Privacy Taxonomy for Verifiable Poll-site Voting Schemes

Bachelor-Thesis von Vladislava Arabadzhieva
Mai 2015

TECHNISCHE UNIVERSITÄT DARMSTADT

Department of Computer Science

Privacy Taxonomy for Verifiable Poll-site Voting Schemes

Vorgelegte Bachelor-Thesis von Vladislava Arabadzhieva

1. Gutachten: Prof. Johannes Buchmann
2. Gutachten: Dr. Denise Demirel

Tag der Einreichung:

Erklärung zur Bachelor-Thesis

Hiermit versichere ich, die vorliegende Bachelor-Thesis ohne Hilfe Dritter nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Darmstadt, den 26 May 2015

(Vladislava Arabadzhieva)

Contents

List of Tables

List of Figures

1 Introduction

Voting is a democratic process in our society that dates from centuries. It has evolved throughout the years to the form as we know it today: voters go to the polling stations, receive ballots with candidates' names, and secretly mark the desired ones. Then, the votes are collected and counted and the results are published. A new form of improvement that has evolved in the last decades is moving from the traditional paper-based poll-site voting to electronic poll-site or even remote voting schemes. However, the new approaches should also meet certain security requirements, in order to provide a secure voting process. One of them is privacy that demands that voters submit their votes in a way that nobody else can gain information about them. Voters should not be able to prove their votes to others and votes themselves should not link to the corresponding voters. They should also be secured against coercers trying to impose their own choices. Moreover, voter privacy should be preserved not only during the voting process, but also afterwards. Voters' identities and their corresponding votes should be kept private for a certain period of time after the voting process or even eternally.

Various poll-site voting schemes have been developed proposing solutions to the problem of privacy and improvements to already existing schemes have been made. However, the efforts to develop voting schemes that satisfy as many security properties as possible often result in trading one property for another. Therefore, different levels of privacy are usually achieved and taxonomies have been developed that allow to analyze, classify, and compare voting schemes according to this criterion. Furthermore, they can be used to identify the most appropriate scheme with respect to privacy.

The goal of this bachelor thesis is to propose a privacy taxonomy for verifiable poll-site voting schemes. We achieve that by following four main steps. We start with presenting several already existing privacy taxonomies with their characteristics, advantages, and disadvantages. They classify voting schemes with respect to perfect privacy, the way voters submit their votes, linkability of a voter and his vote, formal methods, and cryptographic primitives. We analyze the different aspects of privacy they cover and the different privacy levels they define. We then order the presented taxonomies according to their precision which allows us to distinguish their advantages and disadvantages. Then, based on the results of this comparison, we improve the taxonomy we find most precise. One aspect missing in all approaches are the trust assumptions made by the schemes. This is an important aspect, since privacy is provided only if these assumptions hold true. To close this gap, we show how to extend the selected taxonomy by a scope of trust and how this should influence the privacy level achieved. Finally, in our conclusion we suggest several ideas for future work.

Structure overview

This bachelor thesis is structured as follows. First, in Section 2 we present the fundamental terminology used in the thesis. Then, in Section 3 several already existing taxonomies are described, which are then evaluated and compared in Section 4. In Section 5 we present a taxonomy which does not explicitly consider voting systems but introduces the concept of scope of trust. Our approach for a privacy taxonomy is described in Section 6. In Section 7 we make our conclusion and suggest several ideas for future work.

2 Terminology

Before analyzing and improving existing privacy taxonomies, we provide the definitions of the terms used in this thesis. We define certain privacy requirements, which voting schemes should satisfy, and categorize them according to the categorization by Sampigethaya and Poovendran [1], dividing them in two groups: general security requirements and adversary counter-attack requirements. Then, we provide a definition of several security requirements which are not related to privacy, but frequently used in this thesis.

General security requirements

With respect to privacy this class of requirements consists of *voter privacy*, *long-term privacy*, and *everlasting privacy*.

Voter privacy ensures that all votes are cast anonymously and is tightly connected with untraceability/ unlinkability between a vote and a voter. In other words, it should be impossible to identify the voter by looking at a vote and it should be impossible to connect a voter to a vote. We talk about maximal privacy when the privacy of a voter is violated only if all other participants in the election (e.g. voters and authorities) collude.

Long-term privacy assures the privacy and untraceability between a voter and his vote for a certain period of time after the voting process.

Everlasting privacy means that even a computationally unbounded adversary can gain no information about specific votes and, hence, cannot violate voter privacy.

Adversary counter-attack requirements

This class of requirements consists of *receipt-freeness*, *coercion-resistance*, *verifiability*, and *dispute-freeness*.

Receipt-freeness: to provide verifiability of the tallying process some voting schemes hand out a receipt to the voter. However, he should not be able to prove to third parties whether or how he voted even if he wants to do so.

Incoercibility or **Coercion-resistance** is the impossibility for an adversary to force a voter to participate in the voting process in an undesired way. For example, an adversary may force a voter to abstain from voting, affect the way a vote is cast, or force a voter to cast a particular vote. However, the coercer must not know whether the voter actually obeyed or not and the voter must not be able to prove his voting behavior. Therefore, incoercibility is based on the notion of receipt-freeness, but it is a stronger requirement.

Verifiability means that a voter is able to verify whether his vote was recorded and counted correctly. We consider two types of verifiability, according to Sako and Killian [2]: individual verifiability, where a voter can verify his own vote in the tally, and universal verifiability, where anyone, even a casual observer, can verify that all valid votes were counted correctly and the tally represents the sum of all cast votes. Universal verifiability is more practical since it is not realistic for a voter to verifiy his vote individually. Moreover, verifiability is in contradiction to privacy, since it requires linkability of a voter and his vote, otherwise the voter cannot check the correctness of his vote. Still, being able to verify their votes gives the voters more trust in the voting system, because they are able to detect and react to inconsistencies.

Dispute-freeness means that any person, even a casual observer, can publicly verify that all vot-

ers follow the protocol at any stage of the voting process. This requirement is an extension to universial verifiability, where votes are verifiable only at the voting and tallying stages.

3 Existing taxonomies

3.1 The idea of perfect privacy by Coney et al.

In this section we consider the paper by Coney et al. [3]. The authors provide a definition of perfect privacy and perfect ballot secrecy in electronic and non-electronic voting schemes. While perfect privacy only focuses on the information leakage of electronic technology and process/procedures, perfect ballot secrecy also considers that the voter colludes with the adversary. As a criterion for a privacy taxonomy they suggest an entropy-based measuring of the deviation from perfect privacy, using Shannon entropy [4].

3.1.1 Perfect privacy and ballot secrecy

This section deals with defining what a perfectly private voting system is. We first give the authors' more common definition and after that provide their more formal one. Next, we see how they define ballot secrecy.

According to the authors, a voting system is perfectly private if the way a voter votes does not affect the amount and the type of information an adversary can get about this vote. In other words, if an adversary could learn something about the probable voter's choice through information leakage, he could learn the same information even if the voter casts some other vote. More precisely, let the variables V, S, and E be defined as follows:

- V be a random variable denoting the voter's vote as actually cast
- S be the information collected by the adversary through sources other than the voting system (e.g. geographical location, race, etc.)
- E be the information revealed to the adversary by the voting system and process (e.g. information available to poll workers, information stored in any permanent form, or information revealed through/due to the used voting technology and poll place procedures)

In addition, the authors use the notation p_x to denote the probability distribution of a random variable X. Then, they express perfect privacy as follows:

$$p_{V|S}(\boldsymbol{\nu}; s) = p_{V|S,E}(\boldsymbol{\nu}; s, e) \forall \boldsymbol{\nu}, s, e, \tag{1}$$

which means that in a perfectly private voting system the voter's actual vote is conditionally independant of E after conditioning on S. Here, we do not consider any kind of voter's collusion with the adversary or coercion. Any kind of information which the adversary receives is leaked without the voter's participation.

For a more realistic view of a voting system the authors provide a definition considering the possibility of voter coercion and vote buying. Even in the presence of such attacks, it should be impossible for a voter to prove his vote. More precisely, an election system has perfect voter privacy if it is perfectly private even when the voter is in collusion with the adversary and wishes to prove how he voted to the adversary.

3.1.2 Deviation from perfect privacy as a criterion for classifying voting schemes

In the following we show what deviation from perfect privacy means, according to the authors. We then show how they bind it with privacy loss and present their numerical measure for measuring privacy loss.

As mentioned above, a perfectly private system does not reveal any information about a voter's vote. Every system that leaks information has levels of privacy, lower than those of a perfectly private system. This privacy loss can be expressed formally as how much $p_{V|S,E}$ differs from $p_{V|S}$, as previously defined.

We can assume that in a voting system the closer the level of achieved privacy is to that of perfect privacy, the less likely it is for an adversary to guess correctly how a voter voted. This means that the adversary is less certain about the voter's vote, since the voting system reveals very little or even no information about the voter's choice. Otherwise, in voting systems with privacy levels far lower than those of perfect privacy an adversary can get a lot more information and, therefore, certainty about the voter's choice. The authors state that the reduction in uncertainty by lower levels of privacy according to perfect privacy can be due to information leakage from the voting system and process ($p_{V|S,E}$). They also suggest that it can be due to sources different from the voting system and process ($p_{V|S}$). However, a voting system should not be considered "good" simply because knowledge of E does not reveal much information about the voter's vote. This can also be a result of a very small initial uncertainty in the vote. For instance, voters having certain political interests tend to vote similarly which makes their choices predictable with high probability. Moreover, the system may be deployed in a way that no advanced knowledge of $p_{S|V}$ or p_V is available. Consequently, the authors consider the worst-case uncertainty reduction of $p_{V,S}$ to define the amount of privacy loss. They define it as the maximum reduction in uncertainty of a voter's vote, due to information revealed by the election system and process. Numerically, this uncertainty (in a random variable X) can be expressed by Shannon entropy [4]:

$$H(X) = -\sum_{x} p_X(x) lg p_X(x) \tag{2}$$

The entropy $H(X)$ can be seen as the minimum number of bits required, on average, to represent variable X. Then, the authors measure the amount of privacy loss L of a voting system and process as

$$L = max_{p_{V,S}} H(V|S) - H(V|S,E), \tag{3}$$

where $p_{E|V}$ is hold fix and $p_{V,S}$ varies. $H(V|S) - H(V|S,E)$ is the conditional mutual information between the vote and E, conditioned on S, and is always non-negative. To measure the amount of privacy left after using a voting system for N votes, one computes

$$H(V|S,E) \geq H(V|S) - N \times L \tag{4}$$

However, note that this is not a tight bound, since a maximum reduction of entropy for each vote is difficult.

