Verification Systems for Electronic Voting: A Survey

Jordi Pujol-Ahulló, Roger Jardí-Cedó, and Jordi Castellà-Roca

Departament d'Enginyeria Informàtica i Matemàtiques
UNESCO Chair in Data Privacy
Universitat Rovira i Virgili
Av. Països Catalans 26
E-43007 Tarragona, Spain
{firstname.lastname}@urv.cat

Abstract: Voting is an important part of the democratic process. The electorate makes a decision or expresses an opinion that is accepted for everyone. Some parts could be interested in the election results deviation without anyone else noticing it. However, ensuring that the whole voting process is performed correctly and according to current rules and law is, then, even more important. We present in this work a review of existing verification systems for electronic voting systems, from both academia and the commercial world. To do so, we realize a fair comparison against a set of representative voting verification systems, by using an evaluation framework. We define this framework to be composed of several properties and covering important system areas, ranging from the user interaction to security issues. We then model the natural evolution of verifiability issues on electronic voting systems, which are influenced by restrictions on current laws and by technological advances.

1 Introduction

From the birth of democracy in Athens in sixth century BC and the first form of electoral laws, electoral systems have been designed and developed according to country particularities in democratic governments worldwide.

An election process consists of choosing a person or party, namely *candidate*, to represent all members of the community (e.g., a company, a state, or a country). For a candidate, winning an election represents a big responsibility, but it is also very attractive in many ways for other reasons (e.g., funds, ability to change existing rules and laws). Therefore, synergies could appear to deviate from election results to have a certain candidate (not) win.

However, it is a difficult task to check whether the election results correspond to the voters' preferences, since *votes are commonly private and anonymous*. That is, if voter Alice votes for candidate A, any another person must not know or extract Alice's preferences from the election process and results.

In other words, *elections must be verifiable*, even though voters' preferences are linked in no way to them. Therefore, *verifiability* comes to light as the most important election property to provide *trustfulness* to the election results to both candidates and voters.

Verifying that election results correspond to voters' preferences depends on the voting system. From a location viewpoint, most of the existing systems are based on *poll sites*, where voters go to specific places to vote. Remote voting systems (such as mail voting or lastly internet voting systems) are also an alternative.

From a ballot perspective, traditional voting systems use ballots in paper format. They were firstly introduced in the state of Victoria, Australia, in 1856 [Be10]. Paper ballots contain all the necessary information to vote for a specific candidate, in a human-readable format. Thus in the vote counting or *tally*, any person can verify whether the ballot is correct and, if so, to which candidate it is related to. However, the main drawbacks of traditional voting systems are that all operations are manual, as well as their high economic and logistic costs. In addition, the tally process where votes are counted can turn into a long procedure susceptible to human errors, especially when the voting system is complex.

More modern voting solutions incorporate electronic devices to mainly accelerate the tally process and overcome the problems induced by human errors, and also increment accessibility for disabled and illiterate voters. First initiatives appeared in 1964 in some states of the USA, which used punchcards and computer tally machines [Be10]. These kinds of solutions can use different technologies, ranging from punchcards, optical scanners (to scan ballots), to cryptographic techniques. Electronic voting (e-voting) systems thus pose other kinds of challenges to election *verifiability*, whilst at the same time ensuring voter privacy and anonymity.

To put all of this in words, we can differentiate three different types of *verifications*: *individual*, *universal* and *end-to-end*. Briefly speaking, *individual verification* permits voters to check that their individual ballots are correctly cast and counted.

From a system viewpoint, *universal verification* allows poll workers to inspect that the election results correspond to the cast ballots. The aim is to ensure that the whole voting process is performed correctly, what leads to *trustful* election results. In traditional voting systems, both verifications are achieved by a set of *procedures* (i.e., manual operations addressed by election officials, or also by independent entities and observers from candidates). Contrariwise, a mix of *procedures and technologies* usually addresses them in e-voting systems.

A later enhanced property is the *end-to-end* (E2E) *verifiability*. Seen from a voter's point of view, in an E2E verifiable voting system, a voter can check during the voting process that both her ballot is correctly cast and counted in the final tally. The goal is then to

increase the voters' *reliability* in the election results. Note that this property was hardly supportable in traditional voting systems, since the voter Alice concluded her interaction with the voting system when casting the ballot into the ballot box. However, new designs of voting systems and modern technologies facilitate an E2E voter-verifiable voting process.

