

ELECTRONIC VOTING: DEVELOPMENTS, TRENDS, CHALLENGES

Sokratis K. Katsikas ska@aegean.gr
*Dept. of Information and Communication Systems Engineering, Univ. of the
Aegean, Greece.*

Abstract: This paper hopefully contributes to the discussion on what kind of electronic voting systems utilizing Internet technology we should be aiming at and what characteristics these systems should have. It provides an overview of the major constitutional and legal aspects of e-voting, together with their technical implications. It also discusses the security requirements and the system-wide properties that the voting protocol of an electronic voting system is expected to fulfill. An overview of families of existing voting protocols, together with a brief analysis of their characteristics, is provided. The aim is to investigate and discuss the extent to which current voting protocols comply with the identified requirements.

1. INTRODUCTION

The word “democracy”, transference of the Greek word “δημοκρατία (dimokratia)” into the English language, literally means “ruling of the people”. Going back to the ancient Athenian democracy, all citizens of Athens were expected to take active part in the administration of the state; in fact, refusal to being involved was punishable by law. This global participation in politics is of course possible when the numbers of the people involved are low, as was the case with ancient Athens, where very few of the inhabitants actually had citizen status. With the advent of time and the increase in the numbers of citizens, the direct democracy model of ancient Athens evolved into the modern representative democracy model, in which participation in public affairs is achieved through representatives of the citizens. It comes then as no surprise that one of the cornerstones of modern democracy is the process of nominating representatives. Despite the fact that

decision making is nowadays the responsibility of representatives, direct access to the opinion of the people themselves is sometimes required. Therefore, elections, referenda and polls are critical processes and tools for the operation of a modern democracy, as they do not only provide the means for the transfer of power from the citizens to their representatives, but they also support the trust and confidence of citizens in government and in democracy, provided that they are functioning as required and designed.

Several election systems and models have appeared in the course of history, but the most dominant one is certainly the election system that is based on voting. The voting process has been supported by whatever technology was available at times, ranging from clay plaques on which the name of one's favorite candidate would be etched in ancient Athens, to the elaborate electronic voting systems of today. These systems are, in several countries, under intense scrutiny by policy makers, social scientists, computer and network engineers, and citizen groups. The main issues are whether more reliable, user-friendly and less costly voting systems should be developed, what are the essential legal and constitutional requirements that should be met and under what conditions (or whether) these systems would increase citizen participation to the elections. These issues are not yet resolved; instead, a long and interesting debate is still ongoing. Whether they will eventually be resolved remains to be seen. What is certain is that they will not be resolved in the same manner in all societies, as political culture and behavior differs significantly among different societies. However, commonalities do exist and should be appropriately utilized so that the discussion is facilitated.

Remote Internet voting provides the voters with convenience and ease-of-access, by enabling them to cast ballots from any Internet accessible location. This kind of voting offers significant benefits but it also poses substantial security risks and other social concerns. Without official control of the voting platform and of the physical environment, there are several known ways for one to intervene and alter the election results. It is arguable whether all risks and vulnerabilities can be faced with using existing or emerging security technologies. These technologies seem, for the time being, inadequate to address the inherent risks [1]. Additionally, any attempt to introduce e-voting, i.e. a voting process, which enables voters to cast a secure and secret ballot over the Internet or an Intranet, will have to address a series of complex constitutional and legal issues.

Adopting the view that technology will eventually find its way into this (i.e. voting) aspect of everyday life, as it has with almost every other aspect, and realizing that within its limited space it would not be possible to address

all issues related to e-voting, this paper focuses in security and privacy requirements of e-voting systems stemming from constitutional and legal requirements that translate into technical implications, with a view towards influencing the design of e-voting systems adhering to the fundamental principles of democracy. Moreover, it discusses such requirements expected by the heart of the voting system: the voting protocol. Recognizing the fact that the requirements for systems aiming at supporting formal elections are stricter than those for polling systems or opinion expression systems, the emphasis of the discussion is on the former kind. The discussion herein is based on and follows closely those in [2] and [3].

2. E-VOTING: CONSTITUTIONAL AND POLITICAL ISSUES

Over the last years there has been strong interest in online voting as a way to make voting more convenient and attractive, with the intention of coping with the problem of increasing abstention rates and raising low voter turnout, especially among younger people, foreign residents, and business and holiday travelers, handicapped and elderly. This interest reflects the tendency towards the establishment of a modern formation of public and private life, where people substitute physical participation with using communication means. However, democracy is not simply a matter of convenience: As e-voting is not merely a logical extension of everyday transactions and Internet applications in commerce and government, but a way to exercise a political right, deeply embedded in democratic traditions and constitutions, its introduction and acceptability depends upon its ability to respect, safeguard and promote the principles pertaining to this, most decisive, component of democracy.

The new culture introduced by information and communication technologies cannot and should not ignore the principles and values of democracy. Preconditions for this are transparency and confidence that democratic principles are respected. The introduction of an e-voting system conforms to this demand if it respects fundamental democratic principles and citizen rights, and fulfills the requirements arising from these principles and rights. It is commonly accepted that parliamentary elections have to be **free, equal and secret**. Furthermore, the principles of **universal and direct suffrage** belong to the European electoral heritage. The principles of **freedom and secrecy**, as well as the reference to **fair elections** are enshrined, explicitly or implicitly in a number of international instruments like the Additional Protocol to the European Convention on Human Rights or the International Covenant on

Civil and Political Rights. At the same time, the election procedure has to be **transparent** and **subject to public control** and scrutiny. Moreover, a democratic e-voting system should ensure **integrity, availability, reliability and accountability**.