3.2 Framework and taxonomy by Sampigethaya and Poovendran

In contrast to using the deviation from perfect privacy as a criterion for a privacy taxonomy as shown above, the paper by Sampigethaya and Poovendran [1] suggests considering how voters submit their votes to the tallying authority. The authors provide a framework for classifying the different approaches and comparing their properties according to predefined characteristics. Thus, differences in the security properties among the classes can be observed and voting schemes can be selected and designed to satisfy certain application requirements. The authors distinguish the following three general types of voting schemes according to the way the voters submit their votes:

- Hidden voter: The voters anonymously submit votes
- Hidden vote: The voters openly submit encrypted votes
- Hidden voter with hidden vote: The voters anonymously submit encrypted votes

In the following sections the hidden voter, the hidden vote, and the hidden voter with hidden vote classes of voting schemes are discussed. First, the main characteristics of each class, as well as the corresponding division in subclasses are presented. Then, example poll-site voting schemes are given and, finally, based on the authors' contemplations, the features of each subclass are highlighted.

3.2.1 Hidden voter

In voting schemes from the hidden voter class, as the name suggests, the voter remains anonymous. This is achieved by submitting the vote using an anonymous channel [5]. It conceals the voter's identity from the receiving party, in this case: the tallying authority. The vote itself is not encrypted. A class of voting schemes where votes are submitted in an encrypted form, the hidden vote class, is discussed in Section 3.2.2. However, if submitted in clear to the anonymous channel, the vote could be forged and could lose accuracy. Therefore, a secure and where appropriate also encrypted communication between the voter and the anonymous channel is established. The anonymous channel publishes additional information which allows to publicly verify the correctness of the recorded votes output by the channel. Moreover, the tally can be recomputed by everyone.

To ensure accuracy in the voting process, all participating voters must be eligible to vote and the votes of not eligible voters must not be counted as valid. In the hidden voter class of voting schemes voters can identify themselves in two ways: using a token in the form of an encryption key [6] or using a bulletin board [7]. As a result, voting schemes in this class can be categorized in two subclasses: token-based schemes and bulletin board based schemes. These categories are, however, only suitable for online voting schemes. Since the focus of this thesis are poll-site voting schemes, they will not be further discussed.

An example of a poll-site voting scheme from this class is the common voting process in a voting booth. The voters cast in an urn their ballots which contain the votes in plaintext. At the end of the voting process the votes are counted and the tally is computed. Here, the anonymous channel is realized through the ballot urn, which is shaken before computing the tally. In this way it is avoided that the last ballots that were cast are on the top and the first ones - at the bottom of the pile. In other words, the possible linkability between a voter and his vote is avoided and voter privacy is preserved.

3.2.2 Hidden vote

In hidden vote schemes voters submit encrypted votes without remaining anonymous. Therefore, unlike in hidden voter schemes, no anonymous channels are required. Generally, hidden vote schemes use a publicly accessible bulletin board, where the voters, after authenticating themselves, cast their votes in an encrypted form $E_k(v_j, r_j)$. Having in mind that the voters are not anonymous, it is necessary to encrypt the votes, in order to keep privacy. The encryption uses the public key of a probabilistic homomorphic encryption scheme. It makes it possible to add [8], [9] or multiply [10] encrypted messages (in our case: the votes) without decrypting them and to receive an encrypted result. In poll-site voting schemes, casting the vote can be done by scanning the ballot or by using a voting machine. Since all votes must comply with a predefined format, vote validity should be verified before further computations. In case of using a voting machine, the verification is done by the machine itself. By scanning, non-conformity of the votes can be indicated by a failure message.

An example of a hidden vote voting system is Scratch & Vote [11]. After authenticating himself the voter receives a ballot with a randomized list (permutation) of the candidates, unknown to the authorities. It contains all the information necessary for voting, so no communication with the authorities is required. The ballot is perforated vertically in the middle, so that the permuted names of the candidates remain on the left and the places to mark the desired vote - on the right. On the right, there is also a 2D-barcode and a scratch surface bellow it. The scratch surface can be separated through a perforation from the rest of the right side. In the voting booth, the voter first marks the desired vote on the right hand side. Then, he separates the two halves of the ballot and puts the left one in a receptacle, where all left parts are collected. It is important to mention that there is no identifying information on this side. A 2D-barcode at the bottom of the right side contains a machine-readable encryption of the candidates ordering. In this way the correspondence between the marked area and a candidate could be established. The voter then scans his vote together with the encryption of the candidate permutation and takes it as a receipt. He can also take an additional ballot for an audit. By removing the scratch field it can be checked whether the encrypted information matches the candidate order on the ballot. A ballot used for auditing cannot be used for voting. All the encrypted votes are then published on an online bulletin board, where they can be verified by everybody. The tallying authority then verifies the proofs of correctness of the votes and computes the encrypted sum of all valid encrypted votes through homomorphic encryption. Finally, the tallying authority decrypts the sum and posts it, together with a proof of decryption, on the bulletin board, where it can be again verified by everbody. Consequently, like bulletin board based hidden voter schemes, hidden vote schemes also achieve universal verifiabilty.

Hidden vote schemes are divided in three subclasses according to the public key of the homomorphic encryption: vote threshold schemes, authority key threshold schemes, and voter key threshold schemes.

Vote threshold schemes

In this paragraph the idea of vote threshold voting schemes is discussed. The Split-Ballot voting scheme [12] is suggested as an example for a poll-site voting scheme from this class.

Vote threshold schemes use the idea of (t, k) secret sharing [13]. A secret (e.g. a vote) is segmented into k shares and k authorities receive one share each, encrypted with the corresponding

authority's public key. The vote can be reconstructed only when at least t authorities participate together, which means that a single share cannot reveal the vote. Each of the authorities computes through homomorphic encryption the partial tally of all the votes it received. It then decrypts it and adds it to the partial tallies of all other authorities, so that the final tally is computed.

An example in this category is the Split-Ballot voting scheme [12]. Here, the vote is divided between two independent authorities. Each of them prepares two pages for each voter. The voter then chooses one page from each authority and forms uniquely his vote. The other two pages can be used as an audit. More precisely, each ballot consists of three pages that are stacked on top of each other for voting. The first one has been generated by the first authority and contains a list of all candidates' names and their corresponding abbreviations. On the second one, generated by the second authority, there is a table with permutations of the candidates' abbreviations. The number of columns and rows in the table is equal to the number of candidates. The third page contains scannable bubbles, where the voter can mark the desired choice. Holes are cut in the pages, so that when they are stacked together a random column from the table is visible, as well as the scannable bubbles. In this way, the voter can mark the bubble corresponding to the desired candidate. The permutation table is randomly selected by the first authority and the decision which column to be considered is randomly taken by the second one. Therefore, the position of the marked bubble does not reveal anything about the vote, unless the first and the second pages are also known. In this way, voter privacy is achieved and the scheme provides even long-term privacy. After choosing the desired candidate, the voter destroys the first and the second pages. He then scans the last page and keeps it as a receipt. The voter can then check on an online bulletin board that his vote was recorded correctlly. However, without the first and the second pages, he is no longer able to prove to third parties how he voted. Therefore, receipt-freeness and coercion-resistance are achieved. Moreover, since two authorities participate in the process, the scheme is more robust to corrupt behavior, considering accuracy. Accuracy is always satisfied, independant of the authorities being corrupt or not. However, in case of one corrupt authority the scheme only provides computational voter privacy and may no longer be receipt-free. If both authorities are corrupt, the scheme no longer provides receipt-freeness and voter privacy.

Authority key threshold schemes

In authority key threshold schemes votes are encrypted with the public key K of the tallying authority. These schemes use a (t,k)-verifiable secret sharing scheme [14], as several authorities share a common decryption key. This makes the voting system more robust. However, the votes are no longer divided into shares. One representative of this subclass is the previously described voting scheme Scratch & Vote.

Voter key threshold schemes

In this part the authors' motivation for defining the class of voter key threshold schemes is shown. The scheme by Schoenmakers [15] is used as an example of this class.

The authors distinguish voter key threshold schemes as the only category of hidden vote schemes which satisfies dispute-freeness, as described in Section 2. Schemes in this category require a minimum number of voters to participate in the voting process, so that the tally is computable. Voters act as authorities and participate in private keys generating and sharing. These keys are then used for vote encryption. According to Schoenmakers [15], these schemes are appropriate for small

elections only, as they lack a separate authority.

In his scheme, Schoenmakers [15] suggests using a publicly verifiable (t, n) secret sharing scheme for sharing a secret s_j between n voters. The voters use these secrets as their private keys to encrypt their votes. Each voter generates n shares of a secret and distributes them to n voters, including himself. Then, a voter's secret s_j is computed as the sum of all received shares from the n voters. After all votes are submitted, the tally can be computed under the assumption that a threshold number of t voters participated in the voting process and participate in the tallying procedure. If this threshold is not achieved, the tally is not computable.

3.2.3 Hidden voter with hidden vote

The authors see the class of hidden voter with hidden vote schemes as a hybrid of the two previously discussed classes. It addresses the main disadvantages of those classes: fairness in the hidden voter class and efficiency and vote format problems in the hidden vote class. As a solution, this class combines the methods used in those two classes and use an anonymous channel to submit encrypted votes. Based on the further techniques used, the schemes in the hidden voter with hidden vote class can be classified as token-based schemes, homomorphic encryption based schemes, and token and homomorphic encryption based schemes. As this bachelor thesis discusses only poll-site voting schemes, we concentrate only on the homomorphic encryption based schemes.

Homomorphic encryption based schemes

Homomorphic encryption based schemes deal with accuracy and universal verifiability. The anonymous channel can, for instance, be implemented using a verifiable re-encryption mixnet with m mixes. The authors see the type of the mixnet as the main criterion to determine the properties of the schemes.

An example for a homomorphic encryption paper-based voting scheme is Prêt à Voter [16]. Here, the ballot is in the form of a list which can be separated by a perforation down the middle. On the left-hand side there is a list of randomly ordered (mixed) candidate names and on the right-hand side - boxes to mark the chosen candidate. The right hand side also contains the candidate order in encrypted form, hidden under a scratch field. However, a single authority cannot reconstruct this information without the participation of other authorities. This could be seen as a representation of a (t, n)-threshold scheme. During the election process authorities and voters can audit random ballots to see whether they are well-formed. They check if the encrypted information about the candidate ordering matches the real candidate order on the ballot. The ballots used for auditing are no longer valid for voting. After marking the box corresponding to the desired candidate, the voter detaches and destroys the left-hand side of the ballot. The right-hand side - the marked box and the encrypted information about the candidate ordering - represents his encrypted vote. He then scans it and keeps it as a receipt. The scanning machine proves the authenticity of the receipt. All encrypted votes are then published on a bulletin board and their correctness can be verified by the receipt holders. After all votes were submitted, they are transmitted to the tallying authorities through the re-encryption mixnet. In the mixnet, the votes are re-encrypted and permuted. The main idea of the re-encryption mixnet is to anonymize the votes, meaning to destroy the link between the encrypted votes and the corresponding voters. In addition, proofs of correctness are generated and are posted on the bulletin board. During the tallying process, the authorities decrypt the votes and post a non-interactive proof of correct

decryption. Only after decrypting the votes and verifying the vote validity, the whole tally is computed and can be made public.

