And Paper-Based is Better? Towards Comparability of Classic and Cryptographic Voting Schemes

Marc Nemes[2], Rebecca Schwerdt[1], Dirk Achenbach[2], Bernhard Löwe, Jörn Müller-Quade[1]

[1] Karlsruhe Institute of Technology
[2] FZI Research Center for Information Technology

Abstract In today's real-world elections the choice of the voting scheme is often more subject to dogma and tradition than the result of an objective and scientific selection process. As a consequence, it is left to intuition whether the chosen scheme satisfies desired security properties, while objectively more suitable schemes might be rejected without due cause. Employing a scientific selection process to decide on a specific voting scheme is currently infeasibly cumbersome. Even those few schemes which have been thouroughly analyzed do not provide easily comparable analysis results or fail to provide the information desired for real-world application. Hence there is a strong need to increase meaningful comparability, allowing democracies to choose the voting scheme that is best suited for their setting.

In this paper we analyze which factors currently impede the comparability of both classic and cryptographic voting schemes and which information is needed to facilitate meaningful comparisons. As a first result we find that there is a severe lack of general understanding of the workings and properties of the classic paper-based systems which are in use around the world today. In this we highlight that commonly voiced intuitive comparisons—especially to classic paper-based voting—lack the necessary scientific basis and are therefore no sufficient foundation.We then develop an analysis framework to concisely showcase the most important characteristics of a voting scheme as well as to enable comparisons to other schemes. The utility of our analysis framework is demonstrated by analyzing and comparing two examples. Our work underlines the need for more academic work towards the comparability of voting schemes and lays a foundation for addressing this issue.

Keywords: E-Voting · Paper-based Voting · Security Analysis · Comparability.

1 Introduction

In a speech on January 6, 2021, then-US-President Donald Trump claimed the 2020 United States presidential election had been subject to election fraud, thus

costing him his second term of presidency. Due to believing in a stolen election protesters violently stormed the US Capitol. A more transparent and verifiable voting system for the US presidential election might not have prevented the events leading up to the storming of the US Capitol. It would, however, provide less fertile soil for *unfounded* claims of a stolen or correct election. Instead it would be easily verifiable whether election fraud has taken place or not.

For similar reasons of intransparency, electronic voting systems are usually considered inappropriate for real-world applications: Cryptographic methods can make tally results *provably* correct, but are too hard to follow as a layman. Paper-based voting on the other hand is commonly depicted as the gold standard compared to cryptographic systems, as anyone can comprehend and observe the election process—such is the common assumption. Most comparisons, however, regardless of in-person, e-voting, paper-based or cryptographic voting schemes, lack an objective scientific basis and are subject to intuition, opinion and tradition. Hence there is a strong need to increase meaningful comparability, allowing democracies to choose the voting scheme that is best suited for their setting.

1.1 Related Work

Previous work in this sector focuses almost exclusively on the security and comparison of cryptographic voting schemes. Li et al. [19] provide a survey comparing 14 voting schemes in terms of different security guarantees. However, their survey only contains cryptographic voting schemes and concentrates on properties, ignoring the underlying assumptions. As a survey their work also does not provide a general framework to compare new and existing voting schemes. Neumann et al. [21, 22] provide frameworks for the evaluation of voting schemes which are also restricted to internet voting. Kulyk et al. [17] compare several voting schemes for boardroom voting but mainly focus on efficiency. Nevo et al. [23] actually compare online voting with classical voting schemes. Their focus lies on different threats, their likelihood and magnitude when using one voting scheme over the other. Willemson [40] shows several weaknesses of paper based voting schemes, claiming they are mainly preferred due to historical experience, not because they are actually more secure than electronic voting schemes. Pieters [31] offers a framework to compare electronic voting schemes and paper based voting schemes based on familiarity, confidence and trust. Schneider et al. [34] focus only on the effects of electronic voting on the voter choice, compared to paper based voting schemes. Hoffmann et al. [11] try to translate (often ambigious) legal texts into a more technical list of requirements, which would make an objective analysis of paper based voting schemes easier. There are also several papers about the comparison or analysis of the security of postal voting [12, 15, 16, 32]. Therefore, to the best of our knowledge, there is only little published work about the weaknesses and fundamental security of classical, paper based in-person voting schemes.

1.2 Our Contribution

We start by providing a detailed analysis of classic paper-based voting systems in Section 3. This yields the first important result of our work: One can hardly speak about *the* paper-based voting scheme per se, as different electoral systems around the world employ vastly different schemes when looked at in detail. In this analysis we also discover which factors currently prevent meaningful comparisons to classic voting systems employed by today's democracies. In Section 4 we give a brief overview of the cryptographic voting system landscape. We again find that security analyses can seldomly facilitate comparisons between different systems. This leads us to develop a new flexible analysis framework aimed specifically at an improved comparability in Section 5. Our model captures the interplay of security guarantees, the levels of trust placed in different protocol components, the levels of security thus achieved, and the level of rigor in the underlying security analysis. It thus facilitates an easier and objective discussion about the security properties of election schemes—traditional and cryptographic schemes alike. We demonstrate the utility of the framework via two examples in Section 6. In Section 7 we conclude with our vision of how the voting research community could jointly improve one of the foundations of democracy.