Increasing turnout could stand as a democratic goal by itself, a goal that is being promoted through the introduction of e-voting procedures. However, any concerns or recommendations related to electronic voting must be considered in the context of an agenda for making democracy more accessible and meaningful. The introduction of such a system conforms to democratic requirements, only if it is designed to encourage citizen participation in a quantitative (more voters) and a qualitative (more informed voters) way [4,5]. This means that differential access to online technology would be a serious issue and a primary concern. From this perspective the **digital divide** and **access disparity** constitute a critical shortcoming for the feasibility and constitutionality of e-voting procedures. Overcoming the digital divide by general access of the electorate to Internet polling stations or at public access points (kiosks) could be proposed as a solution, although “walking to the e-center to cast an electronic ballot hardly seems like much of a technological leap”. Electronic voting will become democratically acceptable only when the majority of the eligible voters have easy access to the Internet. An adequate non-discriminating procedure should be offered to the voters, in order to enable them to efficiently exercise their voting rights without any obstructions. From this perspective, the notion of universal access is not only critically important for ensuring social acceptability of ICT technologies and of the emerging Information Society; it eventually becomes a constitutionally indispensable requirement.

The kind, as well as the accessibility of the voting procedure affects the principles of universal and equal suffrage, which are among the cornerstones of democratic elections. According to the constitutional requirement of universal suffrage, every eligible voter can participate in the election process and nobody can be - directly or indirectly - excluded or discriminated. The principle of equality further requires that all participants, be they candidates or voters, should have equal chances and (voting) rights. The principle of universal suffrage primarily requires that every voter has the right to participate in an election process, while voting possibilities and technologies should be accessible by every voter. In this perspective, the supplementary and alternative nature of e-voting, as well as the necessity for publicly available and appropriate infrastructure respond to a constitutional requirement, embedded in many constitutional texts.

The voting right extends further to a right to **exact composition of the electorate**. Secure registration and authentication of voters are the means of ensuring that the principles of universal and equal suffrage are respected and that elections cannot be rigged. Voter registration systems and accurate voter registration lists are important for the integrity and the legitimacy of the election process. Providing a secure identification and authentication scheme of eligible voters is a condition sine qua non for e-voting systems to be used in public elections.

The principle of equality results not only in the right to equal accessibility to the election technology. It is furthermore required that each vote will be weighted equally towards the election outcome. An e-voting system must therefore ensure that the “one voter, one vote principle” is respected. In other words, such a system should **prevent duplicability** of the vote (either by the voter, or by a third person) as well as **reusability** of the vote (either by voting more than once online, or by voting online and offline).

The role of political parties will inevitably be affected by the introduction of e-voting: the role and modus operandi of political parties will be changed dramatically insofar as new means result in immediate, but at the same time more complicated, political communication and possibly lead to a weakening of their influence potential. The integrity and legitimacy of the voting act and, more generally of the elections, depends on **safeguarding equal chances** for parties and candidates who participate in public elections. This principle bears a number of implications and consequences for the organization of e-voting procedures. Electoral equality requires that there are no deviations between the printed ballot and its electronic equivalent. A first requirement derived from the principle of equality is that electronic ballots should be edited and displayed in a way analogous to that used for the paper ballots. Changes to the electronic form of the ballot paper could be acceptable only if they are strictly necessary to facilitate the display of the electronic form. Furthermore, the placement of electronic ballots in the (public) voting site (i.e. on the screen of the e-voting site) should ensure equal accessibility. Thus, the structure and appearance of site and ballots should not favor or discriminate against any of the participating parties. Major consideration must be given to the (organizational rather than technical) requirement that all parties should have equal access to the components of the voting system and procedures to control and ensure that it is functioning in a transparent and equal way.

Freedom of voters includes two main aspects: the freedom of voters to **form** their opinion and the free **expression** of this opinion. The principle of free elections requires that the whole election process take place without any

violence, coercion, pressure, manipulative interference or other influences - that may be exercised by the state, an organization, or by one or more individuals. The voter must be able to vote personally and without any extraneous influence. The democratic legitimization of e-voting relies on satisfying the generic voting criteria of a democratic election system. This includes the free expression of the preferences of the voter, even through casting a non-valid or a "white" paper ballot. In order to preserve the freedom of voter decision, the possibility for casting a consciously invalid vote must be provided and guaranteed. **Coercion, vote buying and extortion are of great concern** in connection with other methods of remote or absentee voting. Providing an attestation declaration through a digital signature, instead of a handwritten declaration, as usually done with postal voting, could serve as an institutionally equivalent and feasible solution.

