E-Voting Solutions for Digital Democracy in Knowledge Society

Marian STOICA, Bogdan GHILIC-MICU
Department of Economic Informatics and Cybernetics,
Bucharest University of Economic Studies, Romania
marians@ase.ro, ghilic@ase.ro

Emergent technologies specific to current information and knowledge society, and social networks influence every aspect of our existence, from lucrative activities to recreational ones. There is no part of our life that is not influenced by the explosive development of general information and communication technologies. We witness a spectacular and until recently unimagined metamorphoses of work nature, business process reengineering, controversial evolution of social networks and new directions of electronic government. Over this background of changes, we take on the tasks of deepening the understanding of field that is largely unexplored, namely the electronic vote in digital democracy, without taking any side, pro or against this type of casting our electoral options. The current context encompasses technological, legislative, political, economic and social aspects. Even more, the context of electronic voting in digital democracy involves aspects regarding globalization, technical challenges concerning interoperability, data standardization and security.
***Keywords**: Digital Democracy, Knowledge Society, E-Voting, Cryptographic Schemes, ICT*

1 Introduction

The field of electronic democracy and especially electronic voting is largely unexplored, its dimensions themselves being in a continuous changing process. There are numerous debates on this field, both in practice and literature, most of them on contradicting terms due to security problems and social and political implications. Thus, considering the expansion electronic voting systems built on the development of information and communication technology (ICT), solving the security aspect is crucial. Voting is a critical process of citizen participation to democracy, facilitating the manifestation of general opinion, but most specialists consider designing such a system complex and delicate.

Security of electoral process must be perceived on the level of national security, because the legitimacy of a democracy depends on the degree of equitable, open and trustworthy elections [1]. The lack of trust in organization of the electoral process and government actions is a hot subject in democratic countries, thus also in Romania. Therefore a computerized system for electronic voting is a great responsibility, its failure having grave consequences on public trust in the political class. [2]

Numerous international studies have been recently organized on international level with the purpose of evaluating the advantages and drawbacks of electronic voting. Worth mentioning is the European project *E-democracy: Technical possibilities of the use of electronic voting and other Internet tools in European elections (IP/A/STOA/FWC/2008-096/LOT4/C1/SC2)* [3] carried on between January 2010 and September 2011, which highlights in its final report *E-public, e-participation and e-voting in Europe - prospects and challenges* the European experience in the field. However, the results and proofs are not conclusive because of the large diversity of existing systems that support a wide range of contexts and requirements. Examination of digital democracy cannot be isolated from other scientific and academic fields. Electronic voting is rather a social and political project then a technical one, a component of the political dimensions of the new media technologies, leading to improvements of social nature through increasing the number of citizens involved in the political decision process.

DOI: 10.12948/issn14531305/20.3.2016.06

Traditional voting processes seem to lack security. The concept of hiding a piece of paper inside an envelope to protect its confidentiality is more and more contested. In the current technological context, the voter – considered anonymous – can be easily identified using simple technology the reads finger prints or DNA samples, why wouldn't technology replace such a system? Since numerous countries (like Canada, USA, France, Great Britain, India, Estonia, Holland, Romania etc.) have approached the subject, the basic question is no longer if ICT must or must not be involved in the electoral process, but rather what kind of technology must be used in order to build an electronic voting system.

Electronic participation must be understood as an interaction, mediated by technology, between the sphere of civil society and the sphere of politics. There are solutions and software systems destined to increase this participation, known as electronic methods or e-methods, like blog, webcast, polls, chats, forums, electronic petitions etc. Still, we must understand from the beginning that there is a major difference between e-shopping (for example) and e-voting.

Electronic voting may be analysed from the perspective of a mechanism designed to improve electronic participation, the selection of procedures and technologies being a very important step. The electoral process is different from one nation to another, not only regarding the way to determine the elected candidates (for example proportional or according to majority), but also regarding the procedures and methods used to cast the votes, organizations involved etc.