2 Preliminaries

A *voting system*, *voting scheme* or *voting protocol* is an algorithm to map individual voter choices to a complete tally of those choices. Voting systems generally come with various parameters, such as a list of eligible voters and the choices each voter has. Determining the list of eligible voters as well as defining valid choices do *not* fall within the scope of the voting system, but are rather handled as fixed inputs provided by the specific election. The scope of the voting system ends with the final result of the tally. How such a tally result translates to political consequences, e.g. how many seats a certain party gets in a parliament when they received x votes, lies outside the scope of the voting scheme.

An *election* is a single instance of the actual usage of the voting system which also fixes all the voting system's parameters.

The central entity organizing/conducting an election is called the *voting authority*. It is needed in virtually every voting system but has a varying amount of duties and required trustworthiness depending on the particular scheme.

Properties we desire in voting schemes usually fall under one of three broad categories: *Correctness*, *privacy* and *verifiability*. We discuss these in more detail in Sections 3.2 and 5.

3 Classic Paper-Based Voting Systems

In this chapter we highlight factors which currently impede meaningful comparisons with classical paper-based voting schemes. Firstly, contrary to common conception there is not *the* classic paper-based voting scheme, but rather a large

inhomogeneous field—see Section 3.1. Secondly, paper-based schemes have (to the best of our knowledge, cp. Section 1.1) not only not been subject to formal security analyses, but that efforts in that direction would currently be hampered by different lacks of specification. Details on this can be found in Section 3.2.

3.1 Commonalities and Vital Differences

When thinking of "classic paper-based voting schemes" people will usually have an intuitive understanding of how such a system works. Part of this understanding is well-founded in the common structure which most of the currently employed political voting schemes share. But part of it will also stem from wrongly generalizing the particular system we know from our own home country—which, for most people, is the only system they ever come in close contact with. In this section we will discourage such generalizations by highlighting not only the commonalities but also some significant differences between voting systems employed in different countries. This shows that there is not *the* classical paper-based scheme we can use as a global reference point for comparisons.

Commonalities. One of the many commonalities of paper-based voting schemes is their tiered voting officer system [8, §8; 9, §§1-3,6-8; 20, §§17,23,29,30; 25, §13A-13CC; 33, §§2(1),19(1)]: Usually, a national voting authority assigns local voting officials and assistants to each polling station. They furthermore determine and notify eligible voters. On election day, a voter goes to a polling station where they authenticate themselves and receive a ballot. In a private polling booth, the voter marks their choice and hides it by folding the paper or inserting it into an envelope before placing it in a ballot box.

Despite this common structure significant differences between systems are found at each aspect of the election. We highlight examples in key areas.

Authentication. Possibilities are identification via ID-card (mandatory [7, §41; 26, §61(b)] or by request only [9, §56 (3),(6); 20, §47; 33, §32(1)]) and/or handing in specially issued voting documents [9, §56(1),(3); 20, §47] which are compared to the eligible voters lists present at the polling station. Sometimes, however, when voters are visibly marked once they cast a vote (e.g., with special ink on a finger) [26, §61(a),(b); 33, §§30(2),32(2)(c)], being present at the polling station and not being marked yet can be the only authentication mechanism.

Ballot marking. Ballots are often marked with a pen by crosses or tickmarks [7, §42; 8, §34(2); 20, §48(1)]. To prevent recognizably marked ballots which may be matched to a certain voter during the counting phase, ballots with additional markings or scribbles are often declared invalid [8, §39(1); 20, §69(1)(v),(2)(vi); 29, §47(1)(c); 33, §39(1)(d)]. Alternatively, choices may be indicated by handing in preprinted voting slips/ballots which only contain the selected choice and do not have to be marked at all [36, §§75(a),76(a)]. On the other hand, there are countries where write-in candidates are allowed or ballots with individual markings or scribbling on them are still valid [7, §42(b)]—allowing voters to, for

instance, sign their name and thus give up voting secrecy. There are even countries where choices are marked with the voter's fingerprint in ink [33, §33(3)(b)] or where the connection between the voter and vote is explicitly established by a unique ballot ID which is documented in the list of voters to facilitate traceability of individual votes [29, §§19(2)(c),37(1)(b)]. These different mechanisms have very different implications for the systems' levels of privacy and verifiability.

Verifiability. We find more differences in the permission of observers. Sometimes everyone is allowed to watch the whole voting and/or counting process in any polling station [7, §32; 8, §31; 9, §54], giving the media, external observers, but particularly voters, some form of verifiability. However, it is hardly possible for individuals or even small organized groups to observe the process everywhere. In other cases only eligible voters are admitted into the polling station and they have to leave again as soon as they are done casting their vote [20, §51; 33, §33(4)]. In these systems usually only very specific observers are allowed—like representatives of international organizations or the parties/candidates nominated for election [7, §§29-31; 26, §§20B,50; 29, §32; 33, §§21,37; 36, §73].