E-voting procedures may indeed pose new threats to the freedom and integrity of voter decision, beyond those that postal voting does. The vulnerability of free choice is strongly related to the question of secrecy in e-voting. Secrecy is the precondition of a free political decision, a defining principle of modern democracy. The requirement for secrecy mainly relates to two potential risks: a) the cast vote should not be an object of control of political opinions through public authorities, b) no person should know how a voter intends to vote or/and has voted. In order to face the first risk, the secrecy of the vote, physically protected by traditional voting procedures, has to be guaranteed during the casting, transfer, reception, collection and tabulation of votes. The secrecy of a vote constitutes a fundamental principle, which can be satisfied through the personal and anonymous nature of the voting act. As secrecy is intended to protect freedom of choice, no voter should be able to prove that he/she has voted in a particular way. **Confirmation** of the vote, after the ballot has been transferred and received, enforces the confidence in the system and ensures the rights of the voter, but it cannot relate to the content of the vote. Excluding the individual verifiability of the vote casting process may appear - in view of the potential of new technologies - as a restriction of voters' options, but in fact it constitutes a protection against duress and undue influence.

Secrecy is predicated on voting being a private act in which the individual, in isolation and free from the immediate influence of others, makes up his/her political choice. Coercion in workplaces or homes cannot be excluded. Since the employment relationship is not balanced, it is therefore suggested to avoid e-voting from the workplace. But also "home voting" and the preservation of secrecy and freedom seem to be contradictory in terms, taking in account not only the spatial and social dimension of home voting but also the digital divide between generations. Coercion and influence can

hardly be prevented by technology. Keeping e-voting as a supplementary option to traditional voting, as well as making available publicly accessible infrastructure, in sites monitored by public officials, allow voters to exercise their rights free of coercion of a third party. Moreover, measures should be taken at the policy and regulatory levels, in order to impose compelling and enforceable measures against coercion and to sanction illicit behavior.

Elections are political events and e-voting constitutes a new mode of participation in political processes. Evolutions and innovations of voting systems must be evaluated on the basis of democratic criteria including **transparency, controllability, accountability and legitimacy**. A key element of democratic, free and fair elections is the trust and legitimization that is gained by having a transparent vote casting and counting procedure. The traditional voting “technology” operates in a way that is transparent to the voters and to the other election actors, since in most countries votes are cast and counted in the presence of the parties’ representatives. In the case of online voting, neither the average voter nor the average party representative has the knowledge necessary to understand how the system works. Moreover, whereas traditional systems have the important advantage of decentralization, which is a factual obstacle to large-scale fraud brake, online voting systems are inevitably centralized and rely on equipment, handled by some experts in the absence of public scrutiny. The loss of **visibility**, seen as a loss of (direct) controllability, may undermine the confidence in election procedures and may result in the loss of legitimacy of the outcome. Voters, parties and candidates must be ensured that there has been no malpractice. But trust in an online voting system means having confidence in the machinery and infrastructure rather than simply in the physical and administrative process. As a result, in the case of e-voting much more trust in the technology is needed, as well as in the roles and characteristics of the persons involved (election officials, technology providers, etc.).

Because voting is a public good, **public control** is essential. The regularity of the voting procedure and the control of this regularity are decisive and irreplaceable elements of democratic legitimization. The regularity of elections must not only be affirmed by specialists but should also be confirmed in a way that creates public confidence. Openness must be preserved and encouraged. All operations (authentication, vote recording, tabulation etc.) should be logged and monitored, while secrecy should be preserved. Infrastructure and equipment should be open to inspection by authorized bodies and parties’ representatives. An e-voting system should be developed in such a way as to preserve its **controllability**. Due to the increased complexity of hardware and software the degree of controllability remains questionable. In order for the voting process to be accepted, it is absolutely essential that all

the software used during the operation is fully transparent. Non open-source software is secret by definition and there hardly is a way for anyone to be sure that the software does not include a hidden module, which is secretly aiming at manipulating election results. The question of an open source code appears to be dealt with as an element of an open and revitalized (e-) democracy [6].

Strictly related to the issue of controllability is the question of **liability and accountability**. As voting systems increasingly rely on software and network technologies, it is no longer possible for election officials to be personally knowledgeable or accountable for possible failures. Liability is being “transferred” to other categories of actors and its nature is deeply changing. Furthermore, the fact that in e-voting a number of intermediaries, who are mostly private companies and who are inevitably involved in a public procedure, is involved must be taken into consideration; this complicates the issues of liability and accountability. Even if companies providing equipment and software could be made liable and controllable through appropriate contract clauses, the liability of other intermediaries, such as access, service, and network providers, remains a problem.

Reliability and security requirements are derived from the democratic need to ensure that the outcome of an election correctly reflects the voters’ will. A reliable system must ensure that the outcome of the voting process corresponds to the votes cast, i.e., that it guarantees eligibility, secrecy, equality and integrity. Voting online requires a degree of security beyond the current standard for everyday Internet use. **Security** is a multidimensional notion in the context of e-voting. It primarily refers to the (technically guaranteed) respect for secrecy and freedom, but in reality it covers the entire range of functions and election components such as registration, eligibility and authentication. The ballot being transmitted to the vote counting equipment must be an accurate and non-modifiable copy of the voter’s real choice, with no possibility of modification anywhere in the transmission path, in any of the intervening networks and devices, including the infrastructure used by the voter (integrity). This is an extremely difficult requirement to comply with, given that the opportunity for an external attack would be significantly increased, particularly in view of the vulnerability of personal computers. Security further pertains to the availability of the system and to its protection against accidental or intentional denials of service, which could result in the loss of the capability of the voter to exercise his/her fundamental political rights.

