

# On the Development of Electronic Voting: A Survey

Mona F.M.Mursi  
Professor  
Faculty of Engineering,  
Shoubra, Benha  
University, Egypt

Ghazy M.R.Assassa  
Professor  
Faculty of Engineering,  
Shoubra, Benha University,  
Egypt

Ahmed Abdelhafez  
Communication Dept.,  
Military Technical College,  
Egypt

Kareem M. Abo  
Samra  
Lecturer Assistant,  
Faculty of Engineering,  
Higher Technological  
Institute, Egypt

## ABSTRACT

Voting is a fundamental decision making instrument in any consensus-based society and democracy depends on the proper administration of popular elections. In any election, there exists a set of requirements among which voters should receive assurance that their intent was correctly captured and that all eligible votes were correctly tallied. On the other hand, the election system as a whole should ensure that voter coercion is unlikely. These conflicting requirements present a significant challenge: how can voters receive enough assurance to trust the election result, but not so much that they can prove to a potential coercer how they voted.

The challenge of changing the traditional paper based voting methods used in many developing countries into electronic voting raises a set of functional and constitutional requirements. These requirements are governed by the country in which they operate and are usually not limited to privacy, authentication, fairness, transparency, integrity and incoercibility. This paper presents a survey of electronic voting schemes and systems available to date, classifying them and pointing out advantages and drawbacks of each class. The survey is concluded by presenting a comparative analysis on electronic voting and suggests improvements on some recent e-voting schemes and systems.

## Keywords

Electronic voting, Cryptography, Remote voting, Verifiability

## 1. INTRODUCTION

During the past decade, many governments have begun to introduce modern technology into their voting procedures. Electronic voting (e-voting) is one of the most significant parts of e-democracy, which refers to the use of computers or computerized voting equipment to cast votes in an election. E-voting aims at increasing speed, reducing cost and improving the accuracy of the results rather than classic paper based voting. An electronic voting system creates and manages data securely and secretly, so it must meet security requirements such as confidentiality, integrity, fairness, privacy and verifiability. There are a number of voting systems adopted all over the world with each of them having its particular advantages and problems. The traditional elections methods are no longer preferred due to the long period of preparation, fake voting, faulty voting, mistakes made during vote count, long period of counting and high cost of voting process. In contradiction with this, the manual voting systems still appears prominent among the developed and developing nations [1]. Moreover, in some countries, deliberately introduced manipulations of the votes take place to distort the results of an election in favor of certain candidates.

The Organization for the Advancement of Structured Information Standards (OASIS) [2] described a conceptual perspective of e-voting to be made of three phases namely pre-voting phase, voting phase and post-voting phase. The OASIS specified what they called an Election Markup Language (EML) which was designed especially for the exchange of data within e-voting processes.

E-voting is an interdisciplinary subject and should be studied together with the experts in different domains, such as software engineering, cryptography, politics, law, economics and social science. Nevertheless, many people from different backgrounds have worked on this subject, mostly e-voting is known as a challenging topic in cryptography because of the need to achieve voter anonymity and therefore, to ensure his/her privacy [3].

Although some progress has been made in understanding and supporting the better development of e-voting systems, there is no classification to understand the common characteristics, objectives, and limitations of these approaches. Thus the lack of a comparative study provides little or no direction on choosing the appropriate development techniques for particular needs [4].

This Paper is organized as follows; Section 2 reviews the evolution of election technology. Section 3 gives an overview of the security requirements of electronic voting systems. Section 4 discusses the cryptographic security mechanisms of e-voting schemes. Section 5 classifies the various e-voting schemes. Section 6 compares between the classes pointing out the advantages and disadvantages. Section 7 discusses the vulnerabilities of e-voting systems. Section 8 presents a comparative analysis and suggests improvements on some recent e-voting schemes and systems. Finally, section 9 concludes our work.

## 2. THE EVOLUTION OF ELECTION TECHNOLOGY

### 2.1 Definitions

An *election* is a process to obtain accurate data representing a set of participants' answers to a posed question. A *vote* is what physically represents a participant's answer to a particular question. A vote consists of a selection, generally from a predetermined set of answers, called *candidates*. Sometimes a vote contains a selection which is not an element of the predetermined list, and is called a *write-in vote*. One or more votes are combined into a structure called a *ballot*. Each question in an election is called a *race*, and therefore each race has a set of candidates, potentially receiving votes from voters.

An *authority* is an entity, responsible for conducting the election. An *adversary* is a malicious entity, which attempts to manipulate the voting and/or tallying. An external adversary

may actively try to coerce a voter or buy a voter, and may passively try to breach the privacy of voters. An internal adversary, apart from breaching privacy, may try to modify or reveal the partial tally as well as corrupt the authority.

A *voting scheme* is a protocol which has a means of receiving votes as input, and produces an output which is the sum of the votes cast for each candidate. Therefore, it is a method for conducting an election and the sum may result in a decision. A voting scheme can refer to any method that can successfully manage an election. The voting schemes that have been used historically are called traditional voting schemes such as the voting scheme which uses levers and ordinary paper ballots. In contrast, an *electronic voting scheme*, or *e-voting scheme* is one that makes use of electronic devices to conduct an election.

## 2.2 Computerized Voting Systems

Paper-based voting is the dominant type of voting where votes are cast and counted by hand, using paper ballots. It has been replaced in many countries by computerized voting systems. A chart of the computerized voting systems is shown in Fig 1.

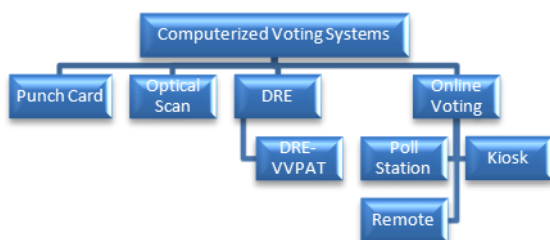


Fig 1: Computerized voting systems

The first type of computerized voting systems is the punch card system. The voter uses a card punch device to indicate their votes on a punch card. Votes are tabulated by passing them through a punch card reader.