Tally. Mostly, ballot boxes are opened and tallied directly within the individual polling stations [7, §§13,39(a); 9, §§67,69; 20, §68(1); 26, §64; 29, §45; 33, §§19(2)(h),38] with partial results being announced there [7, §16; 9, §70; 20, §70; 33, §§19(2)(i),38(3)(a)]. This exchanges the need to transport ballot boxes in a secure way for the need to securely communicate partial results. Other systems tally in one or multiple central locations [20, §72(1)] or explicitly require ballots from one ballot box to be mixed with those of others [29, §45(1A)]. This prevents detailed partial results to be known even to the counting officials.

Many of these differences may seem "only organisatorial". But they also have implications for the voting schemes' levels of privacy, security and verifiability. Note also that these are merely illustrating examples. A detailed comparison of individual schemes would show even more differences—not only in the processes, but also the resulting properties. We do not claim this to be a drawback of the current voting landscape. On the contrary, tayloring a voting scheme to the specific public infrastructure as well as threat levels in the particular democracy is an expedient practice. The scientific and political voting community should, however, be aware how heterogeneous the landscape of classic paper-based voting system is and refrain from comparisons to just "classic paper-based voting".

3.2 Lack of Specification and Security Analysis

The heterogeneous field of paper-based voting systems discovered above does not preclude meaningful comparisons per se. It just highlights the need to specify which exact system something is compared to. Unfortunately comparing another voting system to current solutions is impeded by several other factors.

Some building blocks are used with clear and known (security) intentions: a list of voters is essential to allow at most *one vote per eligible voter*, the voting

booth supports the *privacy of the ballot* and the ballot box helps that *ballots cannot be removed* or *linked to the voter*. Unfortunately, this level of reasoning is commonly the extent of any "security analysis" of classic paper-based voting schemes. We will go into more detail on this and other problems in this section.

Specification. The first problem we encounter is lack of specification. Even though election legislation is often very complex and detailed, most countries lack precise (publicly known) instructions. One common example are modes of transportation and communication: How are ballots transported, and by whom? How are partial tallys communicated? If we do not fully know a scheme, we can not analyse it. Note that the highly praised simplicity of classical voting protocols only applies to the basics. Knowing and understanding every aspect of such a protocol not only exceeds the comprehension of numerous voters but is not possible at all if not every detail of the process is specified and publicly known.

Properties. To the best of our knowledge, there are no formal definitions of desired security properties. Constitutions and international agreements on voting rights give only broad goals like freedom of voting choice or secrecy and equality of votes [6, §26(a); 27, §49(1); 35, §5; 37, §21(3); 38, §25(b); 39, §38]—but leave it to courts to decide whether they are fulfilled or not. And courts usually only deal with this question if someone objects to the current system. As long as clear definitions are lacking, it is impossible to rigorously analyze whether a voting scheme satisfies the required properties.

Security Analysis. Thirdly, we find a lack of security analyses and even security intentions. Most schemes were developed a long time ago and modified often, making it unnecessarily infeasible to get a comprehensive documentation of the reasoning behind some design decisions. While some fundamental ideas of the protocols are clear, legislation on the voting process only states what is to be done without any explanation on why certain provisions are taken, let alone what they actually achieve. For example, it is not trivial to understand if a ballot is identifying and who might be able to trace the vote to the voter. Two examples of this are the unique identifying marks on British ballots [29, §§19(2)(c),37(1)(b)] and the fingerprinted ballots in Ghana [33, §33(3)(b)]. In the UK each ballot has a number or unique identifying mark on the back and a list of which voter filled out which ballot is maintained [29, §§19(2)(c),37(1)(b)]. Hence individual votes are definitely identifying and traceable. During the tally the counting officer is required to count ballots face up so (hopefully) nobody can see both the ballot number and the voter's choice. All people present are asked to maintain secrecy in case they do learn identifying information [28, §66(2)(a); 29, §45(4)]. In Ghana the voter indicates their choice with an inked thumbprint [33, §33(3)(b)]. Since the thumbprint is also part of the biometric identification during voter registration, this indicates ballots are meant to be identifying. On the other hand there are no provisions to ensure that the thumbprint (secretly made in the voting booth) is clear enough to be identifying [33, §§33,39(1)]. This technique may lead to traceable ballots but it is not apparent whether this is intended. Not

knowing the reason and consequences of design decisions does not only encumber security analyses but allows for much easier coercion as voters are less sure about the information an adversary may plausibly obtain.

Many countries seem to be aware that unique ballot marking is a problem. But even those with special measures against this do not fully address the problem. Take for instance the Israeli system [36, §§75,76,78]: The voting booth contains preprinted slips of paper with a single party on them. The voter inserts a single slip of their choice into an envelope. This method prevents unique marks on the ballot but leads to a stateful voting both and thereby new problems: Someone could count how many slips of each party are present before and after someone else votes. Hence voters are also allowed to take a blank slip and write the name of their preferred party onto it—which leads to unique marks again. This example highlights the need to know the intended purpose of certain provisions and to investigate whether they actually achieve it.