3. E-VOTING: SYSTEM SECURITY REQUIREMENTS

The functional requirements of an e-voting system specify, in a well-structured way, the minimum set of services (tasks) that the system is expected to support, highlighting at the same time their desired sequence and all possible interdependencies. Furthermore, functional requirements are related to many of the usability properties of the system, dominating the properties and characteristics of its interaction model with the user. On the other hand, non-functional requirements are related to the underlying system structure; in principle they are invisible to the user and they normally have a severe impact on architectural decisions. Security requirements and several system-wide properties like flexibility, voter convenience, efficiency etc, are derived through the set of non-functional requirements.

In principle, functional requirements for e-voting systems may vary a lot, since each system is aiming to fulfil the specific requirements of the market segment that it is targeting. On the contrary, the vast majority of security requirements and system wide properties are common to all e-voting systems since they determine the required compliance of the system with the election principles (democracy) and the security and privacy issues dictated by the international legal frameworks. Security requirements are, at a large extent, fulfilled by the voting protocol adopted by the system. Furthermore, the voting protocol dominates the majority of the system wide properties (for instance the performance, flexibility, scalability etc. of an electronic voting system are affected by the respective properties of the voting protocol). On the grounds of the discussion in the previous section, the current section addresses the properties that the voting protocol of an electronic voting system should exhibit. The brief description provided for each one aims to highlight, in a slightly technical way, the attributes - that can be later verified and evaluated both in a qualitative and quantitative way - associated with each property. These properties are:

1. **Accuracy**, also referred to as correctness demands that the announced tally exactly matches the actual outcome of the election. This means that no one can change anyone else's vote (inalterability), all valid votes are included in the final tally (completeness) and no invalid vote is included in the final tally (soundness).
2. **Democracy**: A system is considered to be democratic if only eligible voters are allowed to vote (eligibility) and if each eligible voter can only cast a single vote (unreusability). An additional desirable characteristic is that no one should be allowed to duplicate anyone

- else's vote.
3. **Privacy:** Nobody should be able to link a voter's identity to his/her vote, after the latter has been cast. Computational privacy is a weak form of privacy ensuring that the relation between ballots and voters will remain secret for an extremely large period of time, assuming that computational power and techniques will continue to evolve with today's pace. Information-theoretic privacy is a stronger and, at the same time, harder to obtain form of privacy, ensuring that no ballot can be linked to a specific voter as long as the information theory principles remain valid.
 4. **Robustness:** No reasonably sized coalition of voters or authorities (either benign or malicious) may disrupt the election. This includes allowing abstention of registered voters, without causing problems or allowing other entities to cast legitimate votes on their behalf, as well as preventing misbehavior of voters and authorities from invalidating the election outcome by claiming that some other actor of the system failed to properly execute its part. Robustness implies that security should also be provided against external threats and attacks, e.g. denial of service attacks.
 5. **Verifiability:** implies that there are mechanisms for auditing the election in order to ensure that it has been properly conducted. It can be provided in three different forms:
 - a. **Universal or public verifiability:** means that anyone (voters, authorities, external auditors) can verify the election outcome after the announcement of the tally.
 - b. **Individual verifiability with open objection to the tally:** which is a weaker requirement allowing every voter to verify that his/her vote has been properly taken into account and to file a sound complaint in case the vote has been miscounted, without revealing its contents.
 - c. **Individual verifiability:** which is an even weaker requirement, since it allows for individual voter verification but forces voters to reveal their ballots in order to file a complaint.
 6. **Uncoercibility:** An uncoercible scheme does not allow the voters to convince any other party on what they have voted. In an uncoercible voting scheme a voter neither obtains, nor is able to construct, a receipt proving the content of his/her vote. While the concept of uncoercibility is stronger than **receipt-freedom**, the latter term has been used in the literature as the prevalent expression to denote the security requirement resulting by both the receipt-freedom and uncoercibility properties.

7. **Fairness** ensures that no one can learn the outcome of the election before the announcement of the tally. Therefore, acts like influencing the decision of late voters by announcing an estimate, or providing a significant but unequal advantage (being the first to know) to specific people or groups, are prevented.
8. **Verifiable participation**, often referred to also as declarability, ensures that it is possible to find out whether a particular voter actually has participated in the election by casting a ballot. This requirement is necessary in cases where voter participation is compulsory by law (as in some countries, e.g. Australia, Belgium, Greece) or social context (e.g. small or medium scale elections for a distributed organisation board) where abstention is considered a contemptuous behaviour.

In addition to the security requirements, an electronic voting system should comply with several other non-functional requirements. For example the system must be **reliable** (resistant to randomly generated malfunctions), **user friendly**, it must promote the principle of “**equal election**”, it must be based on **open computer architectures** and **open-source software** etc. In this section, only the system-wide properties that are closely linked to the voting protocol are addressed. These are as follows:

1. **Voter convenience** imposes the need for the walk-away property. As in conventional elections, voters should be able to quickly cast their ballot and then “walk away”, without having to return for a new round of communication with the voting authorities in order to complete the voting procedure. Clearly, this requirement is only related to the vote casting process. Furthermore, the specific property ensures that only standard hardware (i.e. no additional equipment other than a networked device) is necessary for participating in the elections. Normally this is a PC, but a PDA or a digital TV set could be also considered.
2. **Voter mobility**: In order to raise the limitations that apply to conventional elections, there should be no restrictions on the location from which a voter can cast a vote. Although it appears that this requirement simply imposes the need for a properly secured centralised voter database, it actually poses significant obstacles to many election schemes that rely on physical assumptions (e.g. voting booths or untappable channels) for combining contradictory security properties, such as verifiability and privacy or receipt-freedom.
3. **Flexibility**: A system should allow a variety of ballot question formats, in various languages and adaptable to many types of election processes. The ability to handle open-ended questions (i.e. write-in

candidates) can be also claimed through this property but is not compatible with receipt-freedom.

