cryptographically Secure Election Scheme (Extended Abstract). In *FOCS*, pages 372–382. IEEE Computer Society, 1985.

[CGS97] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. A Secure and Optimally Efficient Multi-Authority Election Scheme. In Walter Fumy, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118. Springer, 1997.

[Cha81] David Chaum. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[Cha82] David Chaum. Blind Signatures for Untraceable Payments. In *CRYPTO*, pages 199–203, 1982.

[CMFP+06] Benoît Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern, and Jacques Traoré. On Some Incompatible Properties of Voting Schemes, 2006. IAVoSS Workshop on Trustworthy Elections (WOTE 2006).

[Cou03] Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, 2003. `http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf`.

[Cou05] Council of Europe. Legal, operational and technical standards for e-voting. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum. Council of Europe Publishing, 2005. `http://www.coe.int/T/e/integrated_projects/democracy/02_Activities/02_e-voting/`.

[CP92] David Chaum and Torben P. Pedersen. Wallet Databases with Observers. In Ernest F. Brickell, editor, *CRYPTO*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 1992.

[CPS94] Jan Camenisch, Jean-Marc Piveteau, and Markus Stadler. Blind signatures based on the discrete logarithm problem. In Alfredo De Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 428–432. Springer, 1994.

[CRS05] David Chaum, Peter Y. A. Ryan, and Steve A. Schneider. A Practical Voter-Verifiable Election Scheme. In Sabrina De Capitani di Vimercati, Paul F. Syverson, and Dieter Gollmann, editors, *ESORICS*, volume

3679 of *Lecture Notes in Computer Science*, pages 118–139. Springer, 2005.

[Deu06] Deutsche Forschungsgemeinschaft. Wahlordnung für die Wahl der Mitglieder der Fachkollegien der Deutschen Forschungsgemeinschaft (DFG), 2006. Available in German only: `http://www.dfg.de/download/formulare/70_01/70_01_rtf.rtf`.

[DH76] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.

[DKR09] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, July 2009. `http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/DKR-jcs08.pdf`.

[DPP07] Yuxin Deng, Catuscia Palamidessi, and Jun Pang. Weak Probabilistic Anonymity. *Electronic Notes in Theoretical Computer Science (ENTCS)*, 180(1):55–76, 2007.

[DSJ06] Kevin Daimi, Katherine Snyder, and Robert James. Requirements Engineering for E-Voting Systems. In Hamid R. Arabnia and Hassan Reza, editors, *Proceedings of the International Conference on Software Engineering Research and Practice & Conference on Programming Languages and Compilers, SERP 2006, Las Vegas, Nevada, USA, June 26-29, 2006, Volume 1*, pages 259–265. CSREA Press, 2006.

[DY83] Danny Dolev and Andrew Chi-Chih Yao. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2):198–207, 1983.

[ERS02] Donald Eastlake, Joseph Reagle, and David Solo. (Extensible Markup Language) XML-Signature Syntax and Processing. RFC 3275 (Standards Track), March 2002. `http://www.ietf.org/rfc/rfc3275.txt`.

[Est05] Estonian National Election Committee. E-Voting System – Overview, 2005. `http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf`.

[ETS06] ETSI. Technical Specification XML Advanced Electronic Signatures (XAdES). TS 101 903, Version 1.3.2, 2006.

[ETS08] ETSI. Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). TS 101 733, Version 1.7.4, 2008.

[FD06] Stefanie Fischer-Dieskau. *Das elektronisch signierte Dokument als Mittel zur Beweissicherung*. Nomos, Baden-Baden, 2006.

[Fed83] Federal Constitutional Court (Bundesverfassungsgericht). 1 BvR 209, 269, 362, 420, 440, 484/83, December 15 1983.

[Fed09a] Federal Constitutional Court (Bundesverfassungsgericht). 2 BvC 3/07, 2 BvC 4/07, March 3 2009. Available in German only: `http://www.bundesverfassungsgericht.de/entscheidungen/cs20090303_2bvc000307.html`.

[Fed09b] Federal Constitutional Court (Bundesverfassungsgericht). Use of voting computers in 2005 Bundestag election unconstitutional. Press release no. 19/2009, March 3 2009. `http://www.bverfg.de/en/press/bvg09-019en.html`.