3.2.4 Analysis and taxonomy

In this part of the section the classes described above are analyzed and compared, considering the privacy requirements they fulfill. The relations and improvements among the classes are shown and a taxonomy is defined. Please notice, that classes' strengths and weaknesses based on the hardware and the software used during the election process, e.g. corrupt scanning machines or implementations of bulletin boards, are not discussed.

As Sampigethaya and Poovendran [1] state, hidden voter schemes provide the simplest tallying process and computations among the three classes. During the common voting process in a voting booth, described in Section 3.2.1, no encryptions, decryptions, and mixing are used. Votes are cast in plaintext and are simply counted during the tallying stage. The ballots contain only the votes and no identifying information about the voters. Consequently, long-term privacy is preserved since voters cannot be traced from their votes and are not linkable to them. This voting process is also receipt-free, since voters are not provided with any receipt for their cast vote. On one hand, this prevents them from proving to a coercer how they voted. On the other hand, however, since unlinkability between a voter and his vote exists, receipt-freeness also means that voters cannot prove their actual votes, in case they were recorded or counted wrongly. As a result, dispute-freeness and verifiability are sacrificed. Because votes are submitted in plaintext, they can be easily proven to a coercer. A voter may be asked by a corrupted authority to show his vote before casting it into the urn. This, however, is a more obvious attempt on getting to know a voter's vote and requires the collaboration of all participating authorities. A more secret one would be to force the voter to take a picture of his vote, while he is still in the voting booth. Though, the coercer still cannot be sure whether the voter actually cast the photographed vote. It could be the case that the voter threw it away and used a second ballot to submit his desired vote. A better proof for the coercer would be that the voter films/ photographs his whole election process till casting the vote, so that the coercer is sure which ballot exactly is submitted. Moreover, by vote casting, the last submitted votes remain on top of the pile of all votes in the urn. If the urn is opened without shaking, these votes could be linked with some certainty to the corresponding voters. Thus, this scheme is only limitedly coercion-resistant.

Some voting schemes in this class, e.g. Scantegrity II [17], provide the voter with a receipt of his vote. It contains the unencrypted serial number of the ballot and a random unique confirmation code, which corresponds to the desired candidate. After all receipts are published, each voter can verify whether his vote was correctly recorded by comparing the code next to his serial number. In case of a missing vote or vote modifications, the voter can use his receipt to prove his preference to the election officials. Moreover, third parties can also verify the correctness of a vote, if they have a copy of the corresponding receipt. The ballots themselves are decrypted in such a way, that a link between a ballot and the corresponding receipt cannot be established. As a result, the scheme provides long-term privacy and receipt-freeness. However, privacy can be lost if the voter provides an adversary with a photo of his ballot after the confirmation code has become visible. In this case both the serial number and the chosen candidate are visible and, hence, linkable to the voter. Another possible attack is the chain voting attack. A coercer gives a pre-marked ballot to the voter before he goes to the polling station. There, the voter receives a valid ballot from the authorities, as well. He then switches both ballots, submits the manipulated one, and returns the

valid one to the coercer. Thus, the scheme is not coercion-resistant. It follows that it depends on the representative of this subclass whether receipt-freeness and coercion-resistance are provided.

Voter privacy, coercion-resistance, and receipt-freeness are satisfied for the representatives mentioned in the hidden vote class. Votes and any identifying information are never submitted in plaintext. However, voter privacy in this class is only computational and depends on various assumptions. For instance, it is assumed that the participating authorities are honest. Faulty authorities can learn about voters' candidate choices by decrypting their encrypted votes. In Scratch & Vote, for instance, voter privacy is also guaranteed, because the submitted ballots are tallied in an encrypted form and only the tally is afterwards decrypted. Thus, the links between voters and their votes remain hidden.

The described representatives of the hidden vote class are also receipt-free. After scanning their ballots, voters take them as receipts. These receipts, however, neither identify the voter, nor reveal the vote he cast, so he cannot prove his choice to a coercer. Later, the voters can verify that their ballots are correctly published to the bulletin board by comparing the information there with the information on their ballots. In case of wrongly published ballots, voters can complain with their receipts. In addition, since all proofs of correctness are published to the bulletin board, each observer can verify that only valid ballots participate in the tally and that the tally is correct. Though, if a voter loses his receipt, adversaries may publish false votes on the bulletin board undetectedly. They can also force voters to vote and bring them their receipts as proofs, thus, manipulating the vote.

Schemes can tolerate a certain number of corrupt authorities and still maintain a proper voting process. In Split-Ballot, which is a member of the vote threshold schemes subclass, if both authorities are trustworthy, everlasting privacy and receipt-freeness are achieved. Though, in case of one corrupt authority receipt-freeness may be no longer satisfied and only computational vote privacy is provided. Privacy is lost when both authorities are corrupted. The fixed number of corrupt authorities the scheme can handle, independent of the number of voters, makes the scheme not scalable. Scalability is satisfied in voter key threshold schemes, e.g. the scheme in Schoenmakers, where the secret is shared among all n voters. This scheme allows a certain tolerance in case of corrupt voters. If their number is less than the required threshold of participating parties, the voting process is still accomplished correctly.

The hidden voter with hidden vote class differs from the hidden vote class in the way how the cast votes are processed during the tallying stage. As discussed in Section 3.2.2, in the hidden vote class all cast votes are counted in encrypted form, in order to compute the tally (also in encrypted form). Finally, the computed tally is decrypted and announced publicly. In contrast to the tallying process in the hidden vote class, in the hidden voter with hidden vote class the cast votes are first anonymized by an anonymous channel, e.g. a re-encryption mixnet. Then, they are decrypted and, finally, the tally is computed. However, the anonymous channel implementation can be seen as a trade-off between scalability on one hand and universal verifiability and accuracy on the other hand. Voter privacy in the described representatives is achieved, due to the ballot characteristics and the re-encryption mixnet. Candidates' names are randomly mixed on each ballot and votes are submitted in an encrypted form. In case of using a re-encryption mixnet it is assumed that at least one mix is honest. Otherwise, privacy is not guaranteed, since a decrypted vote can be linked to a receipt. It is also important not to decrypt votes before their linkability to the voters is lost. After vote casting, votes are anonymized through re-encryption and permutation in the re-encryption mixnet. After that it is no longer known which voter cast which vote and the linkability between voters and their votes is destroyed. At vote casting each voter receives a

receipt for his choice. Since it contains only encrypted information, the voter is not able to prove his vote to a coercer. Moreover, if the scratch field hiding the secret information is destroyed, the vote is no longer valid. Receipt-freeness and coercion-resistance are also guaranteed by the fact that voters destroy the mixed candidate list. Without it it is not possible to match the marked box on the ballot with a certain candidate.

In Prêt à Voter, for instance, voter privacy is also satisfied by using a (t, n)-threshold scheme. A single malicious authority cannot disrupt the election. On the contrary, the number of malicious authorities needed do disrupt the election is scalable and depends on factors, such as the number of the secret sharing parties, the number of mixes, etc. The scheme is more robust to corrupt behavior than schemes which can handle only a fixed number of corrupt parties. In addition, in Prêt à Voter it is enough that only one honest authority participates in the ballot creating process to preserve voter privacy. As far as the shuffling phase is concerned, faulty behavior can be simply ignored and replaced without privacy loss.

The analysis of the hidden voter, hidden vote, and hidden voter with hidden vote classes is summerized in Table 1.

Table 1: Comparison between hidden voter, hidden vote, and hidden voter with hidden vote

Class / Property	Hidden voter	Hidden vote	Hidden voter with hidden vote
Type of cast vote	plaintext	encrypted (homomorphic encryption)	encrypted (re-encryption mixnet)
Privacy	long-term	computational	computational
Receipt-freeness	scheme-depending	computational	computational
Coercion-resistance	scheme-depending	computational	computational
Possible attacks	chain voting attack	corrupt authorities	corrupt authorities, faulty mixes

3.3 Privacy taxonomy by Langer

In this part of the section the dissertation by Langer [18] is presented. In her work she concentrates on the privacy and the verifiability aspects of voting schemes. More precisely, she defines privacy through unlinkability and proposes a model that captures the relations between both properties. However, here we look only at the author's contemplations on privacy, i.e. the privacy model and the defined privacy levels. Furthermore, for a more profound analysis of voting schemes Langer suggests considering the role of an adversary. She provides an adversary model which, together with the privacy model and levels, forms a taxonomy for voting schemes.

3.3.1 Notations

The author differentiates between real-life people and objects, separating, therefore, voters and candidates from votes and ballots. The following notations are used in the paper:

- V: set of all eligible voters
- C: set of all selectable candidates

- B: set of possible ballots
- S: set of possible votes (selections)

The relations between the entities above are defined as follows:

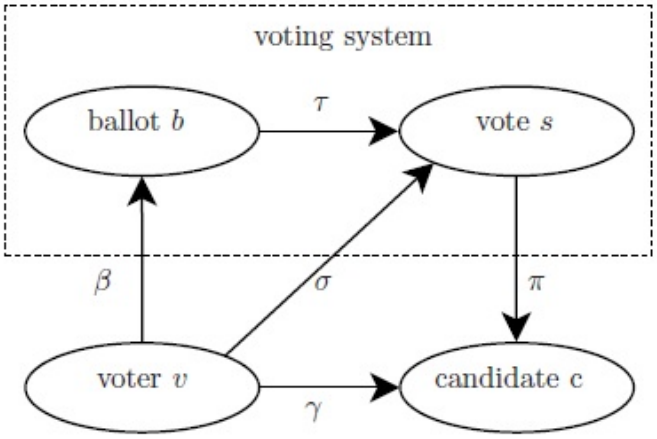
- γ: $V \to C$ maps a voter $v \in V$ to his preferred candidate $c \in C$
- β: $V \to B$ maps a voter $v \in V$ to his ballot $b \in B$
- σ: $V \to S$ maps a voter $v \in V$ to his vote $s \in S$
- τ: $B \to S$ maps a ballot $b \in B$ to the contained vote $s \in S$
- π: $S \to C$ maps a ballot $b \in B$ to the selected candidate $c \in C$

Moreover, $\tau \circ \beta = \sigma$ and $\pi \circ \tau \circ \beta = \gamma$.

3.3.2 Privacy and unlinkability

In this subsection we present the author's definition of privacy in terms of unlinkability. The suggested model is based on the relations between individuals: a voter, a vote, a ballot, a candidate. The author calls this an individual-related model (Figure 1) and uses it to show the relations between privacy and verifiability. Furthermore, she uses the model as a basis for her privacy classification.