For example, in Europe voting varies from internet voting (in Estonia) [4] to fully manual process (in Greece and Italy). Currently employed technologies vary also from classic paperback ballots, punch cards, optical scanning to remote voting systems, each of these technologies having its own advantages and drawbacks. There are many countries in Europe that have experimented with more or less successfully at least one electronic voting solution (see chapter 4).

2 Short History

In order to better understand the notion of electronic voting we should first revisit the evolution of the electoral process in general, correlated with corresponding technologies. Since it is a specific process for democratic societies, the electoral process does not transcend the historical evolution of these societies. Therefore we can talk about ballots used in antiquity (ancient Rome, around 135 B.C), 17th and 18th century in USA and England (1839, *The People's Charter*) and so on. The main problem in all these historic moments was the concern about fraud (still an actual concern, unfortunately). The most popular solution to tackle this problem comes from Australia (1856-1858), with the liberalization of voting for males aged at least 21 in a few administrative regions. The method used would later propagate world-wide, being known as *Australian secret ballot* [5]. The basic form is a paperback document that lists the names of all candidates, allowing the voter to mark his choice (Figure 1). The paper is then inserted into an envelope, sealed and placed in a box. At the end of the day, envelops are opened and votes are counted. Since it is expectable that any person has its own interests, ballots are only manipulated under strict supervision of a member of the opposed political party. The worst problem about this scheme is the way votes are counted.

At the end of 19th century, the mechanical voting machine is introduced in USA (New York, 1892) [6]. At first glance, this machine eliminated the prejudice about vote counting and offered the results immediately. Using these machines, the vote is instantly counted when the voter exits the voting booth, but they offered no way to save the results (create a backup copy), which is a downside. Additionally, the machines were very complex, with hundreds of wheels/pieces that required detailed testing before the beginning of the electoral process.

In 1962 the state of Georgia, US, introduced a voting system based on punched cards (developed by IBM - *Votomating machine IBM Portapunch*). The ballot is a form of the

DOI: 10.12948/issn14531305/20.3.2016.06

Australian secret ballot, designed to be counted with standard data processing devices that worked on punch cards. They were used to ensure votes are cast in a uniform way. These systems have several disadvantages, most important one being the way cards are punched. The system perforates the card in order to record the voter choice but does not endure a clean perforation or a way to discern the voter intention in case of doubts.

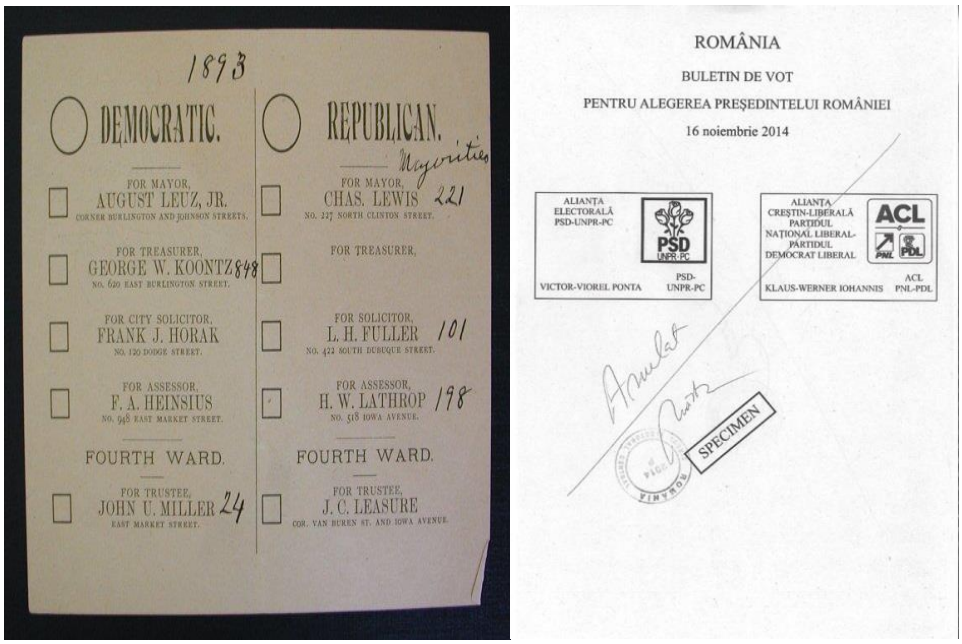

Fig. 1. Ballots in traditional electoral process (USA 1893, Romania 2014). Source: http://homepage.cs.uiowa.edu/~jones/voting/pictures/, http://www.mediafax.ro/politic/

