Classifying Privacy and Verifiability Requirements for Electronic Voting

Lucie Langer, Axel Schmidt, Melanie Volkamer, Johannes Buchmann
CASED
Technische Universität Darmstadt
{langer, axel, buchmann}@cdc.informatik.tu-darmstadt.de, volkamer@cased.de

Abstract: Voter privacy and verifiability are fundamental security concepts for electronic voting. Existing literature on electronic voting provides many definitions and interpretations of these concepts, both informal and formal. While the informal definitions are often vague and imprecise, the formal definitions tend to be very complex and restricted in their scope as they are usually tailored for specific scenarios. Moreover, some of the existing interpretations are contradictory.

This paper provides informal, yet precise definitions of anonymity, receipt-freeness and coercion-resistance and identifies different levels of individual and universal verifiability. The overarching goal of this paper is to investigate which levels are conceivable for implementing these requirements in e-voting systems for elections of different significance (for instance political elections vs. elections in associations).

1 Introduction

A fundamental objective for democratic elections is secrecy of the vote. It requires that only the voter knows his voting decision and nobody else is able to gain information about it. For federal elections of the German Bundestag, this objective is even laid down in German Constitutional Law, which emphasizes its importance. Secrecy of the vote is also a precondition of casting one's vote freely and without coercion [MGKQ03]. If the voter fears that his decision becomes public in the future, the freedom of vote is clearly limited. Therefore it is important that the voter's decision remains secret also in the long term, i.e. when a dozen years or more have passed since the election. German Constitutional Law even requires the secrecy of the vote to hold forever [Wil02].

Recently, the use of specific electronic voting machines in the last federal election of the German Bundestag was ruled unconstitutional by the German Federal Constitutional Court [Cou]. The reason for this decision was that the voting machines used failed to provide a sufficient level of verifiability. In particular, the judgement claims that the voter must be able to verify that his vote was recorded as intended without having detailed knowledge of computer technology. This shows the importance of verifiability for legally binding electronic elections.

From a more technical point of view, there is an established set of *security requirements* for electronic voting [Rie98, BM03, JdV06, Cet07]. The legal terms of secrecy and freedom of vote on the one hand and verifiability on the other hand can be mapped to these requirements as follows: According to [VH04], “the legal objectives of free and secret elections are related to anonymity, receipt-freeness and coercion-resistance of electronic voting”. Thus, to ensure secrecy and freedom of vote, voting schemes should strive for anonymity, receipt-freeness and coercion-resistance, preferably in the long term. The legal obligation for verifiability is captured by the security requirements in two different forms: While individual verifiability refers to the individual voter, universal verifiability refers to the public.

Existing literature on electronic voting provides many definitions and interpretations of these security requirements. While the informal definitions tend to be sketchy and imprecise, the formal definitions usually are very complex and tailored for specific scenarios given by specific voting protocols or assuming particular attack models. Moreover, the extent of the security requirements considered is understood differently and some of the existing interpretations are even contradictory.

Our paper provides informal, yet precise definitions of individual and universal verifiability, anonymity, receipt-freeness and coercion-resistance. The goal is to make a first step towards providing an overview of the different levels which are conceivable for implementing the security requirements for electronic voting in practice. The result can support persons in charge (e.g. election hosts) in deciding which level of the respective requirement they want to meet with regard to the priority of either verifiability or voter privacy.

The paper is structured as follows. In Section 2 we review existing definitions and interpretations of the requirements under consideration. Section 3 provides our definitions and classifications. The relations between the requirements are analyzed in Section 4. Section 5 summarizes and concludes the paper.

2 Review of Existing Definitions and Interpretations

2.1 Privacy Requirements

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 information about any voter’s decision than what is leaked by the tally [CMFP$^+$06, MN06]: If all voters vote identically, then it is clear how each voter voted. The notions of (voter) privacy and (ballot) secrecy are often used synonymously [Hir01, CRS05, MN06]; some authors refer to anonymity instead [Rie98]. Hirt distinguishes between secrecy and anonymity: While secrecy is defined as the infeasibility to assign votes to voters, anonymity refers to the impossibility to tell whether a certain voter voted or not [Hir01]. The need for long-term voter privacy is usually neglected. Only [CMFP$^+$06, MN06, Cet07] incorporate this temporal aspect in their definition of privacy. Chevallier-Mames et al. point out this property by using the expression “unconditional privacy” [CMFP$^+$06], Moran and Naor use “everlasting privacy” [MN06].