In this survey, *we present a fair comparison on the verifiability of electronic voting systems based on poll sites*. We also name them *voting verification systems* (VVSs). The motivation is that poll-site-based voting systems are the most common ones nowadays. Besides, we specialize our study on e-voting systems since they are the most recent trend in democratic voting systems [Ev09]. The systems included in this analysis are remarkable commercial and academic solutions of the last decade. Thus the contribution of this work is twofold: (i) definition of a *common evaluation framework* to fairly compare all systems and (ii) *study and comparison* of remarkable e-voting systems.

Document structure The next section introduces the necessary background for the present work. Sec. 3 presents the evaluation framework and Sec. 4 the analysis of all voting verification systems (VVS). In Sec. 5, we perform the analysis of all the systems and pinpoint the technological trends. Finally, Sec. 6 presents the concluding remarks of this work and some future work.

2 Background

We consider in this study the standard voting process composed of the following phases: (i) *voter registration* and identification, (ii) *vote casting* using ballots and (iii) *vote tally*, where all ballots are securely *tabulated* and unbiased results are made *public*. The voting process also includes all *procedures* and *technologies* to trustfully address the consultations or elections. In addition, we present the system classification of the voting models and voting verification systems, according to the voting location and the U.S. HAVA classification, which will be used later in this work to organize the analyzed voting systems.

2.1 Voting models

We present two classifications of the voting models, according to the place where voters have to attend to vote (see Sec. 2.1.1), as well as according to the U.S. HAVA classification (see Sec. 2.1.2).

2.1.1 Location-based classification

According to the place voters have to go to vote, voting systems are broadly classified into **poll-site-based** and **remote** voting systems. The former type is the most used nowadays, and it is characterized by having voters go to specific buildings, namely poll sites, to cast their votes. Conversely, voters may remotely cast their vote in *remote voting systems*. The most important examples are **vote-by-mail** and **internet voting.**

Recently, a new kind of systems has been proposed: **presential remote**. Such systems allow the casting of votes in a controlled environment (i.e., poll sites) although the tally is electronically conducted at a centralized site, dedicated to securely count all votes. Therefore, this kind of systems benefits from both existing modes, poll-site-based and remote, since they are very helpful when voters are abroad (e.g., the military), whilst at the same time reducing the tally time.

As mentioned earlier, our *focus* is put *on verification systems of poll-site-based systems*, which also allow us to take presential remote voting systems into consideration.

2.1.2 HAVA classification

This classification has been promulgated by the Election Assistance Commission (EAC), an independent agency of the United States government created by the Help America Vote Act of 2002 (HAVA). Appendix C of the 2005 VVSG [El05] separates the VVSs into four types: (i) **process separation-based** VVSs have a modular architecture split into two independent, totally isolated systems dealing with the *generation* and *casting processes, respectively*; (ii) **evidence-based** VVSs are based on capturing *all actions* performed during the voting phase of voters; (iii) **direct** VVSs generate a *parallel* registry of votes, which permits a direct verification of the vote to be cast; lastly, (iv) **end-to-end cryptography-based** VVSs employ cryptographic methods to craft receipts which allow voters to verify that their votes were not modified, without revealing the voting preferences of the voters. We will classify the evaluated electronic VVSs using this classification system.

3 Common Evaluation Framework

In this section, we introduce the classification and properties that we will extract from the set of systems under consideration. All of them constitute the single, structured *evaluation framework* that we will use to ease their fair comparison and analysis.

3.1 Classification of VVSs

We employ the following classification to *percolate* the systems through, respectively, in order to obtain their natural organization. The publication year of the academic publication or system is the last organizational property used.

1. From **electronic-** and **paper-based systems**, we only consider electronic VVSs, which require voting in an *electronic* (instead of a *paper)* format.

2. We use the aforementioned **HAVA classification** to separate them into *process separation-*, *evidence-*, *end-to-end (E2E) cryptography-based* and *direct* VVSs.

3. We further organize them into **integral** or **independent systems**. *Integral* ones perform the whole voting process, while *independent* VVSs are designed solely to verify independently that another voting system's operations can be trusted.

3.2 Evaluated properties from VVSs

We present in this section the characteristics considered against which all systems are to be evaluated. We have classified them into these voting process concerns: *user interaction*, *security*, *integrability* (with an existing voting system), as well as *technical issues*. Note that any property definition is such that a *positive answer* corresponds to a *positive feature*.