In parallel, other US states adopt various systems based on optical scanning. They involve a system where voters cast their choice on a paper ballot, which is stored in a sealed box and later processed (counted) by a scanning system. For the voter the implementation is similar to the traditional vote, the ballot being similar to the Australian one, except the markings on the side that allow the device to identify the voter's choice. The main problem of these systems is their accuracy. [7]

DRE system developed and used 100% in Brazil

iVotronic DRE also usable by visually impaired citizens

Fig. 2. Examples of DRE systems actually used. Source: www.vermelho.org.br, http://www.essvote.com/products/3/6/dre/ivotronic/

At the end of the '80s direct recording electronic systems were introduced (DRE – Direct Recording Electronic voting system), considered the most recent development of voting systems. They are similar to traditional voting machines, only the mechanical parts

DOI: 10.12948/issn14531305/20.3.2016.06

are replaced by buttons. DRE systems record the vote by electronically displaying a ballot which can be marked by the voter either through buttons or directly on the touch screen (Figure 2). Data is electronically processed then ballots and votes are stored in the electronic memory. DRE usage by voters has increased from 7.7% in 1996 to 28.9% in 2004. In 1996 this type of systems were exclusively used in Brazil voting processes. [8]

There are two reasons for full employment of DRE systems in Brazil: first the biometrical fingerprint identification system ensures unique votes from each person and second little education is required in order to use these machines – alphabetization (literacy) index for Brazil is little above 85.0%, according to [9], page 99. From this point of view Brazil ranks 134 out of 215 countries in a hierarchy published by http://www.getamap.net/.

3 Electronic Voting

The generalized trends of decreasing participation in electoral processes, corroborated with an increased usage of Internet constitute serious premises for the emergence of new opportunities for electronic voting. Today, neither the literature nor current electoral practices have a unanimously accepted definition of electronic voting. The term is used ambiguously, in an attempt to describe a large spectrum of electoral tasks, from voter registration to casting the vote through a computer network. Under the digital democracy perspective, many authors consider e-voting as the ultimate voting solution generated by the voter convenience. On the other hand, is supposed to increase the participation of voters, especially by attracting the young voters towards electoral processes.

As an example, the last report of the European Parliament on e-voting (publicly disseminated in [3], but also available on the official site http://www.europarl.europa.eu/) analyses e-voting from the perspective of its potential to increase participation to electoral processes, mainly for European parliamentary elections (page 111 in the report). Thus, the report highlights the importance of prerequisites for implementation of an e-voting system:

- ✓ Correct identification of the voter;
- ✓ Transparency of the voting process;
- ✓ Traceability of the ballot;
- ✓ Vote secrecy;
- ✓ Transparency of vote centralization;
- ✓ Prevention of multiple voting.

Transcending the idea of using electronic devices to make the electoral process easier, more efficient and cheaper (see the DRE systems, for example), electronic voting in the digital democracy may take two shapes: *supervised electronic voting* – requires the presence of a government or electoral authority representative, and *remote electronic voting* – does not require supervision from a representative and may be performed through internet (*i-voting*) or mobile devices (*m-voting* through SMS or web/m-web).

Regarding the remote electronic voting through Internet, the literature groups e-voting solutions in three main classes: kiosk voting, poll station internet voting, remote internet voting – Figure 3).

Kiosk voting model require voting machines to be placed not only in designated polling stations, but also in public location easily and frequently accessed by voters in their daily routine (like markets, gas stations, malls, libraries, auditoriums etc.). The advantage of this model is that the vote may be cast anytime (in the designated time frame) while carrying out the daily routine, with little to no disturbance. In this way the polling station comes closer to the voter.