A second type of vote-counting systems uses optical scanners. Voters indicate their preferences on a paper ballot by filling in bubbles next to candidates' names with a pencil. The ballots are read by optical scanning devices.

### 2.2.1 DRE

The newest type of vote-counting systems is the touch screen system, which are referred to as Direct Recording Electronic Systems (DRE). DRE is considered the first full computer based system [5]. A DRE machine implements all steps in the voting process, from registration and ballot casting to counting. DRE systems consist of buttons and areas on the touch screen. A voter gets a PIN or smart card by showing their ID to the election officer. They enter the PIN or smart card into the DRE. The voter makes his/her choices, the DRE machine shows the choices on the screen and finally gives the voter an opportunity to change his/her choice or submit the choices. Votes are recorded directly in the computer's memory, rather than on a paper or punch card ballot, which makes DREs the only example of completely electronic voting machines. There are other types of DRE equipped with printed audit trails which is often called Direct Recording Electronic System- Voter Verified Paper Audit Trail (DRE-VVPAT). That is, a touch screen based machine that produces a printout of each vote, verified directly by the voter, to maintain physical and verifiable record of the votes cast [4].

### 2.2.2 On-line voting

In order to improve convenience and increase voter turnout, the idea of online voting arises. This type of e-voting involves the use of a computer and the Internet or a private network in support of the voting process. On-line voting can be conducted

in a variety of ways, namely Poll station, Kiosk and Remote e-voting.

*Poll station electronic voting* systems require voters to go to staffed polling sites and cast their votes from electronic voting machines at physical, central locations. The votes are tallied locally or sent remotely for tally. A network, either the Internet or a private network, may be used to transfer ballots from each polling place to a centralized site, where votes are tallied.

*Kiosk e-voting* systems allow voters to vote from computers/ATM-like machines situated within kiosks. The kiosks are setup by the voting authority in suitable locations such as post offices or shopping malls and connected to a central location via the Internet or a private network. A vote cast at the kiosk will immediately be forwarded across the network to the centralized tallying site. The kiosks are not monitored by poll workers at all times and may allow voting over a period of several days or weeks.

*Remote e-voting* (Internet voting) systems allow voters to cast their votes remotely from any computer or digital device connected to a public network such as the Internet; typically from home or at work. Devices such as personal digital assistants and mobile phones may access these systems.

Recent studies on using computer technologies in support of political remote e-voting systems have been proposed. Unfortunately, remote e-voting from home or at work is inherently coercible as there is no guaranteed privacy during ballot casting [6-8]. Estonia was the first country in the world to introduce Internet Voting in binding elections in 2005 [9]. Remote Internet voting systems still suffer from many security problems which rely on the clients, the servers, and the network connections. Denial-of-service (DOS) attacks and viruses still belong to the most challenging security issues.

### 2.2.3 Biometric tokens

Since security of most of the systems are provided by passwords, PINs and ID cards [10-12], some have adopted the idea of using biometric tokens as voter's secure credentials in the registration and authentication stages for increased security. Biometric identifiers cannot be easily misplaced, forged, or shared, thus they are considered more reliable for personal recognition than traditional token or knowledge based methods. Biometric authentication or verification systems authenticate the person's identity by comparing his own biometric template(s) stored in database (one-to-one comparison), while biometric identification systems recognize an individual by searching the entire templates in a database for match (one-to-many comparison) [13]. Biometric solutions are generally client/server solutions, giving systems administrators the ability to audit usage, manage security levels, and remove unauthorized users.

## 2.3 Voting Styles

In an election, the voting style mandates the number of candidate selections that constitute a vote. There are numerous different types of voting styles:

- 1-out-of-2 voting (yes/no voting): Voter's answer is a "yes" or "no". Vote is a one bit: 1 for "yes" and 0 for "no".
- 1-out-of-L voting: Voter has L possibilities and he chooses one of them.
- K-out-of-L voting: Voter selects K different elements from a set of L possibilities. The order of the selected elements is not important.
- K-out-of-L ordered voting: Voter puts into order K different elements from a set of L possibilities.
- Write-in voting: Voter formulates his own answer and writes it down. Vote is a string of letters with specified

maximum length, representing the name of an individual, for example.

There is a pressing need for an analysis of the security of e-voting protocols. A first step towards the security analysis of e-voting protocols consists in precisely defining security with respect to e-voting. Formal definitions have been proposed for several key properties such as privacy, receipt-freeness, coercion resistance, or verifiability [14]. The next section presents an extended list of definitions for the e-voting security requirements.

### 3. VOTING SYSTEMS SECURITY REQUIREMENTS

There are many challenges that face e-voting systems that are raised by the functional and constitutional requirements that are governed by the country in which they operate. Electronic voting systems have to respect the constitutional election principles. For technological solutions, this translates into security requirements that have to be fulfilled by the operational environment in which the voting takes place. For any voting system, some requirements are critical such as authentication, uniqueness, privacy, reliability, verifiability and accuracy. Other requirements are desirable such as convenience, transparency, scalability and cost effectiveness.

Many researchers have described the security requirements for voting systems [15-25], these requirements are presented by their formal definitions as follows.