User interaction The *user interaction* greatly determines the voters' impression and *reliability* of the voting system:

1. **Accessibility** Whether the system *does not* prevent a disabled user to vote.

2. **Use impact** Whether the system *does not* create a more complex (even longer) process to cast a vote.

3. **Reliability** Trust in the whole voting process from a *voter's viewpoint*.

Security The security issues are broadly categorized into these two big sets, namely *voter* and *voting process*:

Voter-related:

4. **Ballot secrecy** The system *prevents* a third entity from seeing the contents of the ballot.

5. **Voter anonymity** The system *prevents* the ballot from being linked to the voter.

6. **Coercion resistant** A coercer *cannot* verify nor demonstrate how the voter voted.

7. **Individual verification.** A voter *can* verify that her vote was accounted for *properly*.

Voting-related:

- **Universal verification:**

8. **Ballot box integrity** Only registered voters' votes *appear* at the end of the voting process (before the tally process) and are unmodified.

9. **Tally accuracy** The tally process *counts* all of the cast votes and not before the end of the voting process (i.e., no partial results are allowed).

10. **Auditability** The e-voting system (with no paper trails) *allows* a third party to analyze what happened before, during, and after the vote was cast, without compromising other security properties, in order to certify the final tally and election results.

Integration Regardless of whether the VVSs are *integral* or *independent*, we will consider the feasibility and effectiveness of adapting/integrating the evaluated system with other voting systems. In particular, briefly speaking, we consider the synchronization of operations, especially when votes are being cast, between a given voting system and the evaluated system *acting as an independent VVS* (as issued in [Sh06]).

11. **Integration** *Ease* of implementing/adapting the evaluated system as an independent verifier system for other voting infrastructures.

12. **Data management** Whether the vote cast subsystem of the voting systems and the evaluated system *guarantee* atomicity, as well as whether this integration is resistant to failures (e.g., user errors, cable disconnections).

Technical issues We also analyze the VVS performance from a *technical viewpoint*:

13. **Simplicity** Whether the verification solution *is* straightforward and simple.

14. **Availability** A suitable voter *must be able to* cast her vote, within the established time period, and be prevented from voting multiple times (if not otherwise allowed).

15. **Scalability** The verifier system computationally *scales*.

16. **Flexibility** This measures the level of freeness *allowed* by the verifier system (e.g., number of candidates, write-in mode).

Properties representation For brevity, when summarizing these sixteen properties for all the evaluated systems, we will use the following notation:

User interaction	↑/↓/~: Good/Weak/Acceptable.
Security	**Y**/**N**/~: **Y**es/**N**o/Partially.
Integration	**NT**: **N**o additional **T**echnical requirements (on voting consoles, etc). **T**: Additional **T**echnical requirements. **NSW**: **N**o additional **S**oft**W**are requirements (on voting consoles, etc). **SW**: Additional **S**oft**W**are requirements.
Data management	**NA**: There is **N**o operation **A**tomicity. **A**: There is operation **A**tomicity. **DL:** There is **D**ata **L**oss. **NDL:** There is **N**o **D**ata **L**oss.
Technical Issues	↑/↓: High/Low
At any property	"N/A": When the property is *not addressed*.

Table 1: Value representation of the considered evaluation properties

4 Presentation and classification of VVSs

We present here all the evaluated *electronic VVSs*. The idea behind them is that they depend primarily on e-voting procedures, even though some of them may have paper *receipts* to provide E2E verifiability. From the HAVA classification, we present solutions on three out of the four types: *process separation-*, *evidence-,* and *end-to-end cryptography-based* (E2E).

4.1 Process separation-based VVSs

As we have presented before, a process-separated VVS is divided into two independent and isolated subsystems: *ballot generation* and *casting*. In this class of systems, the security constraints are mainly applied to the casting process. We present below the most representative one: Modular Voting Architecture, namely "Frog" [BJR01].

4.1.1 Modular voting architecture ("Frog")

S. Bruck, D. Jefferson, and R. Rivest presented this system in 2001 [BJR01]. It is the example *par excellence* of separation process and, therefore, it implements an integral e-voting solution that emphasizes and standardizes a separation between vote *generation* and vote *casting* components.