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]. Uncoercibility is in general 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 uncoercible if "no voter can prove that he voted in a particular way" [Rie98] and hence takes uncoercibility for what generally is understood as receipt-freeness. Moran and Naor provide a very strong notion of receipt-freeness [MN06]: The adversary can coerce the voters 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 [CMFP$^+$06]. They also assume that the adversary can tap the channel between the voter and the voting authority.

In contrast to this, Hirt states that receipt-freeness cannot be achieved without some physical assumptions, the weakest assumption being one-way untappable channels from the authorities to the voters. Similarly, Juels et al. state that anonymous channels are a minimal requirement for any coercion-resistant scheme: "An attacker that can identify which voters have participated can obviously mount a forced-abstention attack" [JCJ05]. According to Hirt, "the concept of incoercibility is weaker than receipt-freeness" [Hir01]. This assertion is also made 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 uncoercible and yet not receipt-free.

However, the relation between receipt-freeness and uncoercibility is usually understood contrarily: Uncoercibility is stronger than receipt-freeness [JCJ05, Smi05, Cet07, DKR09, KT09]. According to [DKR09] and [KT09], uncoercibility even implies receipt-freeness, which is formally proven by the authors. [KT09] uses a symbolic setting based on an epistemic approach, while [DKR09] makes use of the applied pi calculus. However, their definition of coercion-resistance does not consider randomization and forced abstention attacks as introduced in [JCJ05]. Juels et al. provide formal definitions of coercion-resistance and (universal) verifiability [JCJ05]. Their definitions hinge on several experiments involving an adversary in interaction with components of the voting system.

2.2 Verifiability Requirements

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 votes [Rie98, CRS05, Smi05]. [Rie98], [BM03] and [LGT$^+$03] also take into account the chance for open objections made by the voter without sacrificing privacy.

Universal verifiability can be summarized as the possibility for any observer to check that the tally has been correctly computed. Some authors include the property that the tallied votes were cast by legitimate voters in the notion of universal verifiability [Smi05, Hir01], others do not [Hir01, MN06]. Universal verifiability is closely related to accuracy, i.e. the requirement that no vote can be altered, duplicated or eliminated [Rie98, BM03].

Cetinkaya states that verifiability is “the provability that the election is accurate” [Cet07]. Thus, Cetinkaya argues that universal verifiability is not an e-voting security requirement on its own, because “if a protocol claims that it satisfies accuracy, it should be able to prove its claim” [Cet07].

Karlof et al. use the notions “cast as intended” and “counted as cast” and postulate verifiability for both: The voter should be able to verify that his ballot indeed represents the vote cast, and everyone should be able to verify that the final tally is an accurate count of the ballots cast [KSW05]. Benaloh introduces the notion of “end-to-end-verifiability”: “Voters and any other interested parties also gain the capability to check that all votes are associated with legitimate voters and are properly tallied” [Ben06]. Thus, individual and universal verifiability are not distinguished.

With regard to the relation between universal and individual verifiability, [LGT$^+$03] and [BM03] state that individual verifiability (or “atomic” verifiability as named in the latter) is weaker than universal verifiability. This perception can be explained by the fact that Burmester and Magkos have a strong understanding of universal verifiability: “Any observer can be convinced that the election is accurate and that the published tally is correctly computed from votes that were correctly cast” [BM03].

Formal definitions of universal verifiability have been provided in [JCJ05, CMFP$^+$06]; they are not further discussed here.

3 Definitions and Classifications

In the following we provide definitions and classifications of privacy and verifiability requirements for electronic voting schemes. The definitions are informal enough to be understood by readers without detailed technical knowledge in order to allow for an interdisciplinary discussion, and yet precise enough to capture any logical relations, for example the implications shown in [DKR09] and [KT09]. We assume the existence of a public bulletin board as this is a fundamental means to ensure individual and universal verifiability in e-voting.