Figure 1: Individual-related model [18]



The author emphasizes the connection between privacy and unlinkability, stating that privacy requires the unlinkability of voters and their votes. She sees privacy as an individual concern and, consequently, calls the model describing it an individual-related model. In the individual-related model, a voter v, a ballot b, a vote s, a candidate c, and the mappings between them are concerned. The voting process can be generally described as follows: a voter v submits a ballot $b = b(v)$, which contains the vote $s = t(b)$ for a candidate $c = n(s)$. The unlinkability between a voter and his vote can be expressed through the unlinkability between a voter and his chosen candidate. The author assumes that no direct link between a voter and his preferred candidate exists. Instead, the relation between them can be represented indirectly through relating a voter to his ballot,

which then can be related to the vote reflected by the ballot, which relates to the corresponding candidate:

$$\gamma = \pi \circ \tau \circ \beta \tag{5}$$

Since $\sigma = \tau \circ \beta$, there are two approaches to realize unlinkability of voters and their votes: first, unlinkability of a voter and his ballot and, second, unlinkability of a ballot and the vote reflected by it. The first approach is used in voting schemes based on mixnets, which anonymize the voters and, hence, hide their correspondence to ballots. The second one is used in homomorphic schemes, where the tally is computed from the encrypted ballots and only the final result is announced.

3.3.3 Privacy levels

In this section we provide the author's classification of privacy levels based on the previously introduced individual-related model. First, the privacy levels are given based on two criteria: unlinkability and abstention. Then, the logical relations between the levels are shown and a reference to the individual-related model is made.

For her classification of privacy the author considers two sides of privacy. On one hand, privacy is defined as unlinkability between voters and their votes. This definition comprises the unlinkability of a voter and his ballot and of a voter and his vote, as well. On the other hand, it should not be decidable whether a voter voted, or not[1]. The author calls this undecidable abstention. Moreover, she also considers the cases when these properties are violated, but this violation is not provable. Thus, she combines both privacy directions and forms a two-side classification of privacy. The result are the following privacy levels:

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 a voter and a ballot.

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

UL.2 Unprovable linkability.

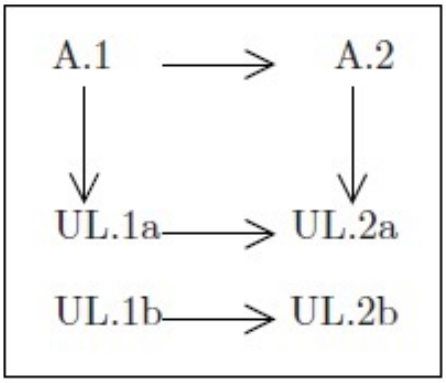
a If it is possible to establish a link between a voter and a ballot, then the link is not provable to third parties.

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

We use the author's figure (Figure 2) to show the logical relations and implications between the different levels:

[1] This is required by the German legislation. In Germany, it is not allowed to publish any information about whether a certain voter voted, or not. This may vary in other countries.

Figure 2: Logical relations between different privacy levels [18]



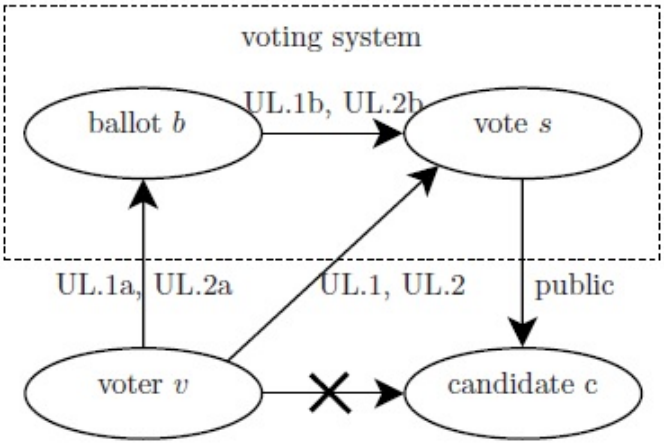
Voting schemes associated to A.1 achieve a higher level of privacy than systems associated to A.2, since A.1 states that abstaining voters remain undetected, whereas A.2 implies the possibility to detect them. Analogously, systems associated to UL.1a and UL.1b provide higher privacy levels than systems associated to UL.2a and UL.2b, respectively. The privacy levels UL.1a and UL.1b, as well as UL.2a and UL2.b are orthogonal. This means that they express two different ways to establish unlinkability of a voter and his vote and unprovable linkability of a voter and his vote, respectively. Hence, voting schemes that can be associated to either UL.1a or UL.1b obtain the privacy level UL.1 and schemes that can be associated to UL.2a or UL.2b reach level UL.2. The author makes the following deductions:

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

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

Figure 3 shows how the different privacy levels except for voter abstention can be adapted to the individual-related model.

Figure 3: Privacy in the (un)linkability model [18]



The privacy classification above does not cover receipt-freeness and coercion-resistance. Since the author finds these properties dependent on certain adversary capabilities, she considers them

in her adversary model, which we discuss in the next subsection.

3.3.4 Adversary model and attacks on privacy

For a more profound analysis of voting schemes the author suggests considering the presence of an adversary, as well. She defines three main directions in which an adversary can affect the voting process and shows which adversary capabilities are needed for each of them. Finally, she considers the possible attacks on privacy, based on the adversary capabilities in each category.

The author considers two main ways in which an adversary can affect a voting system. On one hand, he can affect the communication between entities. This can be done by using existing communication channels or by creating new ones. On the other hand, the adversary can affect the system cryptography. As a result, the auhor classifies adversary capabilities in the following three categories:

I. Existing communication channels

II. New communication channels

III. Cryptography

The adversary's influence in each of these categories is described in the following subsections.

Adversary's capabilities in existing communication channels

In electronic poll-site voting schemes fewer electronic communication channels are used than in electronic online voting. Still, it is important to consider the possible adversary's capabilities in communication channels since also the non-electronic channels pose risks for privacy. As far as using the existing communication channels of a voting system is concerned, the possible adversary's influence is summarized in the following capabilities:

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.

Ia. is the least harmful of all capabilities in terms of privacy. Detecting channel usage (Ia.) does not necessarily reveal additional information about communicating entities or voters' votes. It only shows that the channel is being used, but does not show neither how, nor by whom. However, this attack becomes more dangerous for privacy, if in addition the sender of a message (voter or authority) can be determined (Ib.). Thus, it can be stated with certainty that a certain voter submitted his vote. In case of forced voting, the adversary would know that the coerced voter actually voted. Undecidable abstention (A.1) is lost in this case. Ic. states that the adversary is

able to observe the communication process but still cannot influence them directly. Still, he can link a voter to a vote. UL.1a is, consequently, no longer achieved, although the linkability of a voter and his vote is still unprovable (UL.2a). In levels Id-f. the adversary is able not only to hinder the communication between the entities, but to cast his own messages and modify already cast ones. These levels affect mostly eligibility, vote integrity, and accuracy and will not be further discussed.

The author compares the use of an untappable channel with the use of an anonymous channel to analyze which capabilities apply by each of them. Regarding Juels et. al [5], an untappable channel achieves perfect privacy in information-theoretic sense. Therefore, it prevents all of the capabilities above. However, an anonymous channel can only prevent an adversary from determining the sender of a message (Ib.) The remaining capabilities are, hence, still applicable. As a result, untappable channels can be seen as providing higher privacy levels than anonymous channels.

Adversary's capabilities in creating new communication channels

In order to compromise privacy, an adversary may try to communicate with voters and/ or authorities and learn about voters' votes/ ballots. The adversary can realize this communication by creating new communication channels. Thus, he can attain the following 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 on the bulletin board.

We will see, that these capabilities can compromise privacy mainly by establishing a link between a voter and his ballot/vote.

The capabilities IIa.-IId. allow the adversary to establish a one-way or a two-way communication channel with voters (IIa. and IIc.) and/or authorities (IIb. and IId.), whereas IIe. allows the adversary to corrupt the public bulletin board. IIa. provides a communication channel from the voter to the adversary which can be used by the voter to reveal his ballot and/or vote to the adversary. In poll-site voting schemes such an attack can be performed, for instance, by forcing a voter to make a photo of his or her filled out ballot. In this case, the unlikability between a voter and his ballot (UL.1a) and the unlinkability between a voter and his vote (UL.1) are lost. Receipt-freeness is also compromised, since the voter can provide the adversary with a proof of how he voted. In case the adversary can send messages to the voter (IIc.), he can make him cast a predefined ballot. Thus, not only vote integrity is compromised, but also voter privacy, since a link between the voter and his vote can be established (UL.1 is again lost). IIb. allows an authority to send messaged to the adversary. These can be, for instance, information about decrypting voters' ballots and linking them to the corresponding votes. Hence, the unlinkability between a ballot and a vote can be compromised and the voting system can no longer be assigned to privacy level UL.1. In addition, if the unlinkability between a voter and his ballot is compromised, as well (UL.1a), then a link between the voter and his vote can also be established (UL.1). The author emphasizes on the dangerosity and the massive effect of this attack, as it can reveal the corresponding links

for all voters at the same time.

IId. and IIe. affect mainly eligibility, integrity, and uniqueness and are not further discussed in this thesis.

Adversary's capabilities in cryptography

In order to define the adversary's capabilities according to cryptography, the author opposes the idea of "perfectly" working cryptography in the standard Dolev-Yao model [19]. She considers the idea that cryptography, providing only computational privacy, may be breakable and defines the corresponding adversary's capability as follows:

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

According to the author, an adversary cannot influence cryptography that achieves information-theoretic privacy. The author suggests that breaking cryptography that achieves only computational privacy may be due to cryptographic algorithms becoming insecure over time. Thus, she mentions the problem of long-term privacy to state that even if a voting system provides privacy at present, it may no longer be able to keep it in future.

Breaking cryptography, an adversary can decrypt ballots and link them to the corresponding votes, thus compromising the unlinkability between a ballot and a vote (UL.1b). If unlinkability of a voter and his ballot is also compromised, then the voter can be even linked to his vote (UL.1). Similar to her opinion about IIb., the author finds IIIa. dangerous for privacy, as well, because of its possible massive effect on all voters simultaneously. Both IIb. and IIIa. are highlighted by the author as the most dangerous of all discussed capabilities because they can massively cause a total privacy loss by linking all voters to their votes at the same time. Furthermore, the author concludes that privacy attacks are mainly passive (e.g. eavesdropping, receiving information from cooperating voters/ authorities, etc.), since the adversary does not actively interfere with the voting system (e.g. modify or inject messages). The active attacks mainly violate the integrity of the voting schemes.

Table 2 summarizes which of the discussed capabilities affect privacy.