On the day of the election, the voter identifies himself to a poll worker, who takes a blank *ballot* (ballots are named *frogs*), initializes it and, then, returns the ballot to the voter. Afterwards, the voter inserts his ballot into the *vote generation equipment*; she selects her options through a direct-recording electronic (DRE) voting machine, and her

choices are introduced onto her ballot. The second phase starts here. The voter introduces her ballot into the *vote-casting equipment* and *checks* the content of her ballot. When the voter agrees with the content, her ballot is digitally *signed* (using a single key for all votes), then *frozen* (the frog is blocked against writing), and finally *deposited* into the *frog bin*. At this moment, an electronic copy of her vote is randomly stored in a data unit memory and replicated in other memories for reliability. Once the elections are over, election officials publish the results for each precinct in a Web as two separated, unlinked lists: one with the voters' names and the second one with all cast ballots with a system-wide digital signature. Therefore, anyone can verify the digital signature and compute the election results.

4.2 Evidence-based VVSs

These systems capture the actions performed by voters when casting their votes, independently of the voting system and invisible by the voter. In addition, to ensure information integrity, all recorded events are stored outside of the vote terminal. Under this type of VVSs, we consider VVAATT and VVVAT.

4.2.1 Voter verified audio audit transcript trail (VVAATT)

VVAATT is an *audio verification* system, introduced by T.Selker and S.Cohen in 2004 [Se04, SC05]. This system records the *audio* of all events during the voting process into a physical medium (in a cassette tape or in a CD-W media), at the same time this is complemented by the *visual* verification from the DRE. In the same line, there exists Voter Verified Video Audit Trail (VVVAT), which instead, captures the sequence of screenshots on the DRE terminal (see [Cr07] for an example).

4.3 End-to-end verifiable VVSs

We present in this section the E2E cryptographic-based VVSs, which among other capital properties have an end-to-end (E2E) verifiability. To do so, some of them generate *paper receipts* to allow voters to check that their votes were counted in the tally process. The following solutions are the selected systems under analysis: VoteHere [Ne01], VoteBox [SDW08], Three-Ballot-Based Secure Electronic Voting System [SCM08], and the last ErgoGroup/Scytl proposal [No09b].

4.3.1 VoteHere

VoteHere is an integral solution introduced by C. Andrew Neff and VoteHere, Inc. in 2001 [Ne01, Va01]. This system is based on the use of DRE terminals. It is built considering receipt- and cryptography-based verifications in order to cover both *individual* and *universal* verifications.

For each voter, the voting system builds a *code* for each electable candidate before the election starts. Once the voter has chosen her preferences on the DRE, the DRE shows

the codes related to each candidate. If they correspond with those pre-built codes, the voter confirms her vote and a *receipt* is printed with her *verification codes*. Once the election ends, the *encrypted votes* are made publicly available (guaranteeing ballot secrecy), and then the voter can *check* if her vote was counted (or complain to election officials otherwise).

4.3.2 VoteBox

VoteBox is an integral solution and was developed by D. Sandler, K. Derr, and D. Wallach in 2008 [SDW08]. The VoteBox system uses a technique adapted from Benaloh's work on voter-initiated auditing [Be07] to gain *end-to-end verifiability*. In other words, the voting system actually is an audit system that records everything that happened. Its main properties are as follows:

- **Pre-rendered user interface** The user interface is built from *pre-rendered* graphics, a closed sequence of pages (screens) containing text, and graphics that reduce runtime code size. The only interactive elements are buttons, rectangular regions of the screen (VoteBox supports touch screens), and other assistive technologies (computer mice, keyboards or audio feedback to state transitions).

- **Tamper-evidence and replication** A *permanent*, *tamper-evident* audit system records the events along the voting process and provides resistance to data loss in case of failure or tampering. VoteBox consists of two parts: the supervisor console and VoteBox booths (i.e., voting terminals). A broadcast network connects both parts, so that events from both parts (including ballot casts or supervisor commands) are replicated on all voting terminals and entangled with a hash chaining to provide *immutable* logs.

- **End-to-end verifiability** To encrypt ballots, VoteBox uses the ElGamal cryptosystem and its *additive homomorphic* property. Any cast ballot is encoded in a binary format and encrypted by a public key for the election. Therefore, the tally is addressed by (i) the multiplication of all ballots and (ii) the multiplication result decryption in order to obtain the election results.