4. **Efficiency:** Taking into account the present figures for hardware performance and network capacity, it becomes clear that performance is a property that cannot be neglected. In fact, almost every election scheme proposed so far employs many processing-intensive cryptographic operations, while communication volume tends to increase as more voters are participating, or more authorities are engaged in their protocols. Thus the complexity of a scheme becomes a crucial system parameter.
5. **Scalability:** The time needed by a voter to cast a ballot poses an upper bound to the number of voters that are allowed to participate in a specific election, given the election window (the period of time that online voting is allowed) and the available resources (servers, network availability and capacity, etc.).

Clearly, some of the requirements listed above are contradicting each other, while others cannot be fulfilled given the available technology. Voter privacy, for example, demands that a ballot cannot be linked to the voter. On the other hand, in order to comply with the verifiability property, it should be possible to verify - *inter alia* - that each and every ballot included in the tally, was cast by an eligible voter. Since preserving privacy breaks the link between the voter and the ballot, after the latter is cast, this is definitely not an easy task. Individual verifiability contradicts uncoercibility. In order for the voters to be able to object, in case they notice that their vote has been miscounted, a receipt describing the way they voted should be supplied to them. But the same receipt may be utilised for selling their vote, just by presenting the receipt to the buyer, or make them subject to coercion, since the coercer will be able to verify the way they voted. Moreover, fairness demands that no intermediate results are available to anyone, the election organisers included, before the election has ended. This often reduces voter convenience and eliminates the “walk-away” property, as it will be explained later, since the voter has to further interact with the organisers, possibly for sending a decryption key or otherwise allowing access to his/her ballot. Finally, efficiency often falls for obtaining other properties, especially universal verifiability and uncoercibility, since the employment of computationally complex and communication intensive solutions is necessary.

On the other hand, although many of the security requirements for an electronic voting system are conflicting, they are, at the same time, closely pair-wise interrelated, as the existence of one property implies the second or simply cannot exist without it. An example of such a pair is uncoercibility

and privacy. As already mentioned, the former is a stronger requirement than the latter, since it protects one's vote from disclosure, even if one voluntarily wishes to prove their vote to a third person. An incoercible voting system ensures the privacy of the voter, by definition. Verifiability is a powerful supporter to the accuracy of a voting system. A system possessing strong verification mechanisms thwarts attackers wishing to disrupt an election, since their efforts will have no chance of affecting the result. In some cases, where the identity of the voter remains attached to the ballot, lack of fairness may cause breach of privacy. This can only happen if an intermediate result of the election can be computed, thus making possible to find out how a particular voter voted, by computing a partial tally immediately before and after his/her casting of the vote. Robustness supports, in an indirect way, fairness and often privacy. Fairness is benefited since intermediate results are not leaked when an election is abruptly stopped due to a malicious action. This could lead into producing different results when the election is repeated, even in exactly the same context. Finally, voter mobility and convenience are closely related; since in most cases the requirement for additional hardware also implies that the voter has cast his/her vote from a certain place, appropriately equipped. For example, untappable channels, often required to obtain receipt-freedom, can be only implemented in certain places (e.g. polling places). A scheme offering voter mobility is almost certain to provide for convenience as well.

4. E-VOTING: VOTING PROTOCOLS

A large number of protocols and more generalized schemes for electronic voting have been proposed. Many of them share some common characteristics, a fact that has been utilized as the criterion for their rough classification, presented next. For each protocol family, discussion of the most promising protocol, in terms of its suitability to support electronic voting as a result of satisfying the majority of the previously mentioned requirements, is provided.

4.1. Trusted Authorities

One of the most common approaches to e-voting depends on the involvement of an independent trusted third party. Protocols capitalizing on the concept of trusted authorities attempt to build on the same principle that conventional elections do; that is the existence of one or more trusted agents that will faithfully administer the election. Voters interact with those authorities to register and submit their ballots and rely on them to produce the correct tally, without compromising their privacy. In [7], Karro and Wang