- a) *Eligibility*: Only valid voters who meet certain pre-determined criterion are eligible to vote.
- b) *Authentication*: Only voters who obtained authorization should be able to vote.
- c) *Uniqueness/Non reusable*: No voter should be able to vote more than once. No-one can change or duplicate someone else's vote.
- d) *Privacy*: No one should be able to determine how any individual voted.
- e) *Convenience*: Voters should be able to cast votes with minimal equipment and skills. Convenience must eliminate all physical restrictions, and decrease users having to learn too complex techniques.
- f) *Transparency*: Voters should be able to possess a general understanding of the whole process.
- g) *Walk away*: after voting, the voter is not involved in any other post vote process.
- h) *Dispute Freeness*: Any voting scheme must provide a mechanism to resolve all disputes in any stage.
- i) *Practicality*: A voting scheme should not have assumptions and requirements that may be difficult to implement on a large scale.
- j) *Fairness*: Ensures that no one can learn the outcome of the election before the official announcement of the tally.
- k) *Incoercibility*: A voting scheme should be coercion resistant. Coercion happens when an entity tries to manipulate the manner in which a vote is cast or force a voter to abstain, or may even represent a valid voter by obtaining the voter's credentials.
- l) *Accuracy/completeness*: Voting systems should record the votes correctly.
- m) *Soundness*: No reasonably sized coalition of voters or authorities may disrupt the election.
- n) *Verifiability*: Voters shall be able to verify that their votes are correctly counted for in the final tally (universal or individual).
- o) *Integrity*: Votes should not be able to be modified without detection.
- p) *Reliability*: The system must be resistant to randomly generated malfunctions.
- q) *Robustness*: The voting system should be successful regardless of partial failure of the system.
- r) *Flexibility*: Equipment should allow for a variety of ballot formats so it can be used for several types of elections.
- s) *Auditability*: There should be a reliable and authentic election records.
- t) *Certifiability/Function Check*: Systems should be testable against essential criteria.
- u) *Cost effectiveness*: Systems should be affordable.
- v) *Voter Mobility*: There should be no restrictions on the location from which a voter can cast a vote.
- w) *Receipt Freeness*: A voter should not be provided with a receipt that proves how he/she voted to any other entity.
- x) *Verifiable Participation*: Ensures that it is possible to find out whether a particular voter has participated in the election by casting a ballot or not.
- y) *Efficiency*: Efficiency focuses on avoiding too many steps to reach voting efficiency for voters. The definition of efficiency is that the whole election can be held in a timely manner, for instance, all computations are done in a reasonable amount of time and voters are not required to wait for other voters to complete the process.
- z) *Scalability*: The complexity of the protocols used in a voting scheme, is a major factor in its practical implementation. An efficient voting scheme has to be scalable with respect to storage, computation, and communication needs to accommodate larger number of voters.

There are some conflicts between the requirements by definition. An example of conflicts is Authentication vs. Privacy; to identify and check the credentials of a voter, while at the same time protect the privacy of his/her vote. Another example is Verifiability vs. Receipt Freeness; to enable the voter to verify that his vote is correctly counted for and is cast correctly without giving him a receipt of correct vote cast.

Given the short history of e-voting systems across the world and the inherent limitations in the scope of implementation, it is very difficult to measure the success or failure of any or all of the issues mentioned above. In addition, any voting process, as mentioned earlier, is bound by regulations and cultural values that characterize the different societies involved. Hence, the example of one country may not directly suite the example of another [26].

### 4. CRYPTOGRAPHIC SECURITY MECHANISMS

Cryptography is the key technology to secure electronic data flows. It offers advanced cryptographic techniques that can be combined to design secure voting protocols. For over two decades cryptographic research has been done on this topic, in 1981 Chaum [27] proposed the first such cryptographic election protocol. His work initiated a vast amount of research on several approaches to realize secure solutions for electronic elections. The efficiency and practical applicability of all these approaches has experienced a strong increase in the last years. Provided hereafter is a brief description of the cryptographic mechanisms and modules that constitute the protocols of a voting scheme.

#### 4.1 Mixnet

Mixnet is a technique to create anonymous channels as suggested by D. Chaum [23], a multistage system consisting of cryptography, shuffling and permutations. The function of mixnet is to randomize a sequence of mutated messages such

that the inputs and outputs are unlinkable. Mix-nets in online elections aim at hiding the origin of a ballot so that the link between the identity of the voter and the vote is broken. Messages are mutated either by encrypting & decrypting, or re-encrypting them. The first mix-nets were decryption mix-nets where messages are wrapped in several layers of encryption and then routed through mix servers each of which remove the outer layer of encryption and then forward them in random order to the next one until all layers are removed. “Onion routing” is an implementation of decryption mix-nets.

Most re-encryption mix-nets use randomized public-key encryption schemes such as ElGamal [28] or Paillier [29] cryptosystems, where the size of the cipher texts can be independent of the number of the involved mix servers, and the list of encrypted votes is sequentially re-encrypted and shuffled in each mix server [30]. Mixnet was proposed for e-voting in [31]. Shuffle decryption is considered as more efficient than re-encryption shuffles [3]. A disadvantage of mix-nets is that in their fully robust form they may need complex protocols for generating and maintaining shared private keys, as well as for mixing and proving correctness of the shuffles.

## 4.2 Bulletin Board

Cryptographic voting protocols revolve around a central, digital bulletin board. As its name implies, the bulletin board is public and visible to all, via, for example, phone and web interfaces. It is a public broadcast communication channel that has memory and any information that is broadcast will be stored in memory and readable by anyone [32]. The bulletin board may contain designated, authenticated sections for each eligible voter. An authenticated voter has write-only (append) access to his designated section. The authority also uses the bulletin board to post information. All messages posted to the bulletin board are authenticated, and it is assumed that any data written to the bulletin board cannot be erased or tampered with.

## 4.3 Blind signature

It is a cryptographic protocol that can be used to authenticate a voter without disclosing the content of his ballot. Blind signatures are the electronic equivalent of signing carbon-paper-lined envelopes. Writing a signature on the envelope leaves a carbon copy of the signature on a slip of paper within the envelope. When the envelope is opened, the slip will show the carbon image of the signature. The Blind Signature protocol can be described as follows:

Step 1. a voter V blinds his vote  $v$  using a random string  $r$ , and the public key  $K_A$  of authority A as,  $BV = \text{blind}(v, r, K_A)$ , then signs BV using his private key  $K_V^{-1}$  as,  $\text{Sign}_V(BV, K_V^{-1})$  and sends it to authority A.

Step 2. A verifies the validity of V (by verifying the signature with V's public key  $K_V$ ), then signs BV with his private key  $K_A^{-1}$  as,  $\text{sign}_A(BV, K_A^{-1})$ , and sends it to V.