4.3.3 A three-ballot-based secure electronic voting system

This system [SCM08] is based on the original, paper-based Three-Ballot system [Ri06], but is completely redesigned to provide a full electronic solution. The idea behind the Three-Ballot approach is that a *ballot* consists of three single *parts*, with a list of candidates in the same order on the three parts. In order to vote for a candidate, the voters mark *any two parts* for the corresponding candidate (marking only one part means no vote is cast). When casting the vote, the three parts are separated from each other and mixed with the rest of parts from other voters. The tally operation is done by a simple calculation on the number of marks for each candidate on all the parts. One out of the three parts is randomly chosen by the voter to *copy* and to take home as a *receipt*. The same approach is maintained in this electronic version of Three-Ballot [SCM08].

4.3.4 E-valg 2011

The Norwegian Ministry of Local Government and Regional Development initiated in 2008 a selection process of e-voting technological providers, which finished on December 2009. ErgoGroup[1] and Scytl[2] [No09b] will provide the e-voting solution for the Norwegian municipal elections in 2011 [No09c].

The ErgoGroup/Scytl's solutions provide all the security requirements by using cryptographic techniques. Until now, the ErgoGroup/Scytl consortium has designed various systems to support two types of voting: *poll-site-based* (compatible with DREs) [Sc04] and *remote voting* [PM07]. Moreover, the latter allows a presential remote voting model, which suits the system requirements specification of the E-valg 2011 project [No09d].

ErgoGroup/Scytl's proposal [No09b] is based on a *hybrid scheme* that combines mixing techniques and ElGamal homomorphic properties [Pe09]. The homomorphic cryptography uses a *multiplicative* property [Pe04, Pe09] so that the system performs partial multiplications of the votes. The election private key, used to open the encrypted votes, is generated using a *threshold scheme* [Sh79]. Lastly to retain all desirable security properties, this system uses digital signatures, zero knowledge proofs, and the generation of return codes (i.e., *receipts*).

5 Study and comparison of VVSs

In this section we introduce the analysis of the considered VVSs (Sec. 5.1) and the study of the synergies on voting systems and cryptographic technologies (Sec. 5.2).

5.1 Analysis and comparison of VVSs

We follow the properties considered in our common evaluation framework to compare and analyze all evaluated VVSs. See Tab. 3 for the complete elaboration.

User interaction Given that all VVSs use DREs to emit votes, all of them provide a certain degree of **accessibility**. However, some of them improve it by using audio guides (VVAATT), or indeed with other assistive technologies (such as mice or keyboards) (VoteBox and E-valg). For the E-valg case, this is proved by the studies [Sh06], [No09a]. As for the **use impact**, systems like Frog, VoteBox and Three-Ballot present a more complex and likely longer voting process. For instance, in Frog there exists a strict separation of the generation and cast processes (even though a voter can bring a filled ballot from home); VoteBox allows voters to perform an "immediate ballot challenge" [Be07]; and Three-Ballot uses a multi-ballot composed of 3 parts. Further, in order to increase the **reliability** of the voting system, they provide three kinds of augmented features: (i) frogs (Frog) and *receipts* (VoteHere, VoteBox, Three-Ballot and E-valg)

[1] http://www.ergogroup.no/default.aspx?path={2A1C0F50-F200-43C8-98C6-36CD82F7A587}
[2] http://www.scytl.es

tangible elements for the voter, (ii) audio guides (VVAATT), and (iii) public web bulletins (all except VVAATT).

Security VVAATT/VVVAT do not ensure vote confidentiality, given that all (audio or video) recordings show the *sequential* voting order. In addition, VVAATT/VVVAT suffer from *weak* recording equipment protection (given that they must be accessed often) and *untrustworthy* information extraction techniques. In conclusion, even though the recording support provides audit means, VVAATT/VVVAT are not reliable. Next, we only will focus on the rest of the systems.

Voter-related security Except for Frog, all of the systems use a public key infrastructure (PKI), most of them ElGamal, to ensure **ballot secrecy**. However, these VVSs use very different techniques to guarantee **voter anonymity**. While Frog uses a simple randomization algorithm, Three-Ballot separates each of the three parts of a ballot and stores them using their hash values. More complex techniques also appear: mixing (VoteHere), additive homomorphism (VoteBox) or a hybrid scheme (multiplicative homomorphism and mixing in E-valg). VoteBox, Three-Ballot and E-valg are **resistant to coercion and vote selling**. The same is not true for VoteHere, since it may have a flaw given that it shows both encrypted ballots and receipts with return codes [Ba04]. Lastly, except for Frog, all systems render *augmented* **individual verification** with *E2E* voter *verifiability* through receipts.