[FS86] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In Andrew M. Odlyzko, editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[FS01] Jun Furukawa and Kazue Sako. An Efficient Scheme for Proving a Shuffle. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 368–387. Springer, 2001.

[Gam84] Taher El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In G. R. Blakley and David Chaum, editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, 1984.

[GBP07] Tobias Gondrom, Ralf Brandner, and Ulrich Pordesch. Evidence Record Syntax (ERS). RFC 4998 (Standards Track), August 2007. `http://www.ietf.org/rfc/rfc4998.txt`.

[Ges04] Gesellschaft für Informatik. Ordnung der Wahlen und Abstimmungen, last amended September 21, 2004. Available in German only: `http://www.gi-ev.de/fileadmin/redaktion/OWA/gi-owa.pdf`.

[Ges05] Gesellschaft für Informatik. GI-Anforderungen an Internetbasierte Vereinswahlen (GI requirements for Internet based elections in non-governmental organizations), August 2005. `http://www.gi-ev.de/fileadmin/redaktion/Wahlen/GI-Anforderungen_Vereinswahlen.pdf`.

[GKM+06] Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, and Marcel Weinand. Security Requirements for Non-political Internet Voting. In Robert Krimmer, editor, *Electronic Voting*, volume 86 of *LNI*, pages 203–212. GI, 2006.

[Gla07] Henry Gladney. *Preserving Digital Information.* Springer, Secaucus, NJ, USA, 2007.

[Hir01] Martin Hirt. *Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting*. PhD thesis, ETH Zurich, September 2001. Reprint as vol. 3 of *ETH Series in Information Security and Cryptography*, ISBN 3-89649-747-2, Hartung-Gorre Verlag, Konstanz, 2001.

[HPR92] Volker Hammer, Ulrich Pordesch, and Alexander Roßnagel. KORA – eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme. Arbeitspapier 100, provet, Darmstadt, 1992.

[HS91] Stuart Haber and W. Scott Stornetta. How to Time-Stamp a Digital Document. *Journal of Cryptology*, 3(2):99–111, 1991. `http://www.cs.utk.edu/~dunigan/cns04/timestamp.pdf`.

[HS00] Martin Hirt and Kazue Sako. Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 539–556. Springer, 2000.

[Inta] International Organization for Standardization. ISO/IEC 15408:2008: Information technology – Security techniques – Evaluation criteria for IT security. International Standard.

[Intb] International Organization for Standardization. ISO/IEC 18045:2008: Information technology – Security techniques – Methodology for IT security evaluation. International Standard.

[Intc] International Organization for Standardization. ISO/IEC 19005-1:2005: Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1). International Standard.

[JCJ05] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *WPES*, pages 61–70. ACM, 2005.

[JdV06] Hugo L. Jonker and Erik P. de Vink. Formalising Receipt-Freeness. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 476–488. Springer, 2006.

[JJR02] Markus Jakobsson, Ari Juels, and Ronald L. Rivest. Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking. In *Proceedings of the 11th USENIX Security Symposium*, pages 339–353, Berkeley, CA, USA, 2002. USENIX Association.

[Jon09] Hugo Jonker. *Security Matters: Privacy in Voting and Fairness in Digital Exchange*. PhD thesis, University of Luxembourg, October 2009.

[JP06] Hugo Jonker and Wolter Pieters. Receipt-Freeness as a Special Case of Anonymity in Epistemic Logic, 2006. IAVoSS Workshop on Trustworthy Elections (WOTE 2006).

[JSI96] Markus Jakobsson, Kazue Sako, and Russell Impagliazzo. Designated Verifier Proofs and Their Applications. In Ueli M. Maurer, editor, *EUROCRYPT*, volume 1070 of *Lecture Notes in Computer Science*, pages 143–154. Springer, 1996.

[Kar05] Ulrich Karpen. *Elektronische Wahlen? Einige verfassungsrechtliche Fragen*, volume 10 of *European Association of Legislation (EAL) / Deutsche Gesellschaft fr Gesetzgebung (DGG)*. Nomos, Baden-Baden, 2005.