Internet poll sites allow a greater convenience and better efficiency than traditional voting systems. The voters may choose from several polling stations. The system is not limited to the residential polling station, and the voter may go to any polling station he wants in the country. Once the election officials identify the voter, the voting process, general technological environment (voting system) and security risks are easy to manage.

DOI: 10.12948/issn14531305/20.3.2016.06

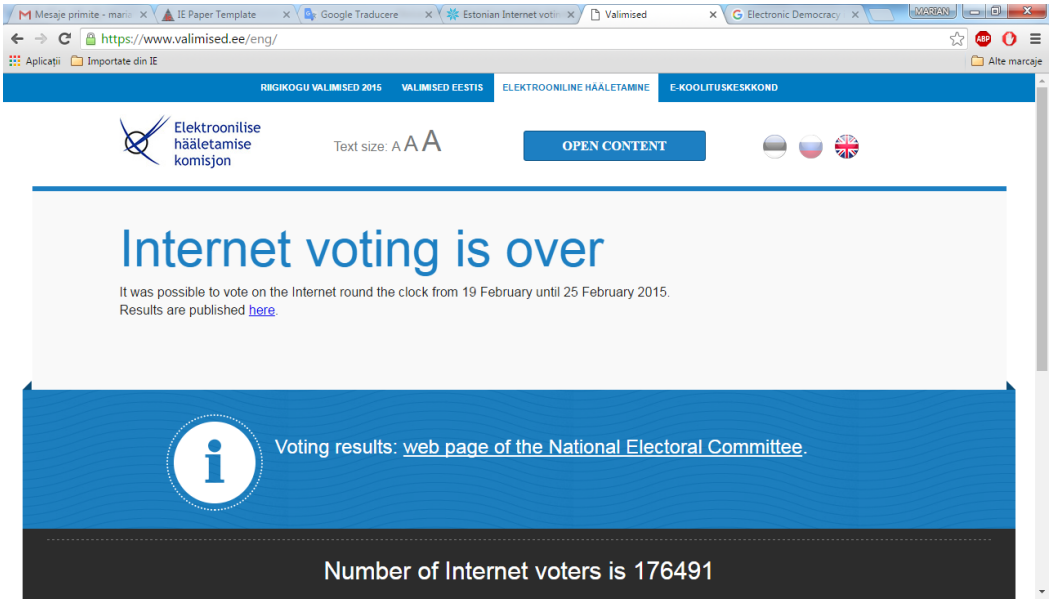

Fig. 3. Estonian I-Voting platform (Parliamentary election 2015)

Remote internet voting seeks to maximize the convenience and ease of access for users, allowing them to vote from any available location through the global network. Considering the voting takes place in a private sphere, security issues become very important. Without an official control of the voting platform there are numerous opportunities for malicious individuals to intervene and affect the election results.

4 European E-Voting Experiences

While some futurologists foresaw an evolution of the human society towards artificial intelligence, passing through information and knowledge society, the contemporary reality shapes a new social paradigm: technology and social network society. We face the most aggressive technological expansion in our history together with the pervasive role of social networks in all spheres of our lives. According to www.socialmediaro.com the most important social platforms are Facebook, Twitter, LinkedIn, Xing, Renren (everybody's web in China), Google+ Disqus, YouTube etc. (any attempt to create a hierarchy would be subjective). One of the most recent (political) events intermediated and supported by the social media was the June 23rd, 2016 referendum in UK regarding this state's position towards European Union (the famous "Brexit"). Once more, technological and social network Europe must make a step forward regarding what we generically call digital democracy.

Thus, most EU states have already adopted or are working on adopting various solutions for electronic voting. Through its specific reports, European Parliament [3] establishes three levels of e-voting systems implementation:

- ✓ First level refers to national-level e-voting, for electing the country president or the parliament (general elections).
- ✓ Second level targets local and/or regional level, for electing local or regional (county) administration.
- ✓ Third level concerns organization-level elections (organizations, associations, corporations), for example election of administration councils, company presidents etc. (one interesting application would be election of university authorities in Romania).