		Security Techniques			
		ZKPs	Digital Signatures	Threshold Scheme	Audit System
VVS	Frog	No	Yes	No	No
	VoteHere	Yes	Yes	Yes	No
	VoteBox	Yes	Yes	Yes	Yes
	Three-Ballot	No	Yes	No	No
	E-valg	Yes	Yes	Yes	Yes

Table 2: Security techniques used by voting verification systems

Voting-related security Except for Frog, all of the systems ensure **ballot box integrity** through different technologies (like ZKPs, digital signatures or threshold schemes). The use of a threshold scheme prevents security attacks against the electoral system. See Tab. 2 for more details. Thus, VoteHere, VoteBox, Three-Ballot and E-valg guarantee **tally accuracy**. Homomorphic algorithms make a more efficient tally than mixing techniques [Pe04, Pe09]. As for **auditability**, Three-Ballot creates logs for any voter-related operation, even though it creates none about the tally process. The evaluated strongest audit systems appear in VoteBox and E-valg, which use *immutable* logs. VoteBox, however, builds a distributed total audit system, while E-valg only centrally audits the critical system elements.

Integration In order to be **integrated**, the evaluated VVSs have some software or technological dependences (see Tab. 3 for more details). However, only VoteBox and E-valg [Sh06] ensure vote atomicity, loss resistant, and tamper evident solutions.

Technical issues VoteBox and Frog are more **complex** than the rest of the systems, given that the former has a distributed infrastructure, and the latter is strictly tied to the separation of processes. However, VoteBox is the only system that structurally provides distributed *replication* of sensible information, which leads to a high degree of system **availability**. Another of VoteBox's good properties is its **scalability**, given that it uses homomorphic cryptography, and thus makes the tally process easier. This property is also shared by E-valg. However, both of them should carefully address presential remote voting, guaranteeing the necessary infrastructure in order not to overload the voting system. Finally, only Frog, VoteHere and E-valg render **flexible** on vote type and format. Notice that VoteBox, by using additive homomorphic cryptography, only supports simple types of votes. Lastly, Three-Ballot is only suitable for multi-ballot formats composed of 3 single parts, even though that the ballot content is flexible.

5.2 Study of trends in VVSs

From the above analysis we can extract *three clear trends* in regard to the following issues: (i) voting location, (ii) voting technology, and (iii) degree of verifiability.

Voting location study We have evaluated *poll-site-based* VVSs. All of them use DREs as voting terminals. Clearly, DREs are very helpful in order to manage votes electronically. It is worth noting the demonstrated trend away from *poll-site-based* toward presential remote voting systems. For instance, VVAATT/VVVAT, Frog, VoteHere and Three-Ballot are of the first type, and VoteBox and E-valg are presential remote voting systems. This trend is a consequence of not only the technology, but also the natural evolution in the democratic rules. However while VoteBox was *adapted* to support presential remote voting schemes, E-valg was *structurally* designed to do so.

Voting technology study We consider here the voting technology used from the ballot cast to the tally and, therefore, VVAATT/VVVAT-based systems are not considered. The idea behind this technology is to address security issues such as voter anonymity, ballot box integrity, and tally accuracy among others. These systems present a clear evolution in this issue. We detail them from simpler to more complex and reliable solutions.

While Frog uses only a simple *randomization* algorithm to anonymize votes, VoteHere uses a more reliable mixing technique to address *voter anonymity*. VoteBox and Three-Ballot use (computationally hard) *additive homomorphic* cryptography to guarantee *voter anonymity* and to perform the *tally*. The most complex, but flexible and reliable technology is used by E-valg, the *hybrid scheme*, which is composed of multiplicative homomorphic cryptography (computationally less hard than additive ones [Pe04, Pe09]) and mixing mechanisms. Clearly, the technology used presents a *trade-off* between ensuring (i) more secure, trustful, and reliable voting technologies, and at the same time guaranteeing (ii) fast and resource-efficient ones. This trend from simple randomization techniques to hybrid schemes is a direct consequence of the continuous permeability of voting systems with regard to the latest cryptographic advances.

Verifiability study We can organize the analyzed systems as follows: (i) VVAATT/VVVAT-based and Frog systems provide deficient or basic verifiability in voting processes, respectively. They mainly guarantee at some degree the individual verifiability, yet the same is not true for universal or E2E verifiability. (ii) VoteHere and Three-Ballot VVSs offer an acceptable degree of verifiability (individual, universal, and E2E). Finally, (iii) E-valg and VoteBox ensure a good level of verifiability, while at the same time they define a tough audit system. To sum up from all of these remarkable VVSs, VoteBox and E-valg are the best alternatives for voting systems. However, E-valg is a better voting system candidate, which should be followed closely. This is because it provides commercial applications, a high degree of verifiability, and a smooth transition from traditional voting systems to electronic ones, not to mention its accessibility and ease-of-use.