proposed a practical and secure voting protocol for large-scale elections based on trusted authorities, which attempts to solve most of the problems that other protocols relying on this concept face. The protocol employs six distinct voting authorities, namely the registrar, the authenticator, the distributor, the counter, the matcher, and the verifier. The communication model is based on the use of off-the-shelf secure communication protocols, like HTTPS, between the voters and the authorities. However, rather complicated methods are used for filtering suspicious communication among the authorities, in order to prevent collusion. The security of this protocol is based on mutual auditing and checkout. Each authority participates in an internally executed communication protocol, designed to prevent collusion. After the election is over, each authority is publicly audited by the others. According to the authors, their construction fulfils democracy, provided that no cheating occurs in the registration phase. Accuracy is obtained because voters are given a receipt and they are allowed to view the published lists at the verification phase. A legitimate vote cannot be altered, duplicated, or removed without being detected. No authority can generate votes for unused ballots without being detected, because of the lists published by the end of the election. Regarding privacy, the only authority that can see the voters' names is the registrar. The registrar, however, can only see the encrypted ballot cast by a particular voter's ID and has no way to decrypt this vote without collaborating with the counter, but the communication model does not allow them to conspire. Voters can be sure that their votes were tabulated by verifying that their IDs and encrypted keys are in the lists posted by the authenticator and the counter, therefore the scheme supports individual verifiability. Although the protocol is not designed to be receipt-free (each voter obtains a receipt, proving the way s/he voted), it allows the voter to change his/her vote. This means that a coercer can only ensure that the voter has cast the desirable vote by forcing her/him to vote just before the closing time of the election. The registrar is aware of the voters that have participated in the election. A list of them can be easily prepared and published, so verifiable participation is obtained. The protocol also fulfils the voter convenience and voter mobility properties. Furthermore, it can be considered efficient, since only limited computation is necessary. Finally, since there are no restrictions on the ballot form, this protocol may accommodate any type of election; therefore, it is flexible.

4.2. Anonymous Voting

Another widely used approach to electronic voting relies on the concept of anonymity. The main idea behind protocols following this approach is to allow voters to anonymously submit their ballot, in order to preserve their privacy. Since this would allow for fraud, the notion of eligibility token has been introduced. These tokens are analogous to voter ID cards or handbooks used during conventional elections for certifying that the bearer or the person depicted in the attached photograph is an eligible voter. The eligibility tokens are provided by the authorities to all eligible voters during the registration phase and after their credentials have been verified. The voters subsequently attach this token to their ballot, thereby validating it, and send them both to the authority through an anonymous channel. It is important to emphasise at this point that the token is assigned to a voter in an untraceable manner, meaning that the issuing authority has no way to correlate tokens with voters. On the contrary, finding out whether a token is valid or not is a trivial task. Obviously, eligibility tokens should be very carefully handled, since anyone who possesses a token is allowed to cast a legitimate ballot. The main differentiation between the protocols of this family is in the way that tokens are generated. In [8] a multi-authority protocol using blind signatures and bit-commitment on the ballot to form an eligibility token, is presented. The token is subsequently submitted via an anonymous channel. This scheme is suitable for large-scale elections, since the communication and computation overhead is fairly small even if the number of voters is large. It is a classical protocol, in the sense that it has been the basis for numerous enhancements and implementations. According to this scheme the participants are the voters, a validator and a tallier. Finally, it is assumed that an anonymous communication channel exists, utilised by the tallier and the voters for their communication. Another protocol, proposed in [9], extends the one proposed in [8]. This scheme includes the candidates in the voting process, each computing a partial tally, in order to prevent malicious authorities from rejecting ballots or stuffing the ballot box. The final tally is produced by the tallier using a t-out-of-N threshold scheme. The model of the original protocol has been further modified with the addition of a trusted third party, whose role is limited to the newly introduced “preparation (announcement) phase”. Furthermore, in addition to the anonymous channels, a bulletin board is utilised for communication. The checks performed by the candidates and the counter, during the voting phase, ensure that a valid ballot will always be accepted by the honest candidates, and the counter and hence this scheme can be considered as accurate. The privacy of the votes is preserved even if the administrator, the counter and the candidates conspire. The scheme is also universally verifiable, since if a voter claims disruption by the validator or the

counter, s/he can keep his/her vote secret and present the certificate instead. Moreover, if the majority of the candidates are honest, a voter or a conspiring group of the candidates cannot disrupt the election; this makes the scheme robust. Given that the blind signature scheme and the threshold scheme are secure, only eligible voters are able to vote and no voter can vote more than once, so the scheme can be also characterised as democratic. Finally, since counting is done only after the voting phase is completed, the scheme can be considered to be fair. However, it is emphasised that the fulfilment of all security requirements by the specific protocol strongly relies on the assumption that the trusted authority is functioning as expected. Furthermore, the inherent problem of forcing the voters to interact twice with the authorities inhibits the fulfilment of the “walk-away” property. Finally, receipt-freedom is not supported and thus a voter can easily sell his/her vote or a coercer can easily extort a voter.

4.3. Homomorphic Encryption

This broad class of electronic election schemes follows a different approach. Instead of hiding the identity of the voters using eligibility tokens and anonymous voting methods, they hide the contents of the ballot itself. The ballot is submitted in a traceable manner, attached to the voter identity, so that the verifiability property is easily satisfied. However, at some certain moment, the tally of the election has to be computed and this implies that the ballot must be decrypted, thereby violating voter privacy. This is avoided by encrypting the ballot using a homomorphic encryption function. Briefly, a cryptographic function E is called (\otimes, \oplus) -homomorphic if the equation: $E(T1)\otimes E(T2) = E(T1 \oplus T2)$ holds for any two plaintext $T1, T2$. Usually, but not necessarily, the operators \otimes and \oplus represent modular multiplication and addition, respectively. Although this property represents a weakness to the strength of this function, it is very important for e-voting applications, since if the encrypted ballots are “multiplied” together they produce a result that is the encrypted tally of the election. In other words, the vote tally can be calculated without decrypting any of the ballots. However, the addition used limits the votes to a “yes” or “no” option (1 or 0, respectively), whereas a proof is required that the encrypted ballot indeed contains such a vote and not an arbitrarily large value. It is clear that the above scenario may fail under a corrupt authority. In order to tolerate a misbehaving “teller”, the encryption of the tally can be distributed to several authorities in such a way that only coalitions of a certain size can decrypt the tally. Schemes adopting this approach are presented in [10,11], the concept being originally introduced in [12-14]. Interesting variations were proposed in [15-16], replacing the homomorphic encryption by publicly verifiable secret sharing, in [17],