Assumptions. Lastly, the lack of security analyses also yields a lack of understanding which assumptions schemes rely upon. In contrast to cryptographic schemes, classic paper-based voting mainly relies on physical assumptions—like the ballot box mixing votes to break linkability to voters. This particular example may be obvious and is sometimes even specifically provisioned for in the voting regulations [9, §51(2)]. However, there are other assumptions we make without even mentioning them, e.g., that the ballot paper and pen cannot convey the voter's choice to an adversary. This assumption may already be violated when voters are able to use individual pens (like a certain color) or mark the ballot in a recognizable way. Considering chemically advanced paper and ink it would even be thinkable that the ballot paper erases the mark by the voter and optionally creates a new one next to a different candidate. An attack like this might have seemed like science fiction when older western democracies developed voting schemes decades ago. Today, they are already possible. The future scientific and technological developments will bring other attacks within the scope of possibility. Think, for instance, about the technological advancements in small scale camera technology in the last 100 years. Apart from these "physical" assumptions, trust assumptions—e.g. that the voting authority as a group has to be trusted—have to be considered as well. Without a security statement indicating which properties a scheme can provide under which assumptions, it is very likely only the most obvious assumptions (like a large enough ballot box) receive any kind of attention and are provisioned for. At the same time other assumptions will still be relied upon although they are clearly not true (anymore).

In this section we have seen that meaningful comparison between newly proposed voting schemes and classical paper-based voting is currently infeasible. Although many examples we found throughout Section 3.1 indicate that classic voting systems do not constitute the fully satisfying gold standard some people still believe them to be. Incomparability is not only based on the largely ignored fact that the field of currently employed solutions is very heterogeneous. More importantly we found that, as of yet, classical paper-based schemes lack the nec-

essary rigorous and thorough specification as well as formal security and privacy analysis to serve as a basis for comparison. We think it an important societal goal to close these gaps.

4 Cryptographic Voting Systems

In this section we discuss specifics of cryptographic voting schemes and problems which hinder their comparability. In some aspects, like tallying speed, cryptographic voting schemes are already superior to classical voting. With scientific analysis and comparison between the two, the advantages of certain cryptographic voting schemes might be found to outweigh their disadvantages, making it reasonable to use them in increasingly many environments. It is up to the entity conducting an election to decide which properties constitute a sufficiently secure system to be used in their election. But even before cryptographic solutions are deemed secure enough to be used in large-scale political elections, we can learn from research into cryptographic voting schemes to improve existing voting systems. But not all of the cryptographic schemes are intended for large-scale political elections, but were developed with different application environments in mind, providing a very heterogeneous landscape as well: Consider the examples of Helios, Scantegrity II, and Wombat Voting. Helios [1] is a web-based open-audit voting system for low-coercion risk environments, like local clubs. Scantegrity II [5] offers a verifiable voting scheme intended to feel like a conventional optical scan system for voters who are not interested in verifying their vote. Wombat Voting [4] focuses on simplicity of design and compatibility with more traditional, paper-based, voting systems [2].

Properties. Different systems not only aim at and provide different security guarantees, but their analyses often use different definitions of verifiability, correctness or coercion resistance [10]. This makes comparisons very tricky, as schemes provide incomparable properties under the same name.

Security Analysis. On top of that there is a large margin in the extent and quality of the provided security analyses and proofs. Authors of a new voting protocol can promise paramount secrecy and foolproof verifiability, but as long as these statements are only based on conjectures without any formal proofs they can't be used in actual elections in good conscience.

Assumptions. While paper-based voting uses mainly physical assumptions, cryptographic voting schemes use building blocks based on math and logic. We do not discuss cryptographic building blocks further at this point but refer the reader to Peacock et al. [30] and van Oorschot [24, p. 29-53]. We want to stress however, that cryptographic voting schemes rely on vastly varying assumptions—mathematical as well as trust assumptions. This is vital for meaningful comparisons but unfortunately mostly ignored so far.

These issues hamper the comparability of cryptogrpahic voting protocols and therefore make it difficult to pick the best suited voting protocol. We try to make this decision easier in the future in the following section.

5 Voting System Analysis

To give a quick overview of a voting scheme and its most crucial components and to allow for easier comparison between two voting schemes, both paper-based and cryptographic, we introduce a matrix notation. Rows in the matrix correspond to security guarantees of the voting scheme, like coercion-resistance or correctness, while columns correspond to the different components of the voting protocol, like a ballot box, Random Number Generator, commitment scheme or a local voting authority. We use the term component instead of party in order to avoid confusion with political parties. A component can be a subset of another component, e.g., a local voting authority can be viewed as a subset of the global voting authority. Elements of the matrix are described by the trust needed in their respective component in order to guarantee the given level of security for the property in this column. See Table 1 for the general structure of this matrix. Two examples can be found in Section 6. Our goal is for creators of new voting protocols to use this notion to generate a matrix for their voting protocol, which can then be compared to other matrices. In the long run, this data could be stored in a database to allow users to get an overview of voting schemes that potentially match their desired criteria.

	Component_1	$\cdots$	Component_N	Level of Sec.	Proof
Sec. Guarantee_1	Level of Trust	$\cdots$	Level of Trust	Level of Sec.	Level of Proof
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
Sec. Guarantee_M	Level of Trust	$\cdots$	Level of Trust	Level of Sec.	Level of Proof

Table 1. General Structure of Analysis Matrix

5.1 Level of Security

When analyzing the security of voting protocols, individual and universal verifiability are often brought up, mostly in the context of a correct tally. We think that every aspect of a voting protocol must be easily verifiable by every voter, either by being impossible to be otherwise by design (e.g., backed by a mathmatical proof), by giving voters a specific receipt, letting them observe the ballot box or the like. Therefore, each row of the matrix must be assigned one of the following levels of security.