Step 3. V verifies signature of A and then unblinds (removes  $r$ ) to obtain  $\text{sign}_A(v, K_A^{-1})$  which is the blindly signed vote  $v$ . Such a protocol was proposed in [33] using RSA cryptosystem [34].

## 4.4 Homomorphic encryption

An encryption algorithm  $E_K$  is said to be Homomorphic for a message  $m$  if given  $E_K(m_1)$  and  $E_K(m_2)$  one can obtain  $E_K(m_1 \odot m_2)$  without decrypting  $m_1$  and  $m_2$  individually, for some operation  $\odot$  which can be modular addition or multiplication. If each voter is only able to vote “no” or “yes”, then by multiplying the encrypted ballots one can receive a product which is equal to the encryption of the sum of the ballots:

$$E(x) \otimes E(y) = E(x \oplus y) \Rightarrow \prod_i^n E(b_i) = E(\sum_i^n b_i) \quad (1)$$

The homomorphic property allows the encrypted votes for each candidate to be summed into a single total without being decrypted [35]. The model is based on the algebraic homomorphic properties of several probabilistic public key cryptosystems. RSA public key cryptosystem [34] possesses multiplicative homomorphism, while ElGamal [28] and Paillier [29] cryptosystems possess additive homomorphism.

## 4.5 Zero knowledge proof

A voter may be required to prove validity of vote, and/or an authority may need to prove validity of a cryptographic operation. Interactive proof is a cryptographic protocol implemented by an entity P (prover) to prove knowledge of a secret to an entity V (verifier) [36]. If such a proof does not leak the secret then it has zero-knowledge property [37]. This proof is applied to homomorphic voting due to the nature of the encrypted vote which requires proof of validity without decrypting the vote. This is an unattractive feature as voters may need to run special-purpose code on their computer, for constructing the zero-knowledge proof of validity for their vote.

## 4.6 Secret sharing


















A single authority trusted to conduct the election can become corrupted or faulty. Robustness can be addressed by distributing trust over multiple authorities. It then becomes necessary to also share secrets (such as a decryption key) between them. A  $(K, n)$  threshold secret sharing scheme [38], where  $k \leq n$  can be used to share a secret  $S$  between  $k$  authorities. The scheme requires a trusted party T that constructs the secret key  $S = K^{-1}$ , publishes the public key  $K$ , and generates  $k$  shares of the secret key. To reconstruct the secret key,  $k$  or more honest authorities have to submit their shares which are then combined. The secret key is computationally protected up to a collusion of  $k-1$  corrupt authorities and  $n-k$  faulty authorities.

## 4.7 Visual cryptography

Visual cryptography is a method to conceal images without cryptographic computations [39, 40]. Visual cryptography exploits the physical properties of transparencies to allow humans to compute the XOR of two quantities without relying on untrusted software. The cryptosystem works by encoding a plain text message into a cipher text printed on two transparencies that encode the key. The message is visually observed when the two transparencies are aligned, even though individually they are indistinguishable from a random dot image. Visual cryptography is especially useful for the low computation load requirement.

Cham [41] adapted the concept by introducing each transparency as a uniform grid of pixels. Pixels are square and take the values of  $\{0, 1\}$ . A pixel is printed  $\blacksquare$  for a 0-valued pixel and  $\blacksquare$  for a 1-valued pixel. Each of the four smaller squares within a pixel is referred to as sub-pixel. Overlaying two transparencies allows light to shine through only in locations where both sub-pixels are clear, and the above encoding exploits this so that overlaying performs a sort of XOR operation. Pixels in the overlay take values in  $\{0', 1'\}$ . Using  $\square_v$  to represent the visual overlay operation, pixels are encoded according to Table I:

TABLE I  
VISUAL CRYPTOGRAPHY TRUTH TABLE

Encoding for transparency	1:  0: 
Encoding for overlay	1':  0':  or 
$\oplus_v$ Truth table	$0 \oplus_v 1 = 1'$   = 
	$0 \oplus_v 0 = 0'$   = 
	$1 \oplus_v 1 = 0'$   = 
	$1 \oplus_v 0 = 1'$   = 

## 5. CLASSIFICATION OF E-VOTING SCHEMES

In a secret voting scheme, voters need to privately communicate their votes towards the final tally. The tallying authority is responsible for receiving the votes and conducting the tallying stage. Based on how voters submit votes to this tallying authority, voting schemes can be classified into 3 broad classes [19]: *Hidden voter* where the voters anonymously submit votes, *Hidden vote* where the voters openly submit encrypted votes and *Hidden voter with hidden vote (HVHV)* where the voters anonymously submit encrypted votes. A review of each class is presented pointing out some existing schemes. A chart of e-voting classes and subclasses is shown in Fig 2.

### 5.1 Hidden Voter

The voter remains anonymous while sending vote without encryption to the tallying authority through an anonymous channel. To ensure that the hidden voter is valid, there has to be some form of identification that is associated with the vote, representing a proof of the voter's validity. Hidden Voter class is subdivided into two subclasses, namely: token based and bulletin board based.

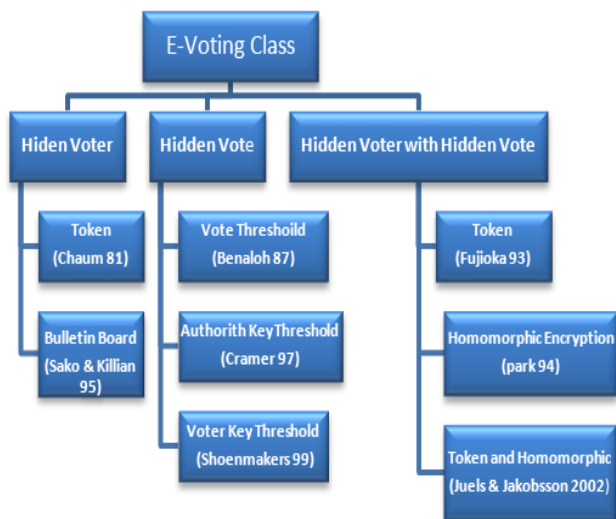


Fig 2: The e-voting classes and subclasses

#### 5.1.1 Hidden Voter - Token based

The identification quantity called token, is obtained by the voter from the authority during the registration stage of the voting scheme. A token must be difficult to forge, and easily verified. It must be valid only for specific election. In order to ensure voter anonymity, the token has to be random and

unlinkable to the voter. During voting stage, voter sends token/vote over the anonymous channel to the tallying authority. A hidden voter Token Based scheme appeared in [27] and subsequently improved in [42, 43].