Speaking of European e-voting experiences, we have to start from Estonian experience, which proved to be a success story started with 2005 local elections (but previously supported by a clever political culture since 2002). At that time, within a three day voting timeframe, the Estonian I-Voting system was used by more than 9000 voters (of the 1.06 million registered voters). In the following years (2007, 2009, 2011, 2015) the number of

DOI: 10.12948/issn14531305/20.3.2016.06

voters using the e-voting system grew heavily, reaching 176,491in February 2005 (see Figure 3). It is also true that Estonia was the victim of a significant cybernetic attack in 2007, immediately after the national elections, which raised serious concerns regarding e-vulnerability. We believe that the main aspect that made the Estonian project a success resides in the relatively low population of the country (1.294 mil. inhabitants in 2016, according to Wikipedia). This allows, in principle, a better management of critical situations that may arise during electoral processes. Also, through its policies, Estonia wanted to implement an e-voting system. Considering the demographic aspect, Cyprus, Luxembourg or Malta could be successful as well.

On first and second level of implementing e-voting solutions, various attempts to automate the electoral process were implemented in other European countries, like Holland, Norway, France, Great Britain, Switzerland, Germany and Romania. For technical, economic or political reasons all these countries have postponed the implementation of a proper generalized e-voting system. In Romania, the first attempt of e-voting was used during October 2003 referendum to validate Constitution modifications. At that time, Romanian government has implemented an electronic voting solution for military personnel deployed in international missions (over 1600 persons participated). The problem of electronic voting remains open for Romania, especially for citizens living abroad.

5 Electronic Voting Algorithms

In a general approach, the voting process may be analysed on three phases: initialization, actual voting and vote counting (Figure 4). From the perspective of an electronic voting system, the initialization phase involves verification of the box that will store the ballots (must be empty), verification and validation of the voter list, candidates, verification and sealing of the ballots. It may also include processes like candidate registration (allow an individual to register his interest to be a candidate), creation of ballots (after all candidates have been registered), voter registration (allows an individual to register his interest to be a voter), distribution of ballots to eligible voters), task management (creation or revocation of rights).

The actual voting phase takes place after voter was successfully authenticated and the ballot was distributed. The process involves casting the vote by the voter, updating the number of voters that casted their vote, sending a confirmation message to the voter (confirm he successfully voted).

Counting the votes starts once voting is finished and involves validation of ballots, counting the number of votes cast for each candidate, comparing the final result with the number of voters recorded by the system in previous phase (thus avoiding frauds by adding/removing ballots) and publication of final results. The system must offer the possibility to recount the votes if required.

Electronic voting systems are similar to any product seeking market success, and providers seek to standardize them. The most remarkable endeavour in this direction belongs to the OASIS consortium (Organization for the Advancement of Structured Information Standards – Advancing open standards for the information society) which proposed in fall 2009 a XML based standard (developed over eight years) developed for data exchange in electoral processes, called Election Mark-up Language (EML). [10] EML was adopted as OASIS standard and registered at technical committee ISO/IEC JTC1 – Information Technology to be adopted as ISO standard (not adopted yet). The standard defines structured data transfer between electronic voting system and electoral service providers from private or public organizations. [10]