Table 2: Adversary capabilities affecting privacy [18]

Ia + b	X
Ib + c	X
Id	
Ie	
If	
IIa	X
IIb	X
IIc	X
IId	
IIe	
IIIa	X

3.4 A formal privacy taxonomy by Dreier et al.

In contrast to the previously discussed papers, the paper by Dreier et al. [20] analyzes privacy formally. The authors concentrate mainly on vote-privacy, receipt-freeness, and coercion-resistance as privacy properties that lead to different privacy levels. Regarding these properties, they provide a set of privacy notions, based on the formal definitions of the applied pi calculus [21]. The resulting taxonomy extends the applied pi calculus in considering "vote-independence" and "vote-copying" attacks.

3.4.1 Privacy definitions and attacks

The authors start their paper with the definitions of the main security properties, required for secure voting systems. They also divide these properties in three categories: correctness and robustness properties, verifiability, and privacy properties. In terms of this thesis, we consider only the privacy properties. Then, we provide the authors' extended privacy classification, based on the definitions of the privacy properties.

The authors assign vote-privacy, receipt-freeness, and coercion-resistance to the group of privacy properties. These properties cover different privacy aspects.

Vote-privacy Voting systems that provide vote-privacy keep votes private, meaning that voters and their votes are not linkable.

Receipt-freeness Voting schemes that provide receipt-freeness ensure that it is impossible for a voter to prove his vote to third parties.

Coercion-resistance Voting systems that provide coercion-resistance prevent that a coercer can be sure whether a coerced voter actually complied to his demands or voted the way he initially intended to.

In their work the authors define the attacks violating privacy as follows. In case there is an attacker targeting a voter and all other votes and the final result are known to the attacker, he can then easily guess that voter's vote. In order to preserve voter's and vote privacy, the authors suppose there exists one other voter, whose vote is also unknown to the attacker. Thus, the authors introduce the terms of "the targeted voter" and "the counterbalancing voter", respectivelly. The counterbalancing voter's role is to make it impossible for the attacker to distinguish whether the coerced voter complied or not. Thus, the authors see privacy as observational equivalence. In addition, they discuss four privacy aspects, based on the definitions of coercion-resistance, receipt-freeness, and vote-privacy: communication between the attacker and the targeted voter, vote-independence, security against forced-abstention-attacks, and knowledge about the behavior of the counterbalancing voter.

1. Communication between the attacker and the targeted voter

   In this category, the authors discuss three possible levels of interaction between an attacker and a voter. The first one is a passive interaction, with no direct communication, between both parties. The attacker only observes publicly available data and communication, e.g. information published on the bulletin board. The authors refer to this level as vote-privacy (VP).

   In the next level the voter provides the coercer with private data, in order to convince

him that he voted in a certain way. However, the coercer cannot be sure whether the voter actually used that data or not. For instance, in the common voting process in a voting booth (Section 3.2.1) the voter can send a ballot to the adversary to prove his vote. Still, since ballots are not unique and the voter can easily receive a new one by request, the coercer cannot be sure that the ballot he received is the actual voter's ballot. The authors call this property receipt-freeness (RF).

In the third level the voter pretends to fully cooperate with the attacker, complying to all his instructions. However, the coercer cannot determine whether the voter actually cooperates or only pretends to do so. The authors refer to this property as coercion-resistance (CR).

Vote-privacy, receipt-freeness, and coercion-resistance comply to the following relation: $CR > RF > VP$. This means that the property of coercion-resistance is stronger than receipt-freeness, which, itself is stronger than vote-privacy

2. Vote-independence/corrupted voter

In this category the authors distinguish two types of attackers: the outsider (O) and the insider (I). An Outsider is described as an external observer [20], whereas an insider possesses control over a legitimate voter, different from the targeted voter and the counterbalancing voter. The insider can gain information about the corrupted voter's vote and secret data and use it to learn about the targeted voter's vote, e.g. by vote-copying. In this way, privacy can be compromised. Since the insider receives information about the voting process from an internal party, he is more powerful than an outsider ($I > O$).

3. Security against forced-abstention attacks

Backes et. al [22] see immunity to forced-abstention attacks as a consequence of coercion-resistance. Juels et. al [5] also relate coercion to forced-abstention attacks, stating that in case of coercion an attacker can force a voter to abstain from voting. Dreier et. al, however, distinguish the security against forced-abstention attacks from coercion-resistance, in order to cover the case of vote-privacy. The authors relate security in case of forced-abstention attacks to observational equivalence. According to the achieved extent of observational equivalence, they define two levels: security against forced-abstention attacks (FA) and participation only (PO). In FA the observational equivalence is required to hold in any case, even if the voter actually abstained from voting. PO covers the cases when the targeted voter does not abstain from voting. Compared to each other, security against forced-abstention attacks (FA) is stronger than participation only ($FA > PO$).

4. Knowledge about the behavior of the counterbalancing voter

We have seen above that the counterbalancing voter is a balancing measure against privacy leakage, in case the attacker knows the final result and how everybody (except the targeted voter) voted. Therefore, his behavior is important and should not reveal further information about the targeted voter. In terms of observational equivalence, the authors consider two levels of knowledge about the counterbalancing voter's behavior: any behavior (AB) and exists behavior (EB). AB states, that observational equivalence holds for any behavior of this voter, e.g. he may or may not post fake ballots. Although the attacker is aware of his behavior, he still cannot be sure whether the targeted voter complied to his instruction, or not. In the second level (EB) the observational equivalence holds for at least

one behavior of the counterbalancing voter. His behavior can also change. The attacker is not sure how many fake ballots the counterbalancing voter cast. EB is, therefore, weaker than AB ($AB > EB$).

Considering the whole level hierarchy, the authors define CR under I, FA, and AB, i.e. $CR(I, FA, AB)$, as the strongest property and VP under O, PO, and EB, i.e. $VP(O, PO, EB)$, as the weakest, respectively.

3.4.2 Hierarchy

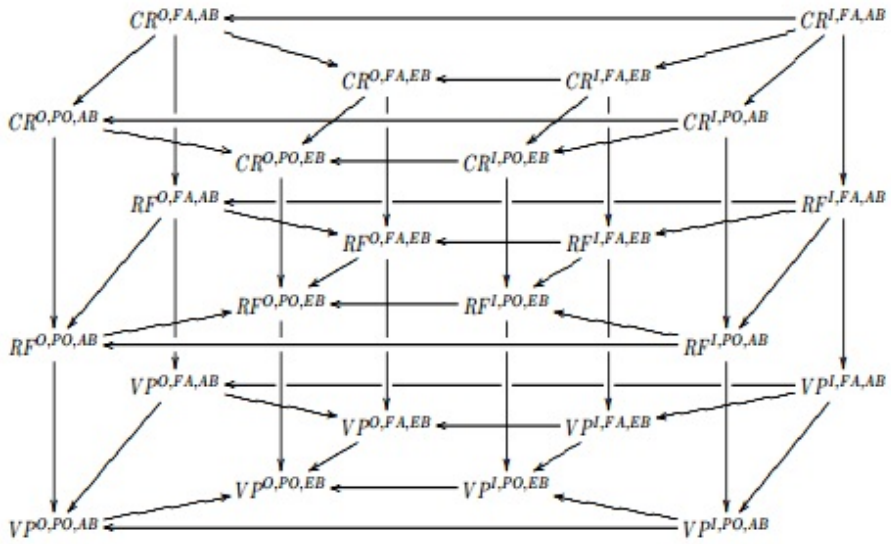
In this section we provide the authors' view on the relations between the different levels and sublevels. First, we introduce some of their parametric notations for each level. Then, we show their contemplations on the dependencies between the sublevels and, finally, show the resulting hierarchy as a graph.

In order to apply the definitions from Section 3.4.1 to the applied pi calculus, the authors define each level formally as a set of parameters:

- Privacy = $\{CR, RF, VP\}$
- Eve = $\{I, O\}$
- Abs = $\{FA, PO\}$
- Behavior = $\{AB, EB\}$

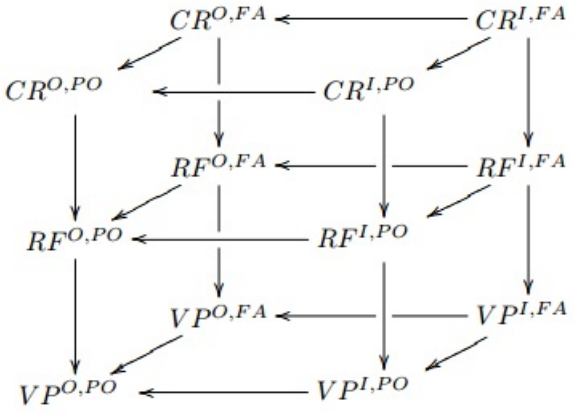
The authors also discuss the relations and dependencies between the sublevels in the hierarchy in terms of achieved privacy. They show that if privacy is achieved in the presence of an inside attacker, then it is also achieved in the presence of an outside attacker ($Privacy(I, Abs, Behavior) \rightarrow Privacy(O, Abs, Behavior)$). Therefore, privacy is more difficult to preserve in case of an insider. Moreover, if a protocol satisfies privacy in case of forced-abstention attacks, then it also satisfies it when the targeted voter does not abstain from voting ($Privacy(Eve, FA, Behavior) \rightarrow Privacy(Eve, PO, Behavior)$). In addition, since $AB > EB$, achieved privacy in terms of AB implies achieved privacy in terms of EB ($Privacy(Eve, Abs, AB) \rightarrow Privacy(Eve, Abs, AB)$). We have already shown that $CR > RF > VP$. This could also be expressed as the transition $CR(Eve, Abs, Behavior) \rightarrow RF(Eve, Abs, Behavior) \rightarrow VP(Eve, Abs, Behavior)$. The authors summarize all interrelations between the levels and the sublevels in the following figure:

Figure 4: Hierarchy of privacy notions [20]



If protocols that do not use fake ballots are considered, the behavior aspect is omitted and we receive the following hierarchy:

Figure 5: Collapsed hierarchy of privacy notions [20]

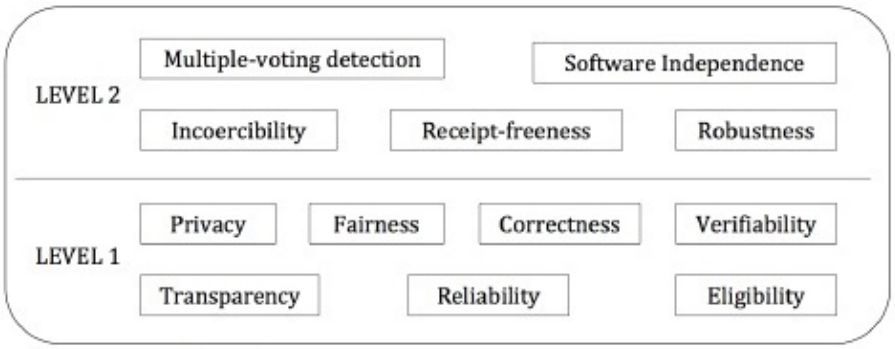


3.5 Taxonomy by Li et al.

In this section we discuss the taxonomy by Li et al. [23]. The authors classify voting schemes according to the cryptographic primitives they use. More precisely, they divide voting schemes in four main categories. In terms of the used cryptographic primitives, they distinguish between mixnets, blind signatures, threshold homomorphic encryption schemes, and secret sharing. As we have seen in Section 3.2, voting schemes that belong to more than one category also exist. For instance, Split-Ballot uses both homomorphic encryption and secret sharing, whereas Prêt à Voter uses homomorphic encryption and mixnets. Based on the examples schemes they discuss, the authors state that all suggested schemes achieve privacy, independent of the type of cryptographic primitives they use. Thus, their classification covers two general privacy levels: achieved privacy and not achieved privacy. Further, Li et al. provide a two-level class distinction according to

the type of requirements that voting systems achieve (Figure 6). They distinguish between basic requirements (Level 1) and advanced requirements in case of attacks (Level 2).