3.1 Bulletin Board, Ballot and Vote

A **bulletin board** is a public channel where data can be published by authorized participants only and, once published, cannot be erased or overwritten by anyone. This communication model was first presented by Benaloh et al. [CF85, Ben87] and supports verifiability in electronic voting schemes.

In the following, a **ballot** denotes the message which is issued by the voter in order to cast a **vote** for a specific candidate. The ballot could for example be an encryption of the vote.

3.2 Anonymity, Receipt-freeness and Coercion-resistance

We subsume anonymity, receipt-freeness and coercion-resistance under the superordinate concept of **privacy**. Depending on the connection between the adversary and the voter as introduced in [KT09], we distinguish the following levels of voter privacy:

Anonymity. The vote cannot be linked to the voter who cast it. There is no communication channel between the voter and the adversary. The adversary can only use the information published on the bulletin board.

Receipt-freeness. The voter cannot prove to an adversary how he voted. There is a one-way communication channel from the voter to the adversary: The voter can send messages to the adversary but the adversary cannot send messages to the voter. Additionally, the adversary can use the information published on the bulletin board.

Coercion-resistance. The adversary cannot coerce the voter to vote in a particular way. There is a two-way communication channel between the voter and the adversary: Both voter and adversary can send messages to each other. Additionally, the adversary can use the information published on the bulletin board.

If we do not assume the use of voting booths, then privacy is usually achieved by cryptographic means. It is well known that cryptosystems which provide only computational security may be broken at some point in the future, e.g. by brute force attacks based on increased computational power or by solving an underlying mathematical problem that is widely believed, though unproved, to be hard. Thus, each of the properties defined above can possibly apply in the long term or in the short term.

We define **in the short term** to be a period of up to ten years as it is reasonable to assume that cryptographic algorithms remain secure at least for this period of time if the underlying parameters (e.g. keylength) are chosen properly. This should also cover the legislative period of the elected body in most cases. By contrast, **in the long term** refers to the time when 20 years or more have passed since the election was carried out. Cryptographic primitives used e.g. for encryption will possibly have been broken at that time. It might be argued that a voter's decision will not be a matter of interest 20 years later. However, when it comes to e-voting in parliamentary elections, long-term anonymity may indeed be required.

3.3 Individual and Universal Verifiability

For the classification of individual verifiability we use a similar approach as introduced in [Pie06]. Pieters distinguishes classical and constructive individual verifiability depending on whether the voter can reconstruct his vote from the information provided. We distinguish weak, average and strong individual verifiability. Furthermore, for each of these levels we distinguish if individual verifiability is restricted to the voting phase **before** tallying and thus to the vote **cast** by the voter, or if it extends to the phase **after** tallying and thus to the vote **counted** for the voter.[1] These two variants are indicated in the following by the terms before / after and cast / counted.

Weak individual verifiability before / after tallying. The voter can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. There is no verifiability or proof provided regarding the question whether the ballot has been cast / counted as intended.

Average individual verifiability before / after tallying. The voter can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. Additionally, he is furnished with a proof that the ballot has been cast / counted as intended. The voter cannot verify the correct content of the ballot in terms of reconstructing the vote from the information he is provided with.

Strong individual verifiability before / after tallying. The voter can verify that his ballot has been cast / counted, i.e. is published on the bulletin board before / after tallying. Additionally, he can verify that the ballot has been cast / counted as intended by reconstructing the vote from the information he is provided with.

The voter's chance of objection in case the ballot has not been cast as intended (or, for a stronger version, not counted as intended) can be classified as follows: An **anonymity-compromising chance of objection** is given if the voter is not able to do an open objection without sacrificing anonymity. An **anonymity-preserving chance of objection** is given if the voter is able to do an open objection without sacrificing anonymity.