#### 5.1.2 Hidden Voter - Bulletin Board based

Voter submits encrypted vote  $E_K(v,r)$  to its authenticated section in the bulletin board. After all votes have been cast, the decryption mixnet is used to open and submit votes in random order, to tallying authority. Any observer can compute the tally sum. Tokens are not needed here since only eligible voters get access to the bulletin board. A hidden voter Bulletin Board based scheme was firstly proposed in [44].

### 5.2 Hidden Vote

Voter submits encrypted vote  $E_K(v,r)$  and a proof<sub>v</sub> of validity (Zero Knowledge Proof), to its authenticated section in the bulletin board. After voting stage, the tallying authority checks validity of proof<sub>v</sub>, collects all valid encrypted votes  $\{E_K(v)\}$  and computes  $E_K(\text{sum}(v))$  "Homomorphic". Tallying authority then posts final tally,  $\text{sum}(v)$ , and proof<sub>A</sub> of correct decryption on bulletin board. Hidden Vote requires no anonymous channel. Validity of votes has to be ensured before combining them. The Tally is obtained by decrypting the sum. Hidden vote class is subdivided into 3 subclasses namely: vote threshold, authority key threshold and voter key threshold.

#### 5.2.1 Hidden Vote - Vote Threshold

The vote is segmented into  $k$  shares by the voter using  $(t, k)$  verifiable secret sharing scheme [45]. Each of the  $k$  authorities receives one encrypted share (encrypted with that authority's public key). Each authority then uses Homomorphic property of its public key cryptosystem and multiplies all the shares it received from voters to get the encrypted partial sum. Each authority then decrypts its partial sum and finally the authorities add their partial sums to get the final tally of votes. A Hidden Vote - Vote threshold Schemes appeared in [46-48] and subsequently improved in [49-51].

#### 5.2.2 Hidden Vote - Authority Key Threshold

Here the voter encrypts the vote with public key  $K$  of a tallying authority. There are multiple authorities sharing the private (decryption) key among themselves using  $(t, k)$  verifiable secret sharing scheme. The scheme was proposed in [32] and later improved in [52-55].

#### 5.2.3 Hidden Vote - Voter Key Threshold

Voter key threshold schemes achieve dispute-freeness property. The voters act as the authorities, and participate to jointly share/generate their private keys, which are then used to encrypt their votes. The tally is computable as long as a threshold number of voters participate in voting and tallying. These schemes are suitable for small scale elections. A Hidden Vote - Voter Key threshold Scheme was proposed in [56] and improved in [57].

### 5.3 Hidden Voter with Hidden Vote (HVHV)

In HVHV, the voter uses the anonymous channel to send an encrypted vote to the tallying authority. HVHV class of schemes is a hybrid of the two previous classes. Hidden voter with hidden vote class is subdivided into 3 subclasses namely: token based, homomorphic encryption based and token and homomorphic based.

#### 5.3.1 HVHV - Token based

It is derived from the hidden voter class. During registration, the voter obtains a blind signature on an encryption of His/Her vote from a registration authority. The voter sends the signed hidden vote anonymously to a tallying authority. A HVHV - Token based scheme was proposed in [58] and improved in [59-61].



### 5.3.2 HVHV - Homomorphic encryption based

HVHV - Token based could not satisfy accuracy as well as universal verifiability. Hence a second category of HVHV schemes, based on homomorphic encryption technique was proposed. The scheme appeared in [31] and improved in [62-67].

### 5.3.3 HVHV - Token and Homomorphic based

This category of HVHV schemes, try to satisfy receipt-freeness and Incoercibility properties. During registration stage, the voter obtains a unique token encrypted with a public key that is shared by k authorities. The public key encryption used is homomorphic. Voter sends encrypted vote combined with the encrypted token, over an anonymous broadcast channel to a bulletin board with no designated sections. It was proposed in [68, 69] and improved in [70].

## 6. COMPARISON BETWEEN THE CLASSES

A comparison is presented between the previously mentioned classes pointing out the advantages and disadvantages of each class. Table 2 shows the classes and their respective fulfillment to some important security requirements.

TABLE II.

COMPARISON BETWEEN THE CLASSES

Class	Subclass	Eligibility	Privacy	Verifiable	Accuracy	Fair	Receipt free	Incoercible	Scalable
Hidden Voter	Token	✓	Com/Max	Ind	x	x	x	x	x
	Bulletin Board	✓	Com	✓	✓	C	✓	x	✓
Hidden Vote	Vote Threshold	✓	Com	✓	✓	C	x	x	x
	Authority Key Threshold	✓	Com	✓	✓	C	✓	x	C
	Voter Key Threshold	✓	Com/Max	✓	✓	C	x	x	x
Hidden Voter with Hidden Vote	Token	✓	Com	Ind	x	✓	x	x	x
	Homomorphic	✓	Com	✓	✓	C	✓	C	C
	Token and Homomorphic	✓	Com	✓	C	C	✓	C	C

Com: computational, Max: Maximal, Ind: Individual, C: Conditional or under assumptions

### 6.1 Hidden Voter schemes

The main advantage is that the tallying process is the simplest among all the three classes, and computation at the voter end is also simple. Accuracy, fairness and robustness cannot be satisfied together. Inaccuracies in the tally can only be resolved by another election which is not fair. The voter participation requirement can be heavy.