proposing a hierarchical multi-candidate election system, and in [18-20]. In [19,20] Damgård and Jurik propose a generalisation of Paillier's scheme [21] using computations modulo $Ns+1$, for any $s \geq 1$, allowing reducing the expansion factor from 2 for Paillier's original system to almost 1. They also propose a threshold variant of it, which is subsequently used to construct an electronic voting scheme along the lines of the one proposed in [11]. Their scheme involves M voters V_1, \dots, V_M , and N authorities A_1, \dots, A_N . The initial scheme only allows for "yes" or "no" voting, but it was later expanded to allow 1-out-of- L elections, essentially by holding L elections in parallel. A bulletin board is used for communication among the participants. The scheme preserves all properties of [11], but improves dramatically the tallying time, since the use of brute force for finding the discrete logarithm corresponding to the result is no more necessary. Receipt-freedom is not considered, but the authors are claiming that combining the framework presented in [22] with their scheme would allow the fulfilment of the specific property.

Table 1 [3] summarises the requirements fulfilled by the protocols and schemes presented above. In order to assess a specific protocol it is essential to evaluate the "requirement fulfillment matrix" in conjunction with the assumptions made by the protocol. For example, some schemes based on the trusted authority model appear to fulfil most of the requirements, but the assumption that every authority remains honest (especially when no cross-controls exist) is very strong and, thus, unlikely to be true in a real environment. Also, receipt-freedom is often obtained under strong assumptions, which render impractical the respective voting protocols.

Table 1: Security requirements fulfilled by protocols and schemes

Voting Protocols and Schemes	Security Requirements											System Wide Properties			
	Accuracy			Democracy											
	Inalterability	Completeness	Soundness	Eligibility	Unreusability	Privacy	Robustness	Verifiability	Uncoercibility	Fairness	Verifiable participation	“Walk-away”	Voter mobility	Flexibility	
TRUSTED AUTHORITIES															
[7]	Yes	Yes	Yes	Yes	Yes	Cmp	No	Indi	¹ No		Yes	Yes	Yes	Yes	
ANONYMOUS VOTING															
[8]	Yes	Yes	No	Yes	Yes	Cmp	No	Opn	No	Yes	No	No	Yes	Yes	
[9]	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	No	Yes	No	Yes	Yes	Yes	
HOMOMORPHIC ENCRYPTION															
[15]	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	No	Yes	Yes	Yes	Yes	No	
[22]	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Indi	Yes	Yes	Yes	Yes	No	No	
[20]	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	³ No	Yes	Yes	Yes	Yes	² No	
[17]	Yes	Yes	Yes	Yes	Yes	Cmp	Yes	Univ	³ No	Yes	Yes	Yes	Yes	² No	

¹ Allows multiple ballots, only the last is taken into account.

² Allows extension to multi-way elections, with increased complexity and cost.

³ Can be obtained by applying the framework presented in [22].

Privacy: Inf= information-theoretical, Cmp = computational.

Verifiability: Indi = individual, Opn = individual with open objection, Uni = universal.

5. CONCLUSIONS

Voting systems have evolved in response to specific problems and needs of political systems. Virtually there is a dialectic/interactive relation between political systems and election systems, as the latter influence and reflect the way the former function and evolve. Technology could and should serve as a means of coping with the crisis of participation and confidence that democracy is facing in our days. It could serve towards making democracy more accessible to citizens but it is not a panacea; it cannot itself revitalize democracy and redress the drift, just as convenience and “mouse-click voting” cannot replace participation.

Changes must be assessed and evaluated on the basis of criteria embedded in democratic constitutions and liberal political culture: equality, freedom, transparency and accountability. We should resist changes that would fail to achieve public confidence or to meet the highest democratic standards. Unequal access to ICT infrastructure and capabilities remains a crucial problem to solve, in order to enable all citizens to have an impact on political life and to avoid a re-construction of new political elites and a “restoration” of (aristocratic?) “two-thirds democracies”.

The employment of electronic voting systems for organizing and conducting large-scale elections in a secure way is feasible, provided that certain deficiencies of existing voting protocols are successfully addressed. Several security requirements of such systems are contradicting each other, thus requiring special treatment. On the other hand, there are requirements that can either not be fulfilled, given the currently available technology, or they can be handled, provided that a substantial increase in cost and complexity is accepted.

None of the existing voting protocols supports in an acceptable way (i.e. with reasonable cost and complexity or/and by avoiding strong and unrealistic assumptions) the entire list of requirements with which the voting protocol of a secure electronic voting system is expected to comply. It is clear that the solutions are not straightforward, in particular since handling specific requirements (such as uncoercibility or universal verifiability) may have side effects on the complexity of the voting protocol, which in turn may affect the performance of the system and thus limit its scalability. However, the extensive research work in the area of cryptographic algorithms and distributed systems is expected to produce, soon, exploitable results.