[KG08] Robert Krimmer and Rüdiger Grimm, editors. *3rd International Conference, Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting.CC, August 6th-9th, 2008 in Castle Hofen, Bregenz, Austria*, volume 131 of *LNI*. GI, 2008.

[KOV07] Thomas Kunz, Susanne Okunick, and Ursula Viebeg. *Long-term security for signed documents: services, protocols, and data structures*, pages 125–139. Nova Publishers, 2007.

[KSW05] Chris Karlof, Naveen Sastry, and David Wagner. Cryptographic Voting Protocols: A Systems Perspective. In *Proceedings of the Fourteenth USENIX Security Symposium (USENIX Security 2005)*, pages 33–50, August 2005. `http://www.cs.berkeley.edu/~ckarlof/papers/cryptovoting-usenix05.pdf`.

[KT09] Ralf Küsters and Tomasz Truderung. An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy (S&P)*, pages 251–266, Washington, DC, USA, 2009. IEEE Computer Society.

[LGT+03] Costas Lambrinoudakis, Dimitris Gritzalis, Vassilis Tsoumas, Maria Karyda, and Spyros Ikonomopoulos. *Secure Electronic Voting: The Current Landscape*, volume 7 of *Advances in Information Security*, chapter 7. Kluwer Academic Publishers, 2003.

[LK02] Byoungcheon Lee and Kwangjo Kim. Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer. In Pil Joong Lee and Chae Hoon Lim, editors, *ICISC*, volume 2587 of *Lecture Notes in Computer Science*, pages 389–406. Springer, 2002.

[LLR06] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the Composition of Authenticated Byzantine Agreement. *J. ACM*, 53(6):881–917, 2006.

[LR08] David Lundin and Peter Y. A. Ryan. Human Readable Paper Verification of Prêt à Voter. In Sushil Jajodia and Javier López, editors, *ESORICS*, volume 5283 of *Lecture Notes in Computer Science*, pages 379–395. Springer, 2008.

[Mer80] Ralph C. Merkle. Protocols for Public Key Cryptosystems. *IEEE Symposium on Security and Privacy*, 0:122–134, 1980.

[MGKQ03] Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, and Gerald Quirchmayr. *E-Voting: Constitutional and Legal Requirements and Their Technical Implications*, volume 7 of *Advances in Information Security*, chapter 4. Kluwer Academic Publishers, 2003.

[MHEA08] Gisela Meister, Detlef Hühnlein, Jan Eichholz, and Roberto Araújo. eVoting with the European Citizen Card. In Arslan Brömme, Christoph Busch, and Detlef Hühnlein, editors, *BIOSIG 2008 – Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, September 11-12, 2008, in Darmstadt, Germany*, volume 137 of *LNI*, pages 67–78. GI, 2008.

[MHR04] Nils Meißner, Volker Hartmann, and Dieter Richter. Verifiability and Other Technical Requirements for Online Voting Systems. In Prosser and Krimmer [PK04], pages 101–109.

[MN06] Tal Moran and Moni Naor. Receipt-Free Universally-Verifiable Voting with Everlasting Privacy. In Cynthia Dwork, editor, *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 373–392. Springer, 2006.

[Nef01] C. Andrew Neff. A Verifiable Secret Shuffle and its Application to E-Voting. In *CCS '01: Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 116–125, New York, NY, USA, 2001. ACM.

[Nef04] C. Andrew Neff. Practical High Certainty Intent Verification for Encrypted Votes. Draft, October 2004. `http://www.votehere.com/old/vhti/documentation/vsv-2.0.3638.pdf`.

[Oka97] Tatsuaki Okamoto. Receipt-Free Electronic Voting Schemes for Large Scale Elections. In Bruce Christianson, Bruno Crispo, T. Mark A. Lomas, and Michael Roe, editors, *Security Protocols Workshop*, volume 1361 of *Lecture Notes in Computer Science*, pages 25–35. Springer, 1997.

[OMA+99] Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. An Improvement on a Practical Secret Voting Scheme. In Masahiro Mambo and Yuliang Zheng, editors, *ISW*, volume 1729 of *Lecture Notes in Computer Science*, pages 225–234. Springer, 1999.