Anonymous channel implementation with robust, verifiable decryption mix-nets can reduce the voter participation. These channels are still hard to implement and not really efficient when used for large scale elections.

### 6.2 Hidden Vote schemes

The voter participation is minimal and universal verifiability property is easy to achieve. There is no requirement for any form of mix-nets. Small scale elections can benefit from simplicity of hidden vote schemes since they can be designed to work without any authority (voter key threshold). The main Disadvantage is that vote format is not flexible to support write-in votes. Some vote formats proposed involve complex computations for the voter and at times for tallying. Complexity

for simple 1-of-2 candidates' election can be relatively efficient compared to HVHV approaches.

### 6.3 Hidden Voter with Hidden Vote

The main advantage is the flexibility of the vote format (including write-in) and relatively low voter computation (no complex proofs are usually necessary), which are desirable properties for large scale elections. Anonymous channel implementation is an issue in HVHV schemes as in hidden voter schemes. Trading scalability of scheme for achieving universal verifiability and accuracy using the mixnet is a factor in deciding between hidden vote and the HVHV approach. The tallying process itself can be time consuming since it requires individual encrypted vote validation, decryption, and vote validation followed by the actual tallying. In hidden vote, the post-vote-casting process involves the verification of proofs and tallying, in HVHV the post vote- casting process involves time consuming mixing and tallying. While hidden vote class does have many desirable properties including dispute freeness, the vote format and incoercibility weaknesses limit its application to practical election.

## 7. E-VOTING SYSTEMS VULNERABILITIES

There are numerous vulnerabilities associated with the various e-voting systems [71-77]. With punch card systems, incompletely punched holes in the form of dimples or hanging chads make the card unreadable. This is known as an under-vote. Similarly, if the voter inadvertently punches too many holes for a given office, this over-vote will also make the card unreadable. By performing a manual recount, it is possible to determine the voter's intent for at least some of these uncounted ballots. However, the manual recount process can be difficult and contentious.

For optical scan systems, an under-vote may be caused when the voter's marks are illegible and an over-vote may be caused when the voter makes too many marks or if the paper gets smudged in the wrong place. The percentage of under-votes and over-votes, which is known as the error rate, can be high.

The high-rate of under-votes and over-votes in paper-based systems is one of the main reasons behind the great interest in DREs. By eliminating the need for the voter to mark a paper or punch a card, DREs significantly reduce the error rate. However, by eliminating the voter's ability to verify the ballot, they introduce a new type of vulnerability: the inability to verify that one's vote has been correctly recorded. This vulnerability is leading a growing number of voters to lose faith in the efficiency of voting.

Given that voters cannot themselves verify that DREs correctly record their votes, another way to maintain faith in these systems would be if some trusted authority could assure voters that their votes were counted. However, this is problematic too because putting trust in a single authority is risky in fear that it might be corrupted.

Current electronic voting systems are not sufficient to satisfy trustworthy elections as they do not provide any proofs or confirming evidences of their honesty. This lack of trustworthiness is the main reason why e-voting is not widely spread even though e-voting is expected to be more efficient than the current plain paper voting. Many experts believe that the only way to assure voters that their intended votes are casted is to use paper receipts [78]. If the paper receipt is in plain text or barcoded, this gives a high rate of bribe and coercion. By using visual cryptography, the chance of bribe and coercion decreases since the voter cannot prove to a potential coercer how he voted.

Internet-based voting systems are vulnerable to attack at three major points [79]; the server, the client, and the communications infrastructure. Penetration attacks target the client or server directly whereas denial of service attacks target and interrupt the communications link between the two. Penetration attacks involve the use of a delivery mechanism to transport a malicious payload to the target host in the form of a Trojan horse or remote control program. Once executed, it can spy on ballots, prevent voters from casting ballots, or, even worse, modify the ballot according to its instructions. Remote control software may compromise the secrecy and integrity of the ballot by those monitoring the host's activity.

Remote voting systems will also have to contend with an attack known as spoofing-luring unwitting voters to connect to an imposter site instead of the actual election server. While technologies such as secure socket layer (SSL) and digital certificates are capable of distinguishing legitimate servers from malicious ones, it is infeasible to assume that all voters will have these protections functioning properly on their home or work computers, and, in any event, they cannot fully defend against all such attacks. Successful spoofing can result in the undetected loss of a vote should the user send his ballot to a fake voting site. Even worse, the imposter site can act as a "man-in-the-middle" between a voter and the real site, and change the vote. In short, this type of attack poses the same risk as a Trojan horse infiltration, and is much easier to carry out.

In principle, poll site voting is much less susceptible than remote voting to the previously mentioned attacks. The software on voting machines would be controlled and supervised by elections officials, and would be configured so as to prevent communication with any Internet host except the proper election servers. However, opportunities for attack and insider fraud would still exist.

An e-voting system can be divided into three main categories namely hardware, software, and human factors. The security-relevant elements for *hardware* are the mechanical, electromechanical, and electrical parts. The security-relevant elements for *software* are the operating system, drivers, compilers, programs, databases, rules used in the program, procedures and sequences (order of voting events, voting protocol, encryption techniques). The security-relevant elements for *human factors* are usability, rules, strategies (e.g. information flow, security management), politics, and other diverse aspects such as transparency, acceptance, and trust. All parts of the system have to be considered as equally important in terms of security risks [80].

## 8. COMPARATIVE ANALYSIS OF SCHEMES

A new concept of verifiability requirement was defined as *end-to-end verifiability* which can be subdivided into cast-as-intended, recorded-as-cast and tallied-as-recorded. Recent works focused on the design of cryptographic schemes, protocols, and techniques to improve the design of e-voting machines. What is most common is that they rely on the underlying cryptographic principles to various degrees of complexity to achieve end-to-end verifiability and coercion resistance.

PunchScan [81, 82] is a cryptographic voting system that is easy to use by the voter as well as by election officials, while at the same time providing a transparent and reliable process. It also provides public verifiability, election integrity and enhanced voter privacy. Scantegrity [83-85] is a successor of PunchScan that meets industrial standard by providing end-to-end verifiability of the integrity of critical steps in the voting process and election results.