VVS	USER INTER.			SECURITY							INTEGR.		TECHNICAL ISSUES			
				VOTER-RELATED				VOTING-RELATED								
								UNIVERSAL VERIFICATION								
	Accessibility	Use Impact	Reliability	Ballot Secrecy	Voter Anonymity	Coercion Resistant	Individual Verification	Ballot Box Integrity	Tally Accuracy	Audtability	Integration	Data Management	Simplicity	Availability	Scalability	Flexibility
Frog	↓	~	↑	N	Y	N	~	~	N	N	SW/T	N/A	↓	N/A	↓	↑
VVAATT	~	↑	↑	N	N	N	N	N	N	~	T	DL/NA	↑	N/A	↓	↓
Vote Here	↓	↑	↑	Y	Y	N	Y	Y	Y	N	SW	N/A	↑	N/A	~	↑
Vote Box	↑	↓	↑	Y	Y	Y	Y	Y	Y	Y	SW/T	NDL/A	↓	↑	↑	↓
Three-Ballot	N/A	↓	↑	Y	Y	Y	Y	Y	Y	Y	N/A	N/A	↑	N/A	~	↓
E-valg	↑	↑	↑	Y	Y	Y	Y	Y	Y	Y	N/A	NDL/A	↑	N/A	↑	↑

Table 3: Detailed properties of the Voting Verification Systems.

6 Conclusions

In this paper, we have presented an evaluation framework, common for all systems, in order to conduct a fair study of the different electronic voting verification systems (VVSs). The strong point of the present study is threefold: (i) we define the common evaluation framework, (ii) we present academic and commercial VVSs, and (iii) we conduct a fair study and comparison among them, having the verifiability analysis as a connecting thread.

Even though the origin of e-voting systems was to accelerate the tally process, the trend is clear and firm towards not only electronic tally, but also electronic vote casting

[Ba06]. Since the introduction of the DREs, more and more initiatives are addressing electronic casting in elections. This trend is also visible in our study.

As we have seen, good designs of e-voting systems may be significantly helpful for disabled and also for illiterate citizens. At the same time, the use of electronic voting technologies may reduce the economic and logistic costs of elections and consultations, while facilitating geographically distributed citizens to vote. Even though there are no conclusive studies, the tally accuracy on e-voting systems is higher than in paper-based voting systems [Ba06]. However, e-voting systems should not be massively introduced – education and increasing the sensibility toward democracy is necessary beforehand– in a society where there exists a high ratio of abstention.

As demonstrated by the technologies used in the latest e-voting systems, we foresee that the future trend in the use of electronic voting will be *remote e-voting*. In this line, there were some first *remote presential* and *internet voting* experiences. The global acceptation of these remote e-voting schemes will empower citizens with new democratic participation tools, which will likely lead to direct and binding citizen consultations and elections.

Bibliography

[Ba04] Barnes, Richard. 2004. VoteHere VHTi. A verifiable e-voting protocol. Cryptography applications bistro. http://www.cs.virginia.edu/crab/VoteHere.pdf/. (accessed Feb. 2010).

[Ba06] Barrat Esteve, Jordi. 2006. A preliminary question. Is e-voting actually useful for our democratic institutions? What do we need it for? In *Proc. of 2nd international conference on electronic voting (E-VOTE '06)*, 51–60. GI, Bregenz, Austria.

[Be10] Bellis, Mary. 3rd November 2009. The history of voting machines. http://inventors.about.com/library/weekly/aa111300b.htm/. (accessed Feb. 2010).

[Be07] Benaloh, Josh. 2007. Ballot casting assurance via voter-initiated poll station auditing. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07)*, 14–14, Berkeley, CA, USA: USENIX Association.