- **Satisfied**: The aspect is satisfied with overwhelming probability.
- **Correctable**: The aspect is not fully satisfied, but discrepancies are detected and corrected efficiently with overwhelming probability following a predefined process.
- **Detectable**: The aspect is not fully satisfied but discrepancies can be detected with overwhelming probability. However, the discrepancies cannot be corrected efficiently with overwhelming probability.
- **Not Satisfied**: The aspect is not fully satisfied and discrepancies cannot be detected with overwhelming probability.

5.2 Proof

For a better comparison of the trustworthiness of a given level of security, the quality of the proof level must be stated.

- **Verified Proof** (✓): The level of security is supported by a formal proof which has been understood and verified by independent scientists.
- **Proof** (📄): The level of security is supported by a formal proof.
- **Proof Sketch** (💡): There doesn't exist a formal proof supporting the level of security, but the authors justify the result by providing a proof sketch which can be turned into an actual proof.
- **Conjecture** (×): The rating of the level of security is based on claims without formal proofs or proof sketches.

5.3 Trust and Corruption

Entries of the matrix are given keywords depending on the level of required trust:

- **Corrupted** (c): the component in this column can be assumed corrupted without affecting the level of security for the security guarantee in this row.
- **Honest-But-Curious** (h): the component in this column may disclose any data it learns, but must strictly stick to the voting protocol in order to guarantee the level of security for the security guarantee in this row.
- **Trusted** (t): the component in this column must strictly stick to the voting protocol and may not disclose any data it learns in order to guarantee the level of security for the security guarantee in this row.

If a component has no influence on a security guarantee, that is, if changing the cell's keyword does not change the property's level of security in any case, it can be left blank. If a component consists of multiple people or components, every component needs to be trusted or honest-but-curious in order to be trusted or honest-but-curious as a whole. If a trusted component is controlled by another component, indirect trust in the other component is required, e.g., if we need to trust a ballot box for the correctness of the tally and the ballot box is controlled by a local voting authority, then we have to trust the local voting authority as well. If there is an indirect trust requirement, we add an asterisk to the entry of the controlling component in the matrix, e.g. h^* or t^*. For a quicker overview, we color matrix cells depending on their value, with *corrupted* cells being marked in green, because it is desirable that components can be corrupted without affecting the level of security.

5.4 Security Guarantees

While the rows (security guarantees) of the matrix can easily be altered or expanded, we propose the following guarantees to ensure comparability between schemes and a broad coverage of desirable properties.

Fairness: A fair voting protocol treats all eligible voters equally. A voter does not have an advantage or disadvantage by casting her vote early or just before the voting phase ends.

- **Equality of Choice**: Any two voters swapping their preference on their ballots does not change the outcome of the tally.
- **Same Knowledge for All Voters**: Each voter has access to the same information before casting her vote. This excludes intermediate results.
- **Same User Experience for All Voters**: Each voter has the same user experience. This excludes ballot papers in random ordered lists.

Privacy: To guarantee that the tallying result reflects the actual choices of voters no one but the voter herself can gain any information about her vote.

- **Voter's Choice (Strong)**: Nobody besides the voter herself can learn any information about her choice.
- **Voter's Choice (Weak)**: Nobody besides the voter herself can learn which candidate she voted for.

Coercion: It should be impossible to deny a voter some of the voting choices or even force her to vote for a specific voting choice. More information about these attacks can be found in the works of Juels et al. [14] and Jones [13].

- **Forced-abstention attacks**: Nobody besides the voter herself can learn whether she voted. Nobody can force a voter to cast an invalid ballot.
- **Randomization attacks**: Nobody can force a voter to submit randomly composed ballot material.
- **Simulation attacks**: Nobody can get enough information from voters to simulate these voters at will, i.e voting on their behalf.
- **Chain Voting**: Nobody can force a voter to cast a pre-marked ballot and return an empty ballot back to them.

Correctness: To prevent manipulation of the election the tallying result may only depend on the actual votes of honest voters.

- **Cast as Intended**: Cast ballots contain a vote for the voter's intended candidate [3].
- **Recorded as Cast**: Ballots are succesfully recorded and are not altered in a way that distorts the intented vote [3].
- **Counted as Recorded**: The tallying result is an actual evaluation of all stored, valid ballots [3].
- **Ballot Stuffing**: Ballots can only be added via the official voting process and nobody can add more ballots than they were allowed to add.
- **Ballot Removal**: Ballots can only be removed via the official voting process once they are cast (e.g., revoting).

Resilience: An attacker that cannot manipulate the election in his favor can still try to sabotage the different election phases if he expects to lose the election. That way he might be able to delay an election or arrange new elections where he has better chances at winning.

- **Voting-Phase**: No eligible voter can be denied from voting during the voting phase.
- **Tally-Phase**: The voting authority can not be hindered from counting all recorded ballots during the tallying phase.
- **Verification-Phase**: Voters can not be hindered from veryfing their vote.
- **No unjustified complaints**: Nobody can falsely claim election fraud without being detected, e.g., claiming that a code from an uncast ballot came from a cast ballot.
- **Recountability**: The votes can be recounted to verify the result of the initial count as often and long as required by the statutory basis.