DOI: 10.12948/issn14531305/20.3.2016.06

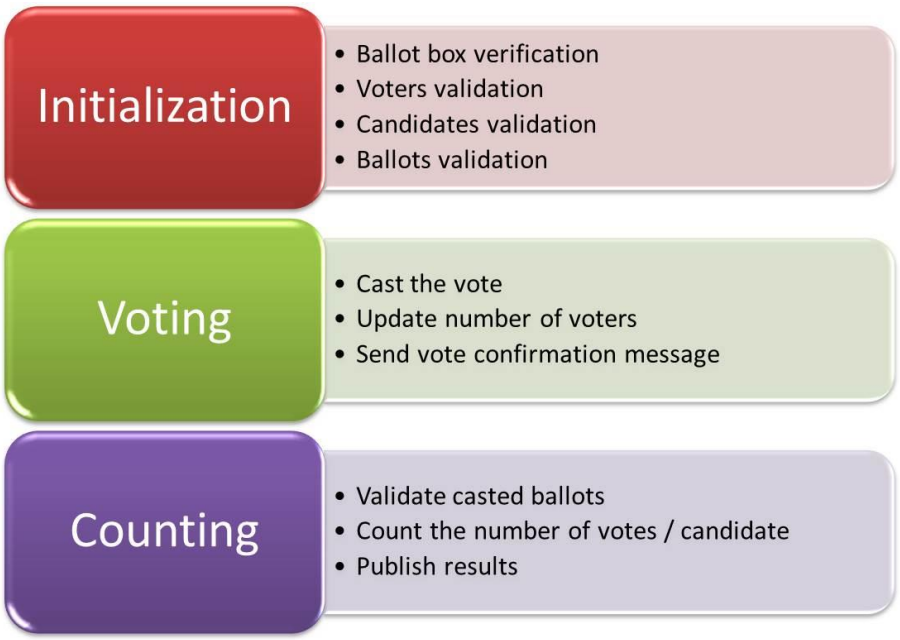

Fig. 4. General steps in the voting process

Developed in an agile approach (see SCRUM methodology) and observing the general phases of an electoral process, EML implements electronic voting in three steps: pre-vote, vote and post-vote (Table 1). [11]
There are various methods to nominate candidates, according to each country's legislation. The nominating process finalizes with the creation of a list. Also, depending on local laws, voters may have to register before participating to actual voting (in many cases they are automatically registered). The voter registration finalizes with a list of eligible voters.

Table 1. General steps of voting process vs. EML

<table>
<tr><th colspan="2">Pre-Vote</th><th colspan="2">Vote</th><th>Post-Vote</th></tr>
<tr><td rowspan="3">Nominate candidates</td><td>Elect candidates</td><td colspan="2">Choose voting option</td><td>Count votes</td></tr>
<tr><td>Candidates' answers</td><td rowspan="4">Cast the vote</td><td>Electronic</td><td>Publish results</td></tr>
<tr><td>Generate candidate list</td><td rowspan="3">Conventional</td><td rowspan="3">Possibility of recounting</td></tr>
<tr><td rowspan="2">Register voters</td><td>Identify voters</td></tr>
<tr><td>Generate voter list</td></tr>
<tr><th colspan="2">Initialization</th><th colspan="2">Voting</th><th>Counting</th></tr>
</table>

The voting phase is based on results from the pre-voting phase, allowing eligible voters to make a choice and cast their vote. The main activity of post-voting is counting the votes and presentation of results. Counting is a crucial step and must allow for recounting possibility.

6 Ensuring Security of Electronic Voting

As any technology, beyond the obvious advantages (reduced medium and long term costs, better participation to elections etc.) of electronic voting, there are some controversial aspects. Among them, the most contested are the lack of transparency, difficulties for individuals that reject technology, security vulnerabilities to cybernetic attacks. In other

DOI: 10.12948/issn14531305/20.3.2016.06

words, a high performance e-voting system must implement good solutions for these problems. One of the most popular solutions for security in electronic voting is the use of cryptographic schemes.

Thus, cryptographic design of voting systems started in the '80s and proved to be very difficult due to the numerous and varied characteristics that must be taken into consideration. Most electronic voting schemes fall into three classes: first class comprises protocols based on asymmetrical cryptography, the second class is based on homomorphic cryptography and the last class combines both.

All protocols have a common structure, comprising two components: an entity verification component that guarantees the eligibility of the voter and uniqueness of votes and a component responsible for cryptographic operations performed on casted votes, thus guaranteeing the security of the process. The difference between these protocols is given by the way first component is implemented. For the second component asymmetrical cryptography and digital signatures are used for authentication and uniqueness, especially because electronic voting sessions must be irrevocable and irreversible to ensure system auditing.

From an architectural point of view, an electronic voting system consists of three main modules, according to the general electronic voting algorithm (see Figure 4): initialization module, voting module, vote counting module. Each of these modules corresponds to a stage of the electronic voting process and involves implementation of specific cryptographic schemes, partially exemplified in Table 2.