Civitas [86] have devised and implemented a refined protocol of JCJ scheme [69] in a system called Civitas. The system has achieved good scalability by partitioning the population of voters by new technical advances such as a secure distributed registration protocol and a scalable vote storage system but unfortunately the system is not really practical due to the quadratic overhead.

Prêt à Voter [87, 88] is a type of electronic voting system that uses paper based ballot forms that are converted to encrypted receipts to provide security and auditability, at the same time remains coercion resistant and easy to use. The concept of visual cryptography was elaborated into non-visual form and is now a basis for Prêt à Voter [88] and Scantegrity II [84].

The Scratch & Vote is another cryptographic voting method proposed in [88]. It provides public election auditability. The method combines a variety of existing cryptographic voting ideas such as homomorphic encryption, the cut-and-choose at the precinct approach, and so on.

In [89], the authors used a process in algebra called Calculus of Communicating Systems with cryptographic primitives to specify and analyze some properties of the e-voting system they built. They presented a small mobile implementation of an e-voting system named M-SEAS (Mobile Secure E-voting Applet System) and used formal verification technique to validate the security properties of the system.

From our point of view, the use of biometrics offers the best technique to secure the voter's identity in the registration and authentication stages. A Brief discussion was presented earlier about the idea of using biometric tokens as voter's secure credentials in various voting stages. Several researches have been proposed in this area but there are several considerations in the design and structure of these protocols and systems.

The author of [5] presented a web based e-voting system and showed how to integrate fingerprint control into the system. The system is equipped with an optical fingerprint scanner SDK (Suprema Inc®, 2010) to accept a scan, recognize the voter, and open the correct voter record in the database and verify the voter. This module uses a dynamic link library (DLL) that can be displayed in a web application. This allows the voter's biometric data to be read by a web application and sent to a web service for verification. Our note was that the voter doesn't have to claim an identity and the e-voting system takes on the burden to identify him. This will lead to an increased load on the servers when applied on a large scale. An improvement to this is to make the voter specify a district where he is registered to minimize the system load. Another note is that the author only presented the verification method using fingerprint while neglecting the whole e-voting system security issues such as vote encrypting while travelling through insecure channels such as the Internet which he built his system as the default and only communication channel.

The author of [11] presented a thorough review of the fundamentals of fingerprint authentications systems. The proposed e-voting system relies heavily on finger print scanners by specifying a scanner for each candidate and the voter chooses the candidate by thumb scanning his finger through the scanner of the candidate he wishes to choose. Our notes were that this is a high cost system when considered on a large scale, the author also claims novelty of an e-voting system while hardly considering other e-voting systems design issues other than verification.

The authors of [10] presented an approach towards a biometric e-voting system, by considering several voting phases. They demonstrated the components of the e-voting systems from e-voting servers, security mechanisms used and the system architecture from an abstract view. They discussed the security

of the biometric smart token and used the match-on-card technology for biometric template verification. Our note was that the voter's participation is heavy as the voter has to generate a unique identification number using some data stored in the voter's e-token, by encrypting the digital stamp of the election committee with the voter's biometric template and hash the result using one way hash function.

The voter is also involved in some other complex cryptographic processes to get the blind signature of the election committee and his anonymous identity. Also our note was that the voter anonymously submits an open vote without encryption which could cause a serious problem to fairness, privacy and integrity. An improvement over the system is to encrypt the voter's choices (vote ballot) with the private key of the anonymous identity that he obtained along with the voting certificate during authentication, or to encrypt the vote ballot with the public key of the election's tallying committee.

The protocols that have been proposed so far do not yet overcome all of the barriers to their use in critical elections. Although DRE machines are popular in public elections in U.S.A., the applicability and scope of the proposed schemes are very limited in these machines. The reason for this is that some cryptographic protocols have some security holes, such that sensitive information about the election can be leaked in one way or another. Therefore, their security must be analyzed by considering the system in its entirety since these protocols are only one part of a larger system composed of voting machines, software design and implementations, and complex election procedures.

The work presented in this paper is one way in which researchers can get a better understanding of the strengths and the weaknesses of existing techniques and thus lay the foundations for engineering, designing, implementing, as well as deploying a new generation of more secure and robust technologies for electronic voting.

## 9. CONCLUSIONS

A voting system is perceived as trusted if it attracts voters and if it leads to confidence regarding the integrity of the published results and the secrecy of the vote. It appears that security features are only one premise underlying a system's acceptance among the electorate. The challenge is to exploit these features at establishing the required trust among the public.

There are three gaps that must be comprehended prior to developing (security) requirements for e-voting systems. These gaps are the *technological gap* —that is, between hardware and software, the *sociotechnical gap* —that is, between social and computer policies, and the *social gap* —that is, between social policies and human behavior.

E-Voting is not like any other electronic transaction. Remote Internet voting is highly susceptible to vote fraud. Remote Internet voting may violate the right to cast a secret ballot and lead to political coercion in the workplace therefore Remote Internet voting poses a threat to personal privacy. Phishing is a problem in Internet voting since the voter may communicate with a fraud site disguised as legitimate voting authority.

Changing technology is not enough; voter education is needed. Transparency in the voting process increases voter confidence. Software used should be open to public inspection. Viruses or spyware which are targeted specifically at an upcoming online election pose a real threat to voters.

There exist a few cryptographic schemes which fulfill a wide range of e-voting requirements. Their disadvantage is "convenience", they use sophisticated cryptographic tools that make them hard to implement and require expertise in various fields.

There is a strong need for empirical research: not much experience is available concerning the practical implementation of Internet voting and its acceptance. Many problems will probably be detected in the course of pilot projects. Considering Internet elections and security a trade-off should be kept in mind; increasing security also means an increase of effort, costs, and complexity. For that reason, careful specification has to be made with respect to the level of security of each voting system.