6. ACKNOWLEDGMENTS

This work has been supported, in part, by the IST/e-vote project (An Internet-based electronic voting system) of the European Commission.

7. REFERENCES

- [1] D. A. Gritzalis (2003), "Preface", in D. A. Gritzalis (Ed.), Secure Electronic Voting, Kluwer Academic Publishers, pp. xi-xiv.
- [2] L. Mitrou, D. Gritzalis, S. Katsikas, G. Quirchmayr(2003), "Electronic voting: Constitutional and legal requirements and their technical implications", in D. A. Gritzalis (Ed.), Secure Electronic Voting, Kluwer Academic Publishers, pp. 43-60.
- [3] C. Lambrinouidakis, D. Gritzalis, V. Tsoumas, M. Karyda, S. Ikononopoulos (2003), "Secure electronic voting: The current landscape", in D. A. Gritzalis (Ed.), Secure Electronic Voting, Kluwer Academic Publishers, pp. 101-122.
- [4] L. Mitrou, D. Gritzalis, S. Katsikas(May 2002), "Revisiting legal and regulatory requirements for e-voting", in Proc. of the 17th IFIP International Information Security Conference, M. El Hadidi (Ed.), Kluwer Academic Publishers, Egypt, pp. 469-480.
- [5] e-vote: An Internet based electronic voting system, Legal and regulatory issues on e-voting and data protection in Europe, EU-IST-2000-29518 (D. 3.4.).
- [6] S. Ikononopoulos, C. Lambrinouidakis, D. Gritzalis, S. Kokolakis, K. Vassiliou (2002), "Functional requirements for a secure electronic voting system", in Proc. of the 17th IFIP International Information Security Conference, pg. 507-520, Egypt.
- [7] J. Karro, J. Wang (1998), "Towards a practical, secure and very large-scale online election", in Proc. of the 15th Annual Computer Security Applications Conference, IEEE Press, USA.
- [8] A. Fujioka, T. Okamoto, K. Ohta(1992), "A practical secret voting scheme for large-scale elections", in Advances in Cryptology, Proceedings of AUSCRYPT'92, LNCS 718, pp. 244-251, Springer-Verlag.
- [9] A. Baraani, J. Pieprzyk, R. Safavi (May 1994), "A Practical electronic voting protocol using threshold schemes", Centre for Computer Security Research, Dept. of Computer Science, University of Wollongong, Australia.
- [10] R. Cramer, M. Franklin, B. Schönemakers, M. Yung(May 1996), "Multi-authority secret-ballot elections with linear work", in Advances in Cryptology – EUROCRYPT'95, LNCS 1070, pp. 72-83, Springer-Verlag.

- [11] R. Cramer, R. Gennaro, B. Schönemakers, "A secure and optimally efficient multi-authority election scheme", in Proc. of EUROCRYPT'97, Germany, Springer-Verlag, LNCS 1233, pp. 103-118.
- [12] J. Benaloh (December 1987), "Verifiable secret-ballot elections", Ph.D. Dissertation, Yale University, YALEU/CDS/TR-561.
- [13] J. Benaloh, M. Yung(August 1986), "Distributing the power of a Government to enhance the privacy of votes", in Proc. of the 5th ACM Symposium on Principles of Distributed Computing, pp. 52-62.
- [14] J. Cohen, M. Fischer(October 1985), "A robust and verifiable cryptographically secure election scheme", in 26th Annual Symposium on Foundations of Computer Science, IEEE Press, pp. 372-382.
- [15] B. Schönemakers (1999), "A simple publicly verifiable secret sharing scheme and its application to electronic voting", in Advances in Cryptology - CRYPTO'99, LNCS 1666, pp. 148-164, Springer-Verlag.
- [16] A. Yung, M. Young(2001), "A PVSS as hard as discrete log and shareholder separability", in Proc. of 4th International Workshop on Practice and Theory in Public Key Cryptosystems, Korea, LNCS 1992, pp. 287.
- [17] O. Baudron, P. Fouque, D. Pointcheval, G. Poupard (August 2001), "Practical multi-candidate election system", in Proc. of the 20th ACM Symposium on Principles of Distributed Computing, USA, pp. 274-283, ACM Press.
- [18] I. Damgård, J. Groth, G. Salomonsen (2003), "The theory and implementation of electronic voting systems", in D. A. Gritzalis (Ed.), Secure Electronic Voting, Kluwer Academic Publishers, pp. 77-100.
- [19] Damgård, M. Jurik (March 2000), "Efficient protocols based on probabilistic encryption using composite degree residue classes", RS-00-5, Dept. of Computer Science, University of Aarhus.
- [20] Damgård, M. Jurik(2001), "A generalisation, a simplification and some applications of Paillier's probabilistic public-key system", in Proc. of the Fourth International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1992, pp. 119-136.
- [21] P. Paillier (1999), "Public-key cryptosystems based on discrete logarithms residues", in EUROCRYPT'99, LNCS 1592, Springer- Verlag.
- [22] M. Hirt, K. Sako (2000), "Efficient receipt-free voting based on homomorphic encryption", Theory and Application of Cryptographic Techniques, pp. 539-556.