We distinguish weak, average and strong universal verifiability as follows:

Weak universal verifiability. Any interested party can verify that the tally is correctly computed from votes that were counted. Only the last step of the election procedure can be verified, i.e. the correct tallying of the votes contained in the ballot box immediately before the tallying phase.

Average universal verifiability. Any interested party can verify that the tally is correctly computed from votes that were cast.

Strong universal verifiability. Any interested party can verify that the tally is correctly computed from votes that were cast by legitimate voters.

4 Analysis

Due to our definitions (and following [DKR09, KT09]), coercion-resistance implies receipt-freeness, and receipt-freeness implies anonymity: The existence of a two-way communication channel between the voter and the adversary (scenario of coercion-resistance) is

[1] It might be argued that you cannot speak of individual verifiability unless the voter is able to verify that his vote has been included in the tally. However, our goal is to provide all possibilities which are conceivable.

equivalent to two one-way channels and thus clearly implies the existence of a one-way channel between the voter and the adversary (scenario of receipt-freeness). Intuitively, the adversary has more capabilities in the scenario of coercion-resistance than in the scenario of receipt-freeness. This holds for the relation between receipt-freeness and anonymity as well: If the voter voluntarily provides the adversary with information in addition to the one which is public, then the adversary has more capabilities than when his knowledge is restricted to public information (e.g. the final tally).

In contrast to our perception, [Hir01] and [BM03] claim that coercion-resistance is weaker than receipt-freeness and that it is possible to have a voting scheme which is coercion-resistant and not receipt-free. Burmester and Magkos give the example of deniable encryption, which allows a voter to lie about his encrypted vote, but cannot prevent him from proving his vote if he intends to do so [BM03]. According to Juels et al. this is not true: Deniable encryption does not protect against coercion as the adversary can furnish the voter with pre-determined parameters [JCJ05]. This is also consistent with our definition of coercion-resistance: The adversary can use the two-way channel to provide the voter with the parameters he wants him to use. The understanding of receipt-freeness being stronger than uncoercibility can be explained by the intuitive conception that it is harder to take countermeasures against a voter who *wants* to cooperate with a coercer.

With regard to our classification of individual verifiability, the variant after tallying is clearly stronger than the one before tallying. If the proof provided for average individual verifiability after tallying is transferable (i.e. the voter can use it to prove the vote contained in the ballot to an adversary), then this property is not simultaneously achievable with receipt-freeness. This corresponds to the assertion by Cetinkaya that there is a trade-off between receipt-freeness and individual verifiability: If a voting system provides any receipt enabling the voter to verify his vote in the final tally, then that receipt can also be used for vote selling [Cet07]. Similarly, Lambrinoudakis et al. identified the conflict between individual verifiability and uncoercibility [LGT$^+$03].

Regarding our classification of universal verifiability, strong universal verifiability implies average universal verifiability and average universal verifiability implies weak universal verifiability: Our definition of weak universal verifiability implies that the requirements of accuracy and democracy[2] may be violated without detection: Altered or duplicated votes may be included and votes cast by eligible voters may have been eliminated from the ballot box; multiple votes cast by eligible voters may have been counted as well as votes cast by voters who are not eligible. Average universal verifiability excludes undetected violation of accuracy, but not democracy: It is revealed if votes have been altered, duplicated or eliminated; however, multiple votes cast by eligible voters may have been counted as well as votes cast by voters who are not eligible. Only strong universal verifiability ensures that any fraud related to accuracy or democracy will be detected. Note that universal verifiability does not include verifying that the requirement of anonymity has been met.

[2] Democracy requires that only eligible voters can vote, and all voters can vote at most once [JdV06].

5 Conclusion

From a legal point of view, secrecy and freedom of vote on one hand and transparency on the other hand are fundamental objectives for democratic elections and electronic voting in particular. Secrecy and freedom of vote can be translated to the security requirements of anonymity, receipt-freeness and coercion-resistance, while transparency refers to individual and universal verifiability. It is a challenge for current voting schemes to reconcile these properties, particularly in the long term: How can individual verifibility be achieved without sacrificing anonymity and receipt-freeness or even coercion-resistance in the long term?