Figure 6: Requirements of e-voting schemes [23]



As seen in Figure 6, Level 1 covers voting systems that achieve privacy, whereas Level 2 covers voting systems that achieve receipt-freeness. Still, voting schemes may achieve properties from both levels simultaneously. Moreover, achieving properties from Level 2 does not necessarily mean that a voting system achieves all properties from Level 1 and vice-versa. The authors state that, in general, all requirements are equally important for voting systems. However, they believe that achieving properties from Level 2 enhance the security of voting systems.

In the previous chapter we presented several taxonomies for classifying voting schemes with respect to privacy. Now, we provide an evaluation and comparison of these taxonomies, starting with which we consider the least precise one and finishing with the most precise one.

As we have seen in Section 3.5, the taxonomy by Li et al. classifies voting schemes in terms of the cryptographic primitives they use, dividing them in four categories. Moreover, based on the requirements the schemes fulfil, the authors define two main categories of voting schemes: schemes that fulfil privacy and schemes that fulfil receipt-freeness. Even though, grouping voting schemes with respect to the cryptographic primitives they use does not guarantee that they achieve the same properties. For instance, UVote, Helios, and Prêt à Voter all use mixnets. However, UVote and Helios do not achieve receipt-freeness, whereas Prêt à Voter does. Additionally, as already stated in Section 3.5, the taxonomy allows assigning a single voting scheme to more than one category at the same time, which makes it imprecise. Furthermore, as the taxonomy does not define any levels, e.g. voter privacy levels, there is no hierarchical classification within a single category or even among the categories. It is also not possible to state that using a certain cryptographic primitive guarantees achieving certain requirements. Thus, the taxonomy only groups voting schemes together based on a common characteristic but does not provide a possibility to actually compare them. Therefore, the taxonomy by Li et al. is too general to provide a thorough classification of voting schemes.

The taxonomy suggested by Sampigethaya and Poovendran in Section 3.2 is similar to the one by Li et al. It classifies voting schemes by another criterion (the way voters submit their votes), but still does not provide a hierarchical classification among and within the classes. The authors consider various properties, but neither is there a class that manages to achieve all of them, nor do they consider tradeoffs that exist among the classes. Moreover, there is no exact classification of voting schemes, since a voting scheme may be assigned to more than one class. For instance, Scratch & Vote and Split-Ballot belong to the hidden vote class but they could belong to the hidden voter with hidden vote class, as well. Hence, the taxonomy by Sampigethaya and Poovendran allows only a general classification of voting schemes.

As we have seen in Section 3.1, Coney et al. provide a more formal taxonomy and suggest the idea of a perfectly private voting system. They classify voting schemes only in terms of privacy. Unlike the taxonomies by Li et al. and by Sampigethaya and Poovendran, they consider privacy loss and the influence of adversaries and outside information leaking sources. We can state that they define two main classes for classifying voting schemes: schemes that achieve perfect privacy and schemes that do not. However, perfect privacy and privacy loss can only be formally computed. Moreover, the authors define a voting system that covers receipt-freeness and coercion-resistance as a system providing perfect ballot secrecy. However, although they say that this is an important property for a realistic view on voting systems, they do not address this notation in their taxonomy. The taxonomy is also too abstract, since it does not provide a firm criterion for classifying voting schemes. It is unclear whether not perfectly private voting schemes still provide a sufficiently high privacy level. More precisely, a voting system is only perfectly private if even a computationally unbounded attacker cannot reveal any information about the vote cast by a voter. However, in many elections it is reasonable to assume that at least the internal attackers (i.e. poll workers, officials) are computationally restricted. It should be defined how much deviation from perfect privacy is required to classify a voting scheme as good or as one that no longer provides privacy. A further problem of this taxonomy is that deviation from perfect privacy is not

a satisfactory criterion for computing privacy. A small deviation does not necessarily mean that a voting system is almost perfectly private. For instance, if voters' tendencies to vote are easily predictable, an adversary could with high probability guess the votes correctly. Then, even in case of information leakage by the system and process, the deviation from perfect privacy will be very small. Though, such a system should not be actually classified as one achieving privacy. As a result, the taxonomy by Coney et al. provides only a general and not precise enough classification of voting schemes.

The taxonomy by Dreier et al., which we presented in Section 3.4, provides an even more formal approach for assessment of voting schemes in terms of vote privacy, receipt-freeness, and coercion-resistance. Unlike the three taxonomies above, this one considers the presence of an attacker who can passively, as well as actively affect the voting process. Thus, the authors define vote privacy as unlinkability of voter and vote in the presence of an attacker who only observes publicly available information. They also define a voting protocol as secure if a voter can protect himself against coercion. Moreover, the taxonomy by Dreier et al. not only assigns voting schemes to concrete levels, based on common features, but also defines a level hierarchy of privacy properties. This allows a more thourough classification and comparison of schemes assigned to the same or to different levels.

Similar to the taxonomy by Dreier et al., the one by Langer, which we presented in Section 3.3, also suggests distinct levels for classifying voting schemes. More precisely, it distinguishes between a privacy model and an adversary model, which also handles receipt-freeness and coercion-resistance. Whereas Dreier et al. see vote privacy as unlinkability of a voter and his vote in case of a passive attacker, Langer distinguishes two aspects of voter privacy. She considers unlinkabilitiy of a voter and his vote even in case of an active attacker, on one hand, and, on the other hand, undecidable voter abstention. Unlike the other proposed taxonomies, in her privacy model she also covers the cases that linkability between a voter and his vote or voter abstention can be detected but not be proven to third parties. Thus, she establishes additional privacy levels for a more thorough classification of voting schemes. In comparison to the previously reviewed taxonomies, the one by Langer provides the most detailed advesary model. The author examines in detail three classes of adversary capabilities and their influence on the levels in the privacy model. She distinguishes between capabilities concerning existing communication channels, capabilities concerning new communication channels, and cryptographic capabilities. The capabilities concerning existing communication channels describe possible passive and active attacks. Passive attacks may affect the unlinkability of a voter and his ballot. Still, even if linkability can be established, it remains unprovable to third parties. Furthermore, she states that active attacks do not affect privacy. As defined in Section 3.3, capability IIb. determines that an election authority can send messages to the adversary, whereas capability IIIa. determines that the adversary is able to break any cryptography which provides only computational security. The author regards these two capabilities as the most severe ones in her adversary model, since they can reveal information about all voters at the same time. This shows that, although most capabilities in the adversary model are not hierarchically ordered, a certain hierarchy can still be observed. Thus, taxonomy by Langer provides the most thorough and precise classification for voting schemes among all considered taxonomies in this thesis.

According to the analysis above, we may conclude that privacy taxonomies should provide distinct privacy levels and consider various privacy aspects, in order to allow a thorough and precise privacy classification of voting schemes. The presence of an adversary and the resulting effects on voting schemes should also be considered. Especially the risk of computationally unbounded

attackers should be taken into account, since everlasting privacy is a desirable property. Not only should separate and explicitly defined privacy levels be provided, but also a hierarchical comparison among and within the levels should be possible. What the already presented taxonomies do not consider is the trust voters have to put into authorities (e.g. poll workers, officials) with respect to privacy. For instance, in voting schemes where votes are cast in an encrypted form, voters must trust the entities that manage the corresponding private keys. In the next section, we provide an example of a taxonomy that considers these issues.

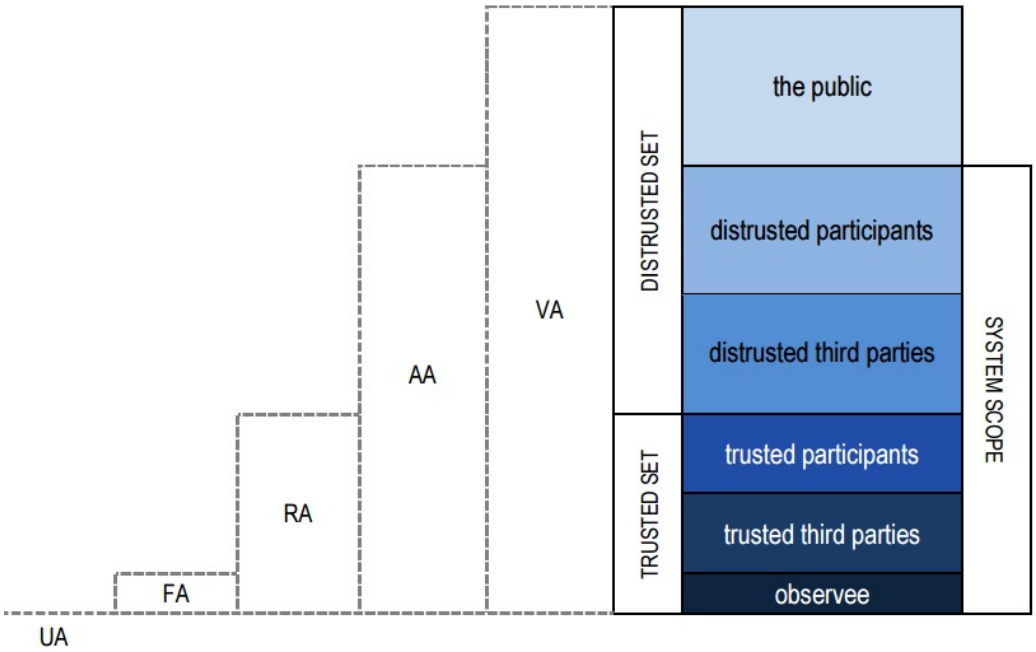
5 Taxonomy by Pleva

In this section we shortly present the taxonomy suggested by Pleva [24], which we use later in Section 6 as a basis for our proposed privacy taxonomy. Pleva suggests a general taxonomy for classifying electronic services and mechanisms, based on the notions of digital anonymity and scope of trust. Considering the recognisability of individuals in terms of personally identifiable information (PII), he defines five levels of anonymity.