[Pas07] Andrea Pasquinucci. Web voting, security and cryptography. *Computer Fraud & Security*, 2007(3):5–8, 2007. `http://www.sciencedirect.com/science/article/B6VNT-4NGKDYC-8/2/49176af5eaad231b5d947845e05cb6fe`.

[Pie06] Wolter Pieters. What proof do we prefer? Variants of verifiability in voting. In *Workshop on Electronic Voting and e-Government in the UK, Edinburgh, UK*, pages 33–39, Edinburgh, 2006. e-Science Institute.

[Pie08] Wolter Pieters. *La Volonté Machinale: Understanding the Electronic Voting Controversy.* PhD thesis, Radboud University Nijmegen, January 2008.

[Pie09] Wolter Pieters. Combatting electoral traces: The dutch tempest discussion and beyond. In Peter Y. A. Ryan and Berry Schoenmakers, editors, *VOTE-ID*, volume 5767 of *Lecture Notes in Computer Science*, pages 172–190. Springer, 2009.

[PIK93] Choonsik Park, Kazutomo Itoh, and Kaoru Kurosawa. Efficient Anonymous Channel and All/Nothing Election Scheme. In Tor Helleseth, editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 248–259. Springer, 1993.

[PK04] Alexander Prosser and Robert Krimmer, editors. *Electronic Voting in Europe – Technology, Law, Politics and Society, Workshop of the ESF TED Programme together with GI and OCG, July 7th-9th, 2004, in Schloß Hofen / Bregenz, Lake of Constance, Austria, Proceedings*, volume 47 of *LNI*. GI, 2004.

[Rei95] Michael K. Reiter. The Rampart Toolkit for Building High-Integrity Services. In *Selected Papers from the International Workshop on Theory and Practice in Distributed Systems*, pages 99–110, London, UK, 1995. Springer-Verlag.

[RFDJ07] Alexander Roßnagel, Stefanie Fischer-Dieskau, and Silke Jandt. *Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente*, August 2007. http://www.bmwi.de, last checked 25.02.2008.

[RFDJK07] Alexander Roßnagel, Stefanie Fischer-Dieskau, Silke Jandt, and Michael Knopp. *Langfristige Aufbewahrung elektronischer Dokumente – Anforderungen und Trends*, volume 17 of *Schriftenreihe "'Der elektronische Rechtsverkehr"'*. Nomos, Baden-Baden, 2007.

[Rie98] Andreu Riera. An Introduction to Electronic Voting Schemes. Technical Report PIRDI-9/98, Universitat Autònoma de Barcelona, October 1998.

[Rii02] Riigikogu Election Act. RT I 2002, passed on June 12, 2002. `http://www.vvk.ee/public/dok/RKseadus_eng.pdf`.

[Riv06] Ronald L. Rivest. The ThreeBallot Voting System. `http://theory.csail.mit.edu/~rivest/Rivest-TheThreeBallotVotingSystem.pdf`, Oct 2006.

[RP05] Peter Y. A. Ryan and Thea Peacock. Prêt à Voter: a Systems Perspective. Technical Report CS-TR-929, Newcastle University, School of Computing Science, Sept 2005. `http://www.cs.ncl.ac.uk/publications/trs/papers/929.pdf`.

[RS06a] Alexander Roßnagel and Paul Schmücker, editors. *Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit?* Economica, 2006.

[RS06b] Peter Y. A. Ryan and Steve A. Schneider. Prêt à Voter with Re-encryption Mixes. In Dieter Gollmann, Jan Meier, and Andrei Sabelfeld, editors, *ESORICS*, volume 4189 of *Lecture Notes in Computer Science*, pages 313–326. Springer, 2006.

[RSA83] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 26(1):96–99, 1983.

[Rya05] Peter Y. A. Ryan. A Variant of the Chaum Voter-verifiable Scheme. In *WITS '05: Proceedings of the 2005 workshop on Issues in the theory of security*, pages 81–88, New York, NY, USA, 2005. ACM.

[Rya08] Peter Y. A. Ryan. Prêt à Voter with Paillier Encryption – extended journal version. Technical Report CS-TR-1114, Newcastle University, School of Computing Science, July 2008. `http://www.cs.ncl.ac.uk/publications/trs/papers/1114.pdf`.