6 Examples

We show the applicability of our matrix approach in two voting schemes—one classical, the German Federal Election [8, 9], and one cryptographic, Scantegrity II [5]. We limit the example matrices to what we consider the most important security guarantees. Tables 2 and 3 show the most insightful parts of the matrices, based on our understanding of the two voting protocols. Some parts of the German Federal Electoral Code hint towards measurements against fraud etc. As no written explanation is given why these measurements are employed, we don't count these hints as proof sketches.

6.1 Comparison

The global and local authority seem to be an essential part of both protocols, required to be at least honest for most of the security guarantees, due to their control over several components. Also, observers at a polling station may often detect a cheating voting authority, but in the time it takes them to issue a complaint to the global voting authority, most of the evidence is lost. A new election with a different local voting authority is the only fix. Even when all components can be assumed trusted, both voting protocols are susceptible to forced abstention attacks, which seems to be an issue for all in-person voting protocols. Overall, the level of security is similar in both schemes, although they use different building blocks to reach their goal. Scantegrity II, being an electronic voting scheme, relies on extra and more complex building blocks, which then result in a faster tally. We can see that for the german federal election, most guaranteed properties are based on conjectures, with no proof or any written explanation. While it is easy to see that the level of security is correct for some of the security guarantees, this observation validates our point that there is no written analysis of the security of paper-based voting schemes. Scantegrity II on the other hand supports every security guarantee with at least a proof sketch, and there even exist verified proofs for the coercion-related security guarantees.

German Federal Election	Component: Ballot	Pen	Ballot Box	Voting Booth	Printer	Identity Card	Voting Card	Local Electoral List	Global Voting Authority	Local Voting Authority	Voter	Observers	LoS: Level of Security	Proof
Privacy														
Voter's Choice (Strong)	t	t	t	t	h*				h*	h	t	c	Satisfied	× [9]
Voter's Choice (Strong)	c	c	c	c	c				h	c	t	h	Detectable	× [9]
Voter's Choice (Weak)	t	t	t	t	h*				h*	h	t	c	Satisfied	× [9]
Voter's Choice (Weak)	c	c	c	c	c				h	c	t	h	Detectable	× [9]
Coercion														
Forced-abstention attacks													Not Sat.	
Randomization attacks	t	t	t	t	h*				h*	h*	t	c	Satisfied	×
Simulation attacks						h	h		h*	h		c	Satisfied	× [9]
Simulation attacks						h	h		h	c		h	Detectable	× [9]
Correctness														
Cast as intended	h	h			h*				h*	h*	h	c	Satisfied	× [9]
Recorded as Cast			h						h*	h*		c	Satisfied	× [9]
Counted as Recorded									h*	h		c	Satisfied	× [9]
Counted as Recorded									h	c		h	Correctable	× [9]
Ballot Stuffing			h				h	h	h*	h		c	Satisfied	×
Ballot Stuffing			c				h	h	h*	h		c	Detectable	×
Ballot Stuffing			h				h	c	h*	h		c	Correctable	×
Ballot Stuffing			h				c	h	h*	h		c	Correctable	×
Ballot Stuffing			c				h	c	h*	c		h	Detectable	×
Ballot Removal	h		h		h*		c	c	h*	h		c	Satisfied	× [9]

Table 2. Excerpt of the matrix for the German Federal Election.

Scantegrity II	Component: Ballot	Magic Pen	Invisible Ink	Voting Booth	Scanner	Printer	Identity Card	Voting Card	Local Electoral List	Bulletin Board	Computation Platform	Global Voting Authority	Local Voting Authority	Voter	Observers	Confirmation Codes	Serial Number on Ballot	Commitments	LoS: Level of Security	Proof
Privacy																				
Voter's Choice (Strong)	t	t	c	t	t	h*					t	h*	h	t	c	t		t	Satisfied	[5]
Voter's Choice (Weak)	t	t	c	t	t	h*					t	h*	h	t	c	t		t	Satisfied	[5]
Coercion																				
Forced-abstention att.																			Not Sat.	✓ [18]
Randomization att.	t	t	c	t	t	h*						h*	h*	t	c	c			Satisfied	✓ [18]
Simulation attacks							h					h*	h		c	c			Satisfied	✓ [18]
Simulation attacks							h					h	c		h	c			Detectable	✓ [18]
Correctness																				
Cast as intended	h	h	h		h*							h*	h*	h	c	c	c		Satisfied	[5]
Recorded as Cast				h						h		h*	h		c	c	h		Satisfied	[5]
Counted as Recorded											h	h*	h		c	c	c	h	Satisfied	[5]
Counted as Recorded											c	h*	h		c	c	c	h	Detectable	[5]
Ballot Stuffing				h			h	h	h	h	h	h*	h		c				Satisfied	[5]
Ballot Stuffing				c			h	c	c	c	c	h*	h		c				Detectable	[5]
Ballot Stuffing				c			c	h	c	c	c	h*	h		c				Detectable	[5]
Ballot Stuffing				c			h	c	c	c	c	h*	c		h				Detectable	[5]
Ballot Removal	h			c	h*		c	c	h	h	h	h*	h		c				Satisfied	[5]

Table 3. Excerpt of the matrix for Scantegrity II.