While for federal elections we should strive for the optimum, one could make concessions for subordinate elections. Depending on the significance and scope of the election, either a strong notion of voter privacy or verfiability might be appropriate. For instance, the long-term privacy of the vote will be important for national elections, while the receipt-freeness will not be as critical since it may be difficult to buy votes on a very large scale without detection [CMFP$^+$06]. Therefore it is important to know the possibilities which are conceivable for implementing verifiability and privacy in electronic voting systems.

We introduced an intuitive and yet precise classification of anonymity, receipt-freeness and coercion-resistance as well as individual and universal verifiability. We also defined different levels of these requirements in order to provide a basis for an interdisciplinary discussion.

We believe that an effective dialog between computer scientists and jurists is a precondition for developing secure electronic voting schemes. Thus, we hope to contribute to this interdisciplinary dialog by providing an appropriate framework for the evaluation of competing security requirements. Our classifications can in particular support the discussion to which extent the considered properties should apply to electronic elections of different significance, e.g. elections in associations or works council elections.

Acknowledgments

This work has been supported by the Center for Advanced Security Research Darmstadt (CASED).

References

[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 2006 on Electronic Voting Technology Workshop*, Berkeley, CA, USA, 2006. USENIX Association. http://www.usenix.org/event/evt06/tech/full_papers/benaloh/benaloh.pdf.

[BM03] Mike Burmester and Emmanouil Magkos. *Towards secure and practical e-elections in the new era*, chapter 5. Volume 7 of Gritzalis [Gri03], 2003.

[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. In *SFCS '85: Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, pages 372–382, Washington, DC, USA, 1985. IEEE Computer Society.

[CMFP$^+$06] Benoît Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern, and Jacques Traoré. On Some Incompatible Properties of Voting Schemes. In *Proceedings of the IAVoSS Workshop on Trustworthy Elections*, 2006.

[Cou] Federal Constitutional Court. Use of voting computers in 2005 Bundestag election unconstitutional. Press release no. 19/2009 of 3 March 2009. http://www.bverfg.de/en/press/bvg09-019en.html.

[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.

[DKR09] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Verifying Privacy-type Properties of Electronic Voting Protocols. *Journal of Computer Security*, 2009. To appear.

[Gri03] Dimitris Gritzalis, editor. *Secure Electronic Voting*, volume 7 of *Advances in Information Security*. Kluwer Academic Publishers, 2003.

[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.

[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.

[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. Technical Report arXiv:0903.0802, arXiv, 2009. An extended version of a paper from IEEE Symposium on Security and Privacy (S&P) 2009, available at http://arxiv.org/abs/0903.0802.

[LGT$^+$03] Costas Lambrinoudakis, Dimitris Gritzalis, Vassilis Tsoumas, Maria Karyda, and Spyros Ikonomopoulos. *Secure electronic voting: The current landscape*, chapter 7. Volume 7 of Gritzalis [Gri03], 2003.

[MGKQ03] Lilian Mitrou, Dimitris Gritzalis, Sokratis Katsikas, and Gerald Quirchmayr. *E-voting: Constitutional and legal requirements and their technical implications*, chapter 4. Volume 7 of Gritzalis [Gri03], 2003.

[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.

[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.

[Rie98] Andreu Riera. An Introduction to Electronic Voting Schemes. Technical Report PIRDI-9/98, Universitat Autònoma de Barcelona, October 1998.

[Smi05] Warren D. Smith. New cryptographic election protocol with best-known theoretical properties. In *Frontiers of Electronic Elections*, 2005.

[VH04] Melanie Volkamer and Dieter Hutter. From Legal Principles to an Internet Voting System. In Alexander Prosser and Robert Krimmer, editors, *Electronic Voting in Europe*, volume 47 of *LNI*, pages 111–120. GI, 2004.

[Wil02] Martin Will. *Internetwahlen - Verfassungsrechtliche Möglichkeiten und Grenzen*. Recht und neue Medien Band 2. Richard Boorberger Verlag GmbH & Co, 2002. Institut für Öffentliches Recht, Philipps-Universität Marburg.