Table 2. Characteristics of cryptographic schemes for various stages of e-voting process

Stage of electronic voting process	**Specific cryptographic scheme**	**Characteristics**
Initialization	Randomized Authentication Token	This is a solution for random generation of a token that the voter may use to authenticate as eligible voter, while remaining anonymous (the system cannot find the identity of the person)
Voting	Blind signatures	Based on RSA algorithm, the concept was introduced by David Chaum in 1982 and represents a method of digital authentication of a message without knowing the content of the message. Electronic voting using blind/blank signature is similar to traditional voting on a piece of paper sealed in an envelope. Later, the validator signs the envelope without knowing its content.
	Separation of Duty	The scheme works with at least two voting servers, one to verify the voting rights and one to store the votes. The voter is authenticated by the first server and if he has the voting right receives a number randomly generated by the server, which is later sent to the second server without any information regarding the voter identity. The voter uses this number to authenticate as eligible voter on the second server and cast his vote.
	Benaloh's Model	This model was proposed by Josh Benaloh in 1987 and is based on a homomorphic scheme: each voter sends his vote to a number of authorities. The vote is encrypted with a public key of the authority, authenticated and saved. At the end of the voting process, each authority counts the received votes and calculates a portion of the

DOI: 10.12948/issn14531305/20.3.2016.06

Stage of electronic voting process	Specific cryptographic scheme	Characteristics
		election results. All the results are then combined to find the general result (that are universally verifiable). These schemes have a simple structure, but they have a high cost because each voter must distribute his vote through a number of channels. [12]
Counting	Homomorphic encryption	This scheme was proposed by Ronald Cramer in 1997 and uses the characteristics of homomorphic encryption algorithms to ensure verifiability of elections on large scale, while maintaining discretion. Homomorphic encryption is a special kind of encryption that implements the following feature: the sum of two encrypted numbers is the same as the encryption of the sum of those two numbers. This is very important in counting the votes. Instead of hiding the voter identity, this scheme hides the content of the vote. The ballot is attached to the digital identity of the voter, this achieving the verifiability condition. When counting the votes, each vote should be decrypted to find the voter's choice. This is actually is avoided in homomorphic cryptography because increasing the number of encrypted ballots leads to a result corresponding to the encrypted final result of the election. [12]

Thus, in homomorphic encryption, each voter encrypts his vote with the public key of an authority and publishes the cryptogram along with a proof that the ballot is valid. At the end of the voting process the authorities multiply the received encryptions to find the encrypted final result. Later, the authorities decrypt this final result to find the scores. The result can be verified by all parties, thus ensuring the verifiability property. For the robustness property, the encryption procedure is distributed among *n* authorities, using a cryptographic threshold. [12]

With all these considerations, ensuring the security of the electronic voting is hard to achieve in e-voting solutions. Certainly, the near future will bring a solution for this weakness and we will see a successful implementation of e-voting systems in Europe and worldwide.

7 Conclusions

The new opportunities for electronic voting in the context of digital democracy have generated solutions and standards. The interest for this direction has increased significantly, on global level various schemes and protocols of implementation being experimented. Thus, the electronic voting process has been intensively studied in the last twenty years, multiple solutions being proposed, each with a plus on security and efficiency. Still, no complete and practical solution for a large scale voting through internet has been found. Also, approaches and conclusions were different, countries like France, Estonia, Austria etc. have completely or partially renounced on the old systems, while others preferred to continue using them. It is obvious that no matter what implementation method is chosen, security plays a crucial role in the context of electronic voting, attention being focused on the technologies and methods to be applied.

The success of electronic voting depends on the ability to solve aspects regarding trust, expressed as security problems derived from political and sociological points of view, as

DOI: 10.12948/issn14531305/20.3.2016.06

well as trust in the technology employed. Under these conditions, ensuring integrity, confidentiality, authenticity and non-repudiation of data through cryptographic solutions may offer an opportunity to generate trust in the involved parties. The implementation of an electronic voting system may be very difficult and expensive, but once it is done, it will bring numerous social and political benefits. Also, e-voting may be a factor in improving active participation of citizens to events that require making a decision based on votes.