In his work, Pleva focuses on the problem of publicity, i.e. the extent of individuals' recognisability. Remaining anonymous requires that any personal identifiable information is kept unobservable to anyone, except for the observee, who the author defines as the party from whose viewpoint the service is analyzed. However, some systems involve trusted third parties which are allowed to observe and manage personal information without anonymity being lost. By default, the observee belongs to the trusted parties, as well. Together, the observee and all trusted entities form the trusted set. All other entities, e.g. the public, are considered distrusted. The trusted set and the distrusted set except for the public form the system scope. The entities which an observee is forced to trust, in order to remain unrecognized, are defined by the author as the scope of trust. If any personal data becomes observable from outside the scope of the system, then it is considered publicly known. The author notes as an extreme case the case when the scope of trust includes only the observee.

Figure 7 gives a better understanding of the system scope, illustrating the scope boundaries in the different anonymity levels.

Figure 7: Scope of trust [24]



As far as anonymity is concerned, Pleva concentrates on connection anonymity and on procedural anonymity. He defines connection anonymity as hiding the identities of the source and the destination during interaction, e.g. the actual data transfer, whereas procedural anonymity addresses the ability of the underlying protocol to hide the source of a message. He also specifies that if anonymity can be breeched under certain circumstances, then it is regarded as conditional

anonymity. Otherwise, if anonymity cannot be breeched under any circumstances, then we talk about unconditional anonymity.

The author also introduces the concept of personally identifiable information (PII) as the information sufficient to uniquely identify/trace a specific individual. He distinguishes between three types of PII according to whether PII is traceable, with or without assistance by a third party, to an individual: directly resolvable (e.g. landline telephone numbers), indirectly resolvable (e.g. bank account numbers), and unresolvable (e.g. DNA). Directly resolvable PII, i.e. direct PII, does not require the assitance of a third party to identify an individual, whereas by indirectly resolvable PII, i.e. indirect PII, identification can be done with the assistance of the third party that manages the PII. On the contrary, unresolvable PII must not provide identification of an individual to anyone.

Additionally, Pleva gives definitions to the notions of identifiability and traceability and presents their relation to each other. Identifiability is defined as the possibility to know the identity of a system participant, due to the data exchanged in the system, whereas traceability is the ability to obtain information about the communicating parties by observing the communication context. Pleva combines both terms in the generalized concept of recognisability, defining it as the possibility of observing PII. According to the author, PII is observable if it is both accessible and interpretable. Analogously to anonymity, recognisability and, respectively, unrecognisability can also be conditional or unconditional. Moreover, recognisability may imply that individuals may become accountable for their actions.

Based on the definitions above, Pleva distinguishes five levels of anonymity.

Level 0 (void anonymity - VA)

Systems are assigned to level 0, if the scope of trust includes all entities outside the system, i.e. the public. More precisely, in these systems the PII of an individual is made publicly available. In this case the individual cannot hide its identity and has to put trust in all entities, i.e. observers from outside of the system. Void anonymity ensures unconditional recognisability and unconditional linkability.

Level 1 (apparent anonymity - AA)

The scope of trust in systems assigned to level 1 includes some distrusted entities but excludes the public. Apparent anonymity can be achieved in two ways: by applying either indirect, or direct PII. Applying indirect PII makes the identification of an individual more complicated. It is assumed that indirect PII becomes observable to distrusted parties, e.g. to the public. Identification is then possible with the participation of a third party, which can be another participant, a trusted party, or a not trusted party. The participation of one such distrusted party is required for achieving apparent anonymity. Applying direct PII can also achieve apparent anonymity, provided that the PII is publicly unobservable, but observable to all trusted parties and to a distrusted party. In general, apparent anonymity ensures unconditional recognisability. Distrusted parties involved in the scope of trust can gain access of both individual's identifiability and traceability data.

Level 2-3 (limited anonymity - LA)

Systems assigned to the level of limited anonymity have a relatively narrow scope of trust. Limited anonymity preserves the anonymity of entities that obey to certain predefined rules/laws. Moreover, it prevents adversary attacks and supports accountability, since the

identities of disobeying parties are revealed. The author sees limited anonymity as the best compromise between privacy and accountability. Depending on how anonymity is preserved, limited anonymity can be divided in two subclasses: revocable anonymity and forfeitable anonymity.

Level 2 (revocable anonymity - RA)

The scope of trust in systems with revocable anonymity includes the observee and at least an identity manager but may also include all trusted entities. The identity manager is a trusted third party that keeps PII private, but can, on demand, reveal it and, thus, revoke anonymity. Therefore, level 2 provides conditional anonymity and unrecognisability that depend on the identity manager. Distrusted parties may gain access of identifiability and traceability data. Reasons to revoke a person's anonymity may be fraud, when an adversary's identity must be revealed, violating predefined policies, or expiration of the need for anonymity.

Level 3 (forfeitable anonymity - FA)

The scope of trust in level 3 contains only the observee. Forfeitable anonymity resembles revocable anonymity in the fact that anonymity is preserved, as long as policies and laws are obeyed. Otherwise, the disobeying individual loses his anonymity, as his PII is revealed by the system. However, whereas revocable anonymity requires a separate entity, responsible for the revocation, e.g. an identity manager, forfeitable anonymity requires that the observee uses a pre-implemented event-driven forfeiture mechanism, such as a cut-and-choose technique or a zero-knowledge proof, to reveal PII. The system administrators are responsible for the proper working of this mechanism. An example of an event that can cause forfeiting anonymity may be an attempt on double-spending in e-payment transactions. In contrast to revokable anonymity, by forfeitable anonymity distrusted entities may gain access only of identifiability data.

Level 4 (unconditional anonymity - UA)

The previously presented levels provide only conditional anonymity, depending on a certain number of entities in the corresponding scope of trust. Unlike them, level 4, as the name suggests, provides unconditional anonymity. Moreover, it also provides complete unidentifiability and complete untraceability. However, the possibility of using PII still exists in the form of initially unlinkable pseudonyms, e.g. hashed IP addresses, which do not allow recognisability. Thus, the author considers the type of achieved linkability as undecided, as it cannot be distinguished between conditional, unconditional, or void. Since no trusted third parties are required to protect users' anonymity, the scope of trust contains no entities.

The characteristics of the anonymity levels above are presented in the following tables.

Table 3: Class-level characterisation of anonymity [24]

Level		Type of Anonymity	Scope of Trust		Recognisability	
Deg.	Abbr.		Lower Bound	Max. Ext.	Type	Source
0	VA	void	system scope	–	unconditional	identifiability or traceability
1	AA	apparent	trusted set	system scope	unconditional	identifiability or traceability
2	RA	revocable	observee	trusted set	conditional	identifiability or traceability
3	FA	forfeitable	void	observee	conditional	identifiability
4	UA	unconditional	–	void	void	none

Table 4: Class-level characterisation of anonymity (cont.) [24]

Level		Type of Linkability	Type of Legal Accountability	
Deg.	Abbr.			
0	VA	unconditional	direct	LOW LEVELS
1	AA	unconditional	direct or indirect	
2	RA	unconditional or conditional	indirect	
3	FA	unconditional or conditional	direct or indirect	HIGH LEVELS
4	UA	[undecided]	void	

6 Privacy taxonomy for poll-site voting schemes covering trust assumptions

In this section we present our approach for a privacy taxonomy for poll-site voting schemes, based on the taxonomies by Langer (Section 3.3) and by Pleva (Section 5). Our taxonomy combines their characteristics and shows which requirements should be met, in order to obtain higher levels of privacy.

As we have seen in Section 3.3.3, Langer defines privacy as unlikability of voters and their votes. She proposes privacy levels based on the idea that the voter's voting behavior cannot be predicted or proven to third parties. This requires that any additional information such as private keys is kept private, so that recognisability of voters and, therefore, their voting behavior, is prevented. However, in her work Langer does not consider under which trust assumptions personal information, i.e. the vote cast, remains private. On the other hand, Pleva's taxonomy is based exactly on the idea of keeping personal information private among a certain group of trusted and distrusted parties and, therefore, defines the extent of individuals' recognisability. Thus, we can further develop Langer's idea by combining it with the concept of scope of trust introduced by Pleva.

With respect to personally identifiable information Pleva distinguishes between direct PII and indirect PII. In some poll-site voting systems voting machines are used by the voters to cast their votes. In this case, the voter first identifies himself, e.g. with his ID card, and then submits his vote. Thus, a relation between his identity and his vote can later be established. Consequently, this approach allows the voting machine to observe direct PII. In comparison, in other poll-site voting schemes, e.g. Prêt à Voter or Scratch & Vote, a receipt is handed out to the voter containing information that links to an encrypted vote. In these schemes, in order to preserve voter privacy, the private key required for decrypting the vote is divided into several shares which are distributed among several authorities. That is, for instance, the case in voting systems based on (t, k) secret sharing. Thus, in this example the receipt, the public data, and the shared private key can be seen as indirect PII. If, for instance, the voter gives his receipt to another person, voter's identification does not follow automatically, but requires the participation of a third party, e.g. a subset of key holders.

With respect to the scope of trust Pleva distinguishes between a trusted and a distrusted set. However, in poll-site voting a trusted set does not exist, since nobody should be able to obtain the voter's vote. All participants are regarded as not trustworthy. Furthermore, since voting systems that achieve no privacy at all are of no interest, the scope of trust cannot include the public. In poll-site voting schemes the corresponding scope of trust includes only the minimum number of authorities required to cooperate, in order to reveal the vote cast by a voter. In Prêt à Voter and Scantegrity, for instance, the voter's vote can be exposed only in case of several corrupt authorities who cooperate with one another. Since the voter must trust these authorities, they can be regarded as the scope of trust. It is important to highlight that a voter does not need to trust all authorities contained in the scope of trust. With respect to shared keys, for instance, privacy is preserved if a majority of key holders act honestly and do not reveal any information about their shares. Therefore, the voter needs to trust only the minimum number of authorities that can decrypt his vote. This is different for voting schemes that use voting machines. Here, the voter has to fully trust the voting machine used.

Introducing the concept of scope of trust to the taxonomy by Langer allows to measure the level of anonymity also depending on the scope of trust. The more narrow the scope of trust is, the higher is the level of privacy obtained. Furthermore, another aspect should be to what extend the

distribution of a secret is scalable. The scope of trust can be either scalable as in Prêt à Voter or in the scheme by Schoenmakers, or fixed as in Split-Ballot, all of which we presented in Section 3.2.2. The scalable scope of trust provides the possibility for a variable number of private key shares, as well as a variable number of key holders, required to participate, in order to decrypt the vote. For instance, in the scheme of Schoenmakers the private key shares are distributed among all voters (as the voters act as authorities). In comparison, in Split-Ballot there are only two authorities that, if malicious, can violate voter privacy. In Section 3.2.2 in the paragraphs about voter key threshold schemes and vote threshold schemes, respectively, as well as in our analysis in Section 3.2.4 we saw that due to the variable number of authorities, participating in the decryption of the vote, the scheme by Schoenmakers is more scalable and robust to corrupt authorities. Hence, it satisfies voter privacy better than Split-Ballot. In general, it holds that schemes with a variable scope of trust are better in terms of satisfying privacy than schemes with a fixed scope of trust. Summarized, we propose to extend the taxonomy by Langer by the following types of scope of trust:

S.1 The scope of trust contains one authority that has access to direct PII.