[BJR01] Bruck, Shuki, David Jefferson, and Ronald Rivest. 2001. *A modular voting architecture ("Frogs")*. In Proceedings of the Workshop on Trustworthy Elections (WOTE '01), California, USA. URL: http://vote.caltech.edu/backup/wote01/pdfs/amva.pdf

[Cr07] Cross, E.V., G. Rogers, J. McClendon, W. Mitchell, K. Rouse,P. Gupta, P. Williams, I. Mkpong-Ruffin, Y. McMillian, E. Neely, J. Lane, H. Blunt, and J.E. Gilbert. 2007. Prime III: One machine, one vote for everyone. In *(On-line) proceedings of 2007 voting competition conference*. http://vocomp.org/papers/primeIII.pdf/. (accessed Feb. 2010)

[El05] Election Assistance Commission (USA). 2005. Voluntary voting system guidelines. http://www.eac.gov/voting%20systems/docs/vvsgvolumei.pdf/attachment_download/file/.

[Ev09] E-voting.cc (competence center for electronic voting and participation). 2009. Map of electronic democracy. *Modern Democracy* 2(1):8–9.

[Ne01] Neff, C. Andrew. 2001. A verifiable secret shuffle and its application to e-voting. In *CCS '01. Proceedings of the 8th ACM conference on computer and communications security*, 116–125. New York, NY, USA: ACM.

[No09a] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Accessibility and usability evaluation of e-vote prototypes. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/report_evoting_usability_accessibility_eval_nr_iter2_final.pdf/. (accessed Feb. 2010).

[No09b] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Contractor solution specification. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/e_valg_systemlosning/Tilbud_ergogroup/SSA-U_Appendix_2A_Contractor_Solution_Specification.pdf/. (accessed Feb. 2010).

[No09c] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. Project directive for e-valg 2011. http://www.regjeringen.no/upload/KRD/Vedlegg/KOMM/Evalg/Project_directive_evalg2011_v101_english.pdf/. (accessed Feb. 2010).

[No09d] Norwegian Ministry of Local Government and Regional Development. 2009. E-vote 2011. System requirements specification. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/e-valg/Anskaffelse/System_Requirements_Specification1.pdf/. (accessed Feb. 2010).

[Pe04] Peng, Kun, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee. 2004. Multiplicative homomorphic e-voting. In *Proceedings of 5th international conference on cryptology in India (INDOCRYPT '04)*, 61–72. Kolkata, India. Springer.

[Pe09] Peng, Kun. 2009. A hybrid e-voting scheme. In *Proceedings of the 5th international conference on information security practice and experience (ISPEC '09)*, 195–206, Berlin, Heidelberg: Springer-Verlag.

[PM07] Puiggali, Jordi, and Vitor Morales-Rocha. 2007. Independent voter verifiability for remote electronic voting. In *Proceedings of international conference on security and cryptorgraphy (SECRYPT '07)*, 333–336. Barcelona, Spain. Springer.

[Ri06] Rivest, Ronald L. 2006. The three-ballot voting system. Unpublished draft.

[Sc04] Scytl Online World Security S. A. 2004. Auditability and voter verifiability for electronic voting terminals. http://www.scytl.com/_a_home/PNYX.VM_White_Paper.pdf. (accessed Feb. 2010).

[SC05] Selker, Ted, and Sharon Cohen. 2005. An active approach to voting verification. http://vote.caltech.edu/drupal/files/working_paper/vtp_wp28.pdf/. (accessed Feb. 2010).

[SCM08] Santin, Altair O., Regivaldo G. Costa, and Carlos A. Maziero. 2008. A three-ballot-based secure electronic voting system. *IEEE Security and Privacy* 6(3):14–21.

[SDW08] Sandler, Daniel, Kyle Derr, and Dan S. Wallach. 2008. Votebox. A tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th conference on security symposium (SS'08)*, 349–364. Berkeley, CA, USA: USENIX Association.

[Se04] Selker, Ted. 2004. The voter verified audio audit transcript trail. http://www.dos.state.pa.us/election_reform/lib/election_reform/VVAATT_CalTech.pdf/. (accessed Feb. 2010).

[Sh79] Shamir, Adi. 1979. How to share a secret. *Commun. ACM* 22(11):612–613.

[Sh06] Sherman, Alan T., Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, Donald F. Norris, John Pinkston, Andrew Sears, and Dongsong Zhang. 2006. An examination of vote verification technologies: findings and experiences from the Maryland study. In *Proceedings of the USENIX/accurate electronic voting technology workshop 2006 on electronic voting technology workshop (EVT'06)*, 10–10. Berkeley, CA, USA: USENIX Association.

[Va01] Varner, Philip E. 2001. Vote early, vote often, and vote here. A security analysis of VoteHere. PhD diss., University of Virginia.