[Sch90] Wolfgang Schreiber. *Handbuch des Wahlrechts zum Deutschen Bundestag: Kommentar zum Bundeswahlgesetz*. Heymann, Köln, 1990.

[Sch91] Claus-Peter Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174, 1991.

[Sch00] Berry Schoenmakers. Fully Auditable Electronic Secret-Ballot Elections. *Xootic magazine*, 8(1):5–11, July 2000. `http://www.xootic.nl/magazine/jul-2000/schoenmakers.pdf`.

[Sha79] Adi Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[SK95] Kazue Sako and Joe Kilian. Receipt-Free Mix-Type Voting Scheme – A Practical Solution to the Implementation of a Voting Booth. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *EUROCRYPT*, volume 921 of *Lecture Notes in Computer Science*, pages 393–403. Springer, 1995.

[Smi05] Warren D. Smith. Cryptography meets voting, September 2005. `http://www.math.temple.edu/~wds/homepage/cryptovot.pdf`.

[SP06] Krishna Sampigethaya and Radha Poovendran. A framework and taxonomy for comparison of electronic voting schemes. *Computers & Security*, 25(2):137–153, 2006.

[SRKK09] Ben Smyth, Mark D. Ryan, Steve Kremer, and Mounira Kourjieh. Election verifiability in electronic voting protocols (Preliminary version). In Olivier Pereira, Jean-Jacques Quisquater, and François-Xavier Standaert, editors, *Proceedings of the 4th Benelux Workshop on Information and System Security (WISSEC'09)*, Louvain-la-Neuve, Belgium, 2009. `http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/SRKK-wissec09.pdf`.

[VG08] Melanie Volkamer and Rüdiger Grimm. Development of a Formal IT Security Model for Remote Electronic Voting Systems. In Krimmer and Grimm [KG08], pages 185–196.

[VH04] Melanie Volkamer and Dieter Hutter. From Legal Principles to an Internet Voting System. In Prosser and Krimmer [PK04], pages 111–120.

[VK06] Melanie Volkamer and Robert Krimmer. Secrecy forever? Analysis of Anonymity in Internet-based Voting Protocols. In *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*, pages 340–347, Washington, DC, USA, 2006. IEEE Computer Society.

[Vol08] Melanie Volkamer. *Evaluation of Electronic Voting. Requirements and Evaluation Procedures to Support Responsible Election Authorities.* PhD thesis, Universität Koblenz-Landau, 2008.

[VSL+09] Melanie Volkamer, Guido Schryen, Lucie Langer, Axel Schmidt, and Johannes Buchmann. Elektronische Wahlen: Verifizierung vs. Zertifizierung. In Stefan Fischer, Erik Maehle, and Rüdiger Reischuk, editors, *GI Jahrestagung*, volume 154 of *LNI*, pages 1827–1836. GI, 2009.

[VV08] Melanie Volkamer and Roland Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008. `https://www.bsi.bund.de/cae/servlet/`

contentblob/480286/publicationFile/29305/pp0037b_engl_pdf.pdf.

[WAB07] Stefan G. Weber, Roberto Araújo, and Johannes Buchmann. On Coercion-Resistant Electronic Elections with Linear Work. In *ARES '07: Proceedings of the The Second International Conference on Availability, Reliability and Security*, pages 908–916, Washington, DC, USA, 2007. IEEE Computer Society.

[Wil02] Martin Will. *Internetwahlen – Verfassungsrechtliche Möglichkeiten und Grenzen*, volume 2 of *Recht und neue Medien*. Richard Boorberger Verlag GmbH & Co, 2002. Institut für Öffentliches Recht, Philipps-Universität Marburg.

[XS06] Zhe Xia and Steve Schneider. A New Receipt-Free E-Voting Scheme Based on Blind Signature (Abstract), 2006. IAVoSS Workshop on Trustworthy Elections (WOTE 2006).

[ZLH08] Wolf Zimmer, Thomas Langkabel, and Carsten Hentrich. Archisafe: Legally compliant electronic storage. *IT Professional*, 10(4):26–33, 2008.