Trust in voting technology can only be established when operating a system that complies with high security standards. On the other hand, securing a system even to the maximum imaginable extent alone will hardly increase any trust among the public. *End-to-End Verifiability* comes to light as the most important election property to provide *trustfulness* to the election results to both candidates and voters.

## 10. REFERENCES

- [1] OO Olusola, OE Olusayo. A Review of the Underlying Concepts of Electronic Voting. In Information and Knowledge Management, ISSN 2224-5758, Vol 2, No.1, 2012.
- [2] Election Markup Language (EML) Specification Version 7.0. 8 December 2011. OASIS Committee Specification01. Available online at <http://docs.oasis-open.org/election/eml/v7.0/cs01/eml-v7.0-cs01.html>
- [3] OO Okediran, EO Omidiora. A Comparative Study Of Generic Cryptographic Models For Secure Electronic Voting. In British Journal of Science, ISSN 2047-3745, Vol. 1 (2), 2011.
- [4] K Weldemariam, AVillafiorita. A Survey: Electronic Voting Development and Trends. In Proceedings of the 4th international conference on electronic voting EVOTE 2010.
- [5] AdemAlpaslan. Web based secure e-voting system with fingerprint authentication. In Scientific Research and Essays Vol. 6(12), pp. 2494-2500, 18 June, 2011.
- [6] Weinstein L. Risks of Internet voting. Communications of the ACM, Vol 43, No. 6; (2000). p. 128.
- [7] M Rubin AD. Security considerations for remote electronic voting over the internet. Communications of the ACM, Vol 45, No. 12; (2002). p. 39-44.
- [8] Tsekmezoglou E. A critical view on internet voting technology. Available online at [www.minbar.cs.dartmouth.edu/greecom/ejeta/fourth-issue/;2005](http://www.minbar.cs.dartmouth.edu/greecom/ejeta/fourth-issue/;2005).
- [9] PriitVinkel. Internet Voting in Estonia. In LNCS 7161, pp. 4–12, Springer-Verlag Berlin Heidelberg, 2012.
- [10] TahaKh. Secure Biometric E-Voting Scheme 2011. In ICICIS 2011, Part I, CCIS 134, pp. 380–388, Springer-Verlag 2011.
- [11] D. Ashok Kumar. A Novel design of Electronic Voting System Using Fingerprint. In International Journal Of Innovative Technology & Creative Engineering (Issn:2045-8711) Vol.1 No.1 January 2011.
- [12] Mohamed Aborizka. A Novel in E-voting in Egypt. In IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007.
- [13] Anil K. Jain, Arun Ross. An Introduction to Biometric Recognition. IEEE transactions on circuits and systems for video technology, vol. 14, no. 1, january 2004.



- [14] Véronique Cortier and Cyrille Wiedling. A Formal Analysis of the Norwegian E-voting Protocol. In LNCS 7215, pp. 109–128, Springer-Verlag Berlin Heidelberg, 2012.
- [15] Lambrinouidakis C, Gritzalis D. Building a reliable e-voting system: functional requirements and legal constraints. Proceedings of the 13th International Workshop on Database and Expert Systems Applications (DEXA'02); 2002. p. 435.
- [16] Gritzalis D, editor. Secure electronic voting. Advances in information security, vol. 7. Kluwer Academic Publishers; 2002a.
- [17] Gritzalis D. Principles and requirements for a secure e-voting system. Computers & Security 2002b;21(6):539–56.
- [18] Mitrou L, Gritzalis D. Revisiting legal and regulatory requirements for secure e-voting. Proceedings of the IFIP TC11 17th International Conference on Information Security; 2002. p. 469 – 80.
- [19] Sampigethaya, K. and Poovendran, R. A framework and taxonomy for comparison of electronic voting schemes. Elsevier Computers & Security, Vol. 25, No. 2; 2006. p. 137-53.
- [20] Qadah GZ. Electronic voting systems: Requirements, design, and implementation. Elsevier Standards and interfaces, Vol. 29, No. 3; 2007. p. 376-86.
- [21] Volkamer M, McGaley M. Requirements and evaluation procedures for e-voting. The second international conference on availability, reliability and security (ARES'07); 2007. p. 895-902.
- [22] Cetinkaya O. Towards secure e-elections in turkey: requirements and principles. The second international conference on availability, reliability and security (ARES'07); 2007. p. 903-07.
- [23] Krimmer R, Triessnig S. The development of remote e-voting around the world: A review of roads and directions. Springer-Verlag Lecture notes in computer science (LNCS). Vol. 4897; 2007. p. 1-15.
- [24] M Volkamer. Evaluation of electronic voting: requirements and evaluation procedures to support responsible election authorities. In Lecture Notes in Business Information Processing, Volume 30, 2009 Springer Publishing Company 2009.
- [25] OO Okediran, EO Omidiora. A Framework For A Multifaceted Electronic Voting System. International Journal of Applied Science and Technology Vol. 1 No.4; July 2011.
- [26] M Khasawneh, O Al-Jarrah. Modeling and Simulation of a Robust e-Voting System. In Communications of the IBIMA
- [27] Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 1981;24(2):84–8.
- [28] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory July 1985;31(4):469–72.
- [29] Paillier P. Public-key cryptosystems based on composite degree residue classes. In: Advances in cryptology – EUROCRYPT '99. LNCS, vol. 1592; 1999. p. 223–38.
- [30] Shahram Khazaei. Cryptanalysis of a Universally Verifiable Efficient Re-encryption Mixnet. In Cryptology ePrint Archive, Report 2012/100, available online at <http://eprint.iacr.org>, 2012.
- [31] Park C, Itoh K, Kurosawa K. Efficient anonymous channel and all/nothing election scheme. In: Advances in cryptology – EUROCRYPT '93. LNCS, vol. 765. Springer Verlag; 1994. p. 248–59.
- [32] Cramer Ronald, Gennaro Rosario, Schoenmakers Berry. A secure and optimally efficient multi-authority election scheme. In: Advances