7 Vision

We identified a number of desirable improvements in this paper—to paper-based elections as well as to cryptographic schemes. The broad spectrum of shortcomings raises the question which main topics should be addressed scientifically in the upcoming years. In our opinion it is important to rigorously analyze existing systems (Section 3) and to further improve the comparability of voting schemes (Section 5)—starting with the definition of explicit security goals. These serve as a basis for security proofs and comprehensible explanations of security properties to the voters.

In addition to an increased transparency for the voters, the usability of voting systems has room for improvement. Voting should be as easy as possible to avoid unintentional mistakes as well as coercion based on a voter's uncertainty. Some of the baseline guarantees voting schemes need to fulfill are well-recognized, like coercion resistance or verifiability. Others currently seem to be ignored mostly because they are impractical to achieve—like formal security proofs for software or trust-redundancy. In a trust-redundant system, its trust anchor is comprised of a scalable group of people or components. Of this group only a subset needs to be trustworthy or cooperative—like in a mix-net, where one correct mix step suffices to ensure security. Different users may trust different subsets of this group.

Besides diligently documenting all assumptions (see Section 5), researchers should aim at using less assumptions to fulfill more guarantees. The prospect of automatically verifying all the software used in a voting scheme is promising. A different avenue for future research is voting schemes whose security guarantees are independent of the software—if the voter receives a correctly-formulated receipt, the voting software cannot have cheated.

We have identified four design principles that seem to help avoid difficult-to-achieve assumptions: Firstly, no component with a computing unit or memory is aware of the voter's choice. Secondly, all components ensuring an aspect of security must be trust-redundant in the system. Thirdly, remaining attacks must not scale well; it must be expensive to perform an attack that affects enough ballots to change the outcome of the election. Lastly, the system's security should be independent of the concrete software implementation.

It is our hope that the scientific community continues to work together to improve democratic decision making wherever elections are free and equal.

8 Conclusion and Future Work

Meaningful comparisons between different voting schemes are currently infeasible to a large extent. In particular, comparisons to currently employed paper-based systems are difficult, because the latter lack a proper scientific analysis. But comparisons to and between cryptographic voting systems also suffers from a lack of formal analysis, inhomogeneous definitions and an exclusive focus on security guarantees without concern for the underlying assumptions.

With the matrix-based analysis method we proposed in Section 5 it is possible to mitigate these problems and give interested parties a solid basis on which to find the best system for their purpose.

We see several directions in which this method might be further expanded and improved upon. The usual aim of a security analysis is to give *maximal* configurations of corruption under which a property is *still fullfilled* and *minimal* configurations under which a guarantee can *already* be *broken*. This is done under the plausible assumption that there is some form of continuity, i.e., the more corruption and the less trust, the fewer properties can be provided by the system. There are, however, examples to contradict this: Most guarantees are given with respect to honest parties, e.g., "privacy" usually implies that a system protects the privacy of honest (or coerced), but not maliciously corrupted, voters. Too many corruptions will violate privacy, but if every voter is corrupted, privacy is trivially satisfied. We think the question whether there are any meaningful examples violating continuity merits further research. The trust model we use in this paper is rather basic. If several components are merged, e.g., several people into one voting authority, they are required to all fulfill (at least) the trust level stated for the whole group. Many building blocks, however, can facilitate more involved (and strictly weaker) trust assumptions like having at least k out of n honest components. Our analysis framework can currently only represent this by considering all members of the group individually. In the future we hope to find methods to concisely integrate this into our analysis method.

References

1. Helios Voting, https://vote.heliosvoting.org/ Accessed: 2021-05-01
2. Wombat Voting System, https://wombat.factcenter.org/ Accessed: 2021-05-01
3. Ali, S.T., Murray, J.: An overview of end-to-end verifiable voting systems (2016)
4. Ben-Nun, J., Fahri, N., Llewellyn, M., Riva, B., Rosen, A., Ta-Shma, A., Wikström, D.: A new implementation of a dual (paper and cryptographic) voting system. In: 5th International Conference on Electronic Voting 2012 (EVOTE2012). Gesellschaft für Informatik eV (2012)
5. Chaum, D., Carback, R.T., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y.A., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity ii: End-to-end verifiability by voters of optical scan elections through confirmation codes. IEEE Transactions on Information Forensics and Security **4**(4), 611–627 (2009). https://doi.org/10.1109/TIFS.2009.2034919
6. Deena Hussain at the Request of Ministry of Legal Reform, Information and Arts: Functional Translation of the Constitution of the Maldives (2008)
7. Elections Commission of the Maldives: The Presidential Election Regulation (2013)
8. German Bundestag: Federal Election Law (in German), BGBl. I S. 1288, 1594, 2395 (1993), english Translation: https://www.bundeswahlleiter.de/en/dam/jcr/4ff317c1-041f-4ba7-bbbf-1e5dc45097b3/bundeswahlgesetz_engl.pdf Accessed: 2021-05-13
9. German Federal Ministry of the Interior, Building and Community: Federal Election Regulations (in German), BGBl. I S. 1769 (ber. 258), 1328, 1329 (1985), english Translation: https://www.bundeswahlleiter.de/en/dam/jcr/e146a529-fd3b-4131-9588-8242c283537a/bundeswahlordnung_engl.pdf Accessed: 2021-05-13