S.2 The scope of trust contains more than one authority that has access to direct PII.

S.3 The scope of trust contains more than one authority that has access to direct PII. The amount of authorities contained in the scope of trust is scalable.

S.4 The scope of trust contains one authority that has access to indirect PII.

S.5 The scope of trust contains more than one authority that has access to indirect PII.

S.6 The scope of trust contains more than one authority that has access to indirect PII. The amount of authorities contained in the scope of trust is scalable.

As shown above, the possibility to make decisions about voters' behavior and to keep voter privacy depends on the corresponding scope of trust. Introducing the idea of scope of trust to the taxonomy by Langer allows us to provide a more detailed classification of her privacy levels and to see the relations between achieved privacy and scope of trust. Thus, voting schemes can be more precisely classified and be assigned to more appropriate privacy levels, although according to Langer's taxonomy they may belong to the same ones. For instance, Split-Ballot and the version of Prêt à Voter that provides long-term security [25] belong to the same privacy level, according to Langer's taxonomy. However, as we have seen above, due to their scopes of trust, we can now conclude that this version of Prêt à Voter satisfies privacy (scope of trust level S.6) better than Split-Ballot (scope of trust level S.5), since the number of key holders is scalable.

7 Conclusion

Although a tendency towards developing and applying online voting systems already exists, poll-site voting is still the most popular and most used way to vote. Existing voting systems are constantly examined and further improved, in order to satisfy certain security criteria. The goal of this bachelor thesis was to develop a taxonomy for poll-site voting schemes in terms of privacy. Taxonomies are essential since they allow us to analyze and classify systems in terms of a certain security property. Systems do not often satisfy all security properties optimally. Sometimes they trade certain properties for others. A taxonomy enables us to identify an optimal approach to classify voting systems with respect to certain requirements and properties. In this thesis, we concentrate only on privacy, but it can be regarded as a step towards a more thorough classification of voting schemes. We considered several privacy taxonomies which use different criteria to classify voting systems. Then, we compared them according to the various privacy aspects each one considers and, finally, proposed our taxonomy, based on the ideas of the already presented taxonomies.

In Section 2 we presented the fundamental terms used in this thesis. We divided them in two main categories according to whether they capture the presence of an adversary or not. We decided to differentiate between voter privacy, long-term privacy, and everlasting privacy, in order to cover more privacy aspects and, thus, present a more throrough classification of voting systems.

In Section 3 we presented five privacy taxonomies. We described their approaches for classifying voting schemes, analyzed and evaluated them, and ordered them in terms of their precision.

In Section 3.1 we presented the taxonomy by Coney et al., which is based on the idea of perfect privacy. We saw that this taxonomy is rather formal and abstract. In addition, we concluded that the deviation from perfect privacy is not a sufficient criterion for the classification of voting schemes, since it could not provide an unequivocal categorization of privacy levels.

In Section 3.2 we presented the taxonomy by Sampigethaya and Poovendran. We described the three classes they suggest, considering the way voters submit their votes to the tallying authority, and provided corresponding example voting schemes. We saw that neither of the three different approaches manage to satisfy all security properties and trade-offs. Moreover, the taxonomy does not provide a hierarchical classification among and within the classes. In addition, it allowed us to assign voting schemes to more than one class at the same time.

Section 3.3 described the taxonomy by Langer, which suggested a privacy, as well as an adversary model with distinct levels of classification. We saw that this taxonomy does not only consider weaknesses that should be avoided, but also the case, that these weaknesses yet occur, but cannot be proven to third parties. Moreover, a certain hierarchy among the levels could be observed. Based on these observations, we concluded that the taxonomy by Langer is the most thorough and precise taxonomy considered in this thesis, and used it as a basis for our proposed taxonomy in Section 6.

Section 3.4 presented the taxonomy by Dreier et al. The authors suggest a tight connection between privacy and the presence of an adversary. We saw that the taxonomy provides a thorough and hierarchical, but still rather formal classification of voting schemes.

In Section 3.5 we saw a privacy taxonomy that classifies voting schemes in terms of the used cryptographic primitives, on one hand, and in terms of achieved requirements, on the other hand. However, we saw that this taxonomy is rather imprecise, since it neither defines any distinct privacy levels, nor does it allow a unambiguous scheme classification.

What all of the presented taxonomies do not consider is the voter's trust in other participants in

the system. More precisely, who a voter should trust, in order to preseve his privacy. Therefore, in Section 5 we described a classification which does not explicitly regard voting systems, but considers the aspect of trust. We presented the taxonomy by Pleva, who provides a general classification of electronic services in terms of individual's publicity and recognisability. We regarded this section as a preparation for our proposed taxonomy.

In Section 6 we suggested our taxonomy, based on the ideas of Langer and Pleva. We transferred Pleva's notions of scope of trust and personally identifiable information to poll-site voting schemes and related the result to Langer's taxonomy. Thus, we proposed a taxonomy for poll-site voting schemes, which provided not only a privacy classification even in case of an adversary, but also a means to secure personal data as a basis for achieving privacy with respect to the trust assumptions made.

In this bachelor thesis we saw that privacy in voting schemes can be classified in terms of different criteria and provided an improved taxonomy. Since this thesis concentrates on privacy, further properties, such as integrity, efficiency, and usability were not thorougly discussed. However, they are an essential part of secure voting systems and should be a topic of future work in this field. In fact, taxonomies should be developed that analyze voting schemes with respect to all security requirements demanded for a secure voting system. In addition, such a taxnomy would not only allow to analyze the security, but also the trade-offs between different properties. Further research could be also done on secure storage of votes, which goes beyond the scope of the voting process itself, but is an important feature of private voting systems.

In conclusion, we can state that although poll-site voting systems have been used for centuries, they still have security weaknesses. As they still represent the most popular way of voting, it is essential to further research, develop, and improve them.

References

[1] Krishna Sampigethaya and Radha Poovendran. *A framework and taxonomy for comparison of electronic voting schemes*. Computers & Security 25 (2) (2006) 137-153.

[2] Sako K, Killian J. *Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth*. In: Advances in cryptology - EUROCRYPT 1995. LNCS, vol. 921. Springer-Verlag; 1995. p. 393-403.

[3] Lillie Coney, Joseph L. Hall, Poorvi L. Vora, and David Wagner. *Towards a Privacy Measurement Criterion for Voting Systems*. In National Conference on Digital Government Research, May 2005.

[4] Claude E. Shannon. *A Mathematical Theory of Communication*. Bell System Technical Journal 27 (3): 379-423.

[5] Ari Juels, Dario Catalano, and Markus Jakobsson. *Coercion-resistant electronic election*. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, WPES, pages 61-70. ACM, 2005.

[6] Chaum D. *Untraceable electronic mail, return addresses, and digital pseudonyms*. Communications of the ACM 1981;24(2): 84-8.

[7] Ronald Cramer, Gennaro Rosario, andf Berry Schoenmakers. *A secure and optimally efficient multi-authority election scheme*. In: Advances in cryptology - EUROCRYPT 1997. LNCS, vol. 1233. Springer-Verlag; 1997. p. 103-18.

[8] ElGamal T. *A public-key cryptosystem and a signature scheme based on discrete logarithms*. IEEE Transactions on Information Theory July 1985;31(4):469-72.

[9] Paillier P. *Public-key cryptosystems based on composite degree residue classes*. In: Advances in cryptology - EUROCRYPT 1999. LNCS, vol. 1592; 1999. p. 223-38.

[10] Rivest R, Shamir A, Adleman L. *A method for obtaining digital signatures and public key cryptosystems*. Communications of the ACM 1978;21:120-6.

[11] Ben Adida and Ronald L. Rivest. *Scratch & Vote: self-contained paperbased cryptographic voting*. In Workshop on Privacy in Electronic Society (WPES), pages 29-40, 2006.

[12] Tal Moran and Moni Naor. *Split-ballot voting: Everlasting privacy with distributed trust*. ACM Transactions on Information and System Security, 13(2), 2010.

[13] A. Shamir. *How to share a secret*. Communications of the ACM 1979;22(11):612-3.

[14] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch. *Verifiable secret sharing and achieving simultaneous broadcast*. In: Proceedings of IEEE foundation of computer science 1985. p. 335-44.

[15] B. Schoenmakers. *A simple publicly verifiable secret sharing scheme and its applications to electronic voting*. In: Advances in cryptology - CRYPTO 1999. LNCS, vol. 1666. Springer-Verlag; 1999. p. 148-64.

[16] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. *Prêt à Voter: a voter-verifiable voting system*. IEEE Transactions on Information Forensics and Security, 4(4), pp. 662-673, 2009.

[17] D. Chaum, R. T. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, and P. L. Vora. *Scantegrity II: end-to-end verifiability by voters of optical scan elections through confirmation codes*. IEEE Transactions on Information Forensics and Security, vol. 4, p.611-627, 2009.

[18] Lucy B. Langer. *Privacy and Verifiability in Electronic Voting*. TU Darmstadt [Ph.D. Thesis], (2010).

[19] Danny Dolev and Andrew Chi-Chih Yao. *On the security of public key protocols*. IEEE Transactions on Information Theory, 29(2):198-208, 1983.

[20] Jannik Dreier, Pascal Lafourcade, and Yassine Lakhnech. *A Formal Taxonomy of Privacy in Voting Protocols*. IEEE Workshop on Security and Forensics in Communication Systems (SFCS 12): May 2012.

[21] Martin Abadi and Cedric Fournet. *Mobile values, new names, and secure communication*. In POPL 2001, 2001, pp. 104-115.

[22] M. Backes, C. Hritcu, and M. Maffei. *Automated verification of remote electronic voting protocols in the applied pi-calculus*. CSF, vol. 0, pp. 195-209, 2008.

[23] Huian Li, Abhishek Reddy Kankanala, and Xukai Zou. *A Taxonomy and Comparison of Remote Voting Schemes*.

[24] Peter Pleva. *A Revised Classification if Anonymity Levels*.

[25] Denise Demirel, Maria Henning, Jeroen van de Graaf, Peter Y. A. Ryan, Johannes Buchmann. *Prêt à Voter Providing Everlasting Privacy*. VoteID 2013: The 4th International Conference on e-Voting and Identity, July 2013, S. 156-175.