References

[1] D. Jefferson, A.D. Rubin, B. Simon, D. Wagner (2004, January 5). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Available: http://euro.ecom.cmu.edu/program/courses/tcr17-803/MinorityPaper.pdf

[2] D.P. Moynihan, „Building Secure Elections: E-Voting, Security, and Systems Theory", Public Administration Review, volume 64, issue 5, pp. 515-528, September 2004

[3] R. Lindner, G. Aichholzer, L. Hennen (Editors) (April 7, 2016), Electronic Democracy in Europe: Prospects and Challenges of E-Publics, E-Participation and E-Voting [On-line], Springer International Publishing Switzerland 2016, ISBN 978-3-319-27419-5 (eBook). Available: https://books.google.ro/books?id=HGmwCwAAQBAJ&dq=IPOL-JOIN_ET(2011)471584_EN&hl=ro&source=gbs_navlinks_s [April 14, 2016]

[4] Estonian National Electoral Committee. Internet Voting in Estonia, http://www.vvk.ee/voting-methods-in-estonia/ [April, 2016]

[5] Australian Electoral Commission, Events in Australian electoral history, http://www.aec.gov.au/elections/australian_electoral_history/reform.htm [April, 2016]

[6] D.W. Jones, Voting and Elections (2001-2005), http://homepage.cs.uiowa.edu/~jones/voting/ [April, 2016]

[7] C. Uscatu, "Electronic Universal Voting", Informatica Economică Journal, no. 4 (48)/2008, pp. 130-135

[8] DRE voting machine, https://en.wikipedia.org/wiki/DRE_voting_machine [April, 2016]

[9] H.C. Matei, S. Neguț, I. Nicolae, Enciclopedia statelor lumii, 11th edition, Ed. Meronia, București 2008, ISBN 978-973-7839-38-1

[10] OASIS, https://www.oasis-open.org/org [April, 2016]

[11] A. Al-Ameen and S. Talab, "The Technical Feasibility and Security of E-Voting", The International Arab Journal of Information Technology, Vol. 10, No. 4, July 2013, pp. 397-404

[12] M. Burnester and E. Magkos, "Towards Secure and Practical E-Elections in the New Era", in Secure Electronic Voting (Dimitris Gritzalis Ed.), Springer International Publishing Switzerland 2003, ISBN 978-1-4613-4981-5 (eBook). Available: http://link.springer.com/chapter/10.1007%2F978-1-4615-0239-5_5

Marian STOICA received his degree on Informatics in Economy from the Bucharest University of Economic Studies in 1997 and his doctoral degree in economics in 2002. Since 1998 he is teaching in Bucharest University of Economic Studies, at Informatics and Cybernetics Economy Department. His research activity, started in 1996 and includes many themes, focused on management information systems, computer programming and information society. The main domains of research activity are Information Society, E-Activities, Tele-Working, and Computer Science. The finality of research activity still today is represented by over 80 articles published, 25 books and over 40 scientific papers presented at

DOI: 10.12948/issn14531305/20.3.2016.06

national and international conferences. Since 1998, he is member of the research teams in over 30 research contracts with Romanian National Education Ministry and project manager in 5 national research projects.

Bogdan GHILIC-MICU received his degree on Informatics in Economy from the Academy of Economic Studies Bucharest in 1984 and his doctoral degree in economics in 1996. Between 1984 and 1990 he worked in Computer Technology Institute from Bucharest as a researcher. Since 1990 he teaches in Academy of Economic Studies from Bucharest, at Informatics in Economy Department. His research activity, started in 1984 includes many themes, like computers programming, software integration and hardware testing. The main domain of his last research activity is the new economy – digital economy in information and knowledge society. Since 1998 he managed over 25 research projects like System methodology of distance learning and permanent education, The change and modernize of the economy and society in Romania, E-Romania – an information society for all, Social and environmental impact of new forms of work and activities in information society.

DOI: 10.12948/issn14531305/20.3.2016.06