10. Haines, T., Smyth, B.: Sok: Surveying definitions of coercion resistance (2020)
11. Hoffmann, A., Schulz, T., Hoffmann, H., Jandt, S., Roßnagel, A., Leimeister, J.M.: Towards the use of software requirement patterns for legal requirements (01 2012). https://doi.org/10.2139/ssrn.2484455
12. Isobel White: Postal voting and electoral fraud 2001-09 (03 2012)
13. Jones, D.W.: Chain voting (08 2005)
14. Juels, A., Catalano, D., Jakobsson, M.: Coercion-Resistant Electronic Elections, pp. 37–63. Springer Berlin Heidelberg, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12980-3_2, https://doi.org/10.1007/978-3-642-12980-3_2
15. Killer, C., Stiller, B.: The Swiss Postal Voting Process and Its System and Security Analysis, pp. 134–149 (09 2019). https://doi.org/10.1007/978-3-030-30625-0_9
16. Krimmer, R., Volkamer, M.: Bits or paper? comparing remote electronic voting to postal voting. pp. 225–232 (01 2005)
17. Kulyk, O., Neumann, S., Budurushi, J., Volkamer, M., Haenni, R., Koenig, R., Von Bergen, P.: Efficiency evaluation of cryptographic protocols for boardroom voting. In: 2015 10th International Conference on Availability, Reliability and Security. pp. 224–229 (2015). https://doi.org/10.1109/ARES.2015.75
18. Küsters, R., Truderung, T., Vogt, A.: Proving coercion-resistance of scantegrity ii. In: Soriano, M., Qing, S., López, J. (eds.) Information and Communications Security. pp. 281–295. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
19. Li, H., Kankanala, A., Zou, X.: A taxonomy and comparison of remote voting schemes. pp. 1–8 (08 2014). https://doi.org/10.1109/ICCCN.2014.6911807
20. Ministry for Economic Affairs and the Interior: Folketing (Parliamentary) Elections Act of Denmark, Consolidated Act No. 369
21. Neumann, S., Volkamer, M.: A holistic framework for the evaluation of internet voting systems. pp. 76–91 (01 2014). https://doi.org/10.4018/978-1-4666-5820-2.ch004
22. Neumann, S., Volkamer, M., Budurushi, J., Prandini, M.: Secivo: a quantitative security evaluation framework for internet voting schemes. Annals of Telecommunications **71** (06 2016). https://doi.org/10.1007/s12243-016-0520-0
23. Nevo, S., Kim, H.: How to compare and analyse risks of internet voting versus other modes of voting. EG **3**, 105–112 (01 2006). https://doi.org/10.1504/EG.2006.008495
24. van Oorschot, P.: Cryptographic Building Blocks, pp. 29–53 (04 2020). https://doi.org/10.1007/978-3-030-33649-3
25. Parliament of India: The Representation of the People Act, Act No. 43 (1950)
26. Parliament of India: The Representation of the People Act, Act No. 43 (1951)
27. Parliament of the Republic of Ghana: The Constitution of the Republic of Ghana (Amendment) Act, 526th Act (1996)
28. Parliament of the United Kingdom: Representation of the People Act (Consolidated Version) (1983)
29. Parliament of the United Kingdom: Representation of the People Act (Consolidated Version), Schedule 1 (1983)
30. Peacock, T., Ryan, P., Schneider, S., Xia, Z.: Chapter e90. Verifiable Voting Systems (12 2013). https://doi.org/10.1016/b978-0-12-803843-7.00090-9
31. Pieters, W.: Acceptance of voting technology: Between confidence and trust. pp. 283–297 (05 2006). https://doi.org/10.1007/11755593_21
32. Puiggalí, J., Morales Rocha, V.: Remote voting schemes: A comparative analysis. vol. 4896, pp. 16–28 (10 2007). https://doi.org/10.1007/978-3-540-77493-8_2
33. Republic of Ghana: Public Elections Regulations, C.I. 91 (2016)

34. Schneider, R., Senters, K.: Winners and losers of the ballot: Electronic vs. traditional paper voting systems in brazil. Latin American Politics and Society **60**, 41–60 (05 2018). https://doi.org/10.1017/lap.2018.5
35. The Knesset of Israel: Basic Law: The Knesset (5718-1958)
36. The Knesset of Israel: Knesset Elections Law (Consolidated Version), No. 40 (5729-1969)
37. United Nations General Assembly: Universal Declaration of Human Rights, Resolution 217 (1948)
38. United Nations General Assembly: International Covenant on Civil and Political Rights, Resolution 2200A (XXI) (1966)
39. West Germany Parliamentary Council: Basic Law of the Federal Republic of Germany (in German), BGBl. S. 1, 2048 (1949)
40. Willemson, J.: Bits or paper: Which should get to carry your vote? Journal of Information Security and Applications **38**, 124–131 (2018). https://doi.org/https://doi.org/10.1016/j.jisa.2017.11.007, https://www.sciencedirect.com/science/article/pii/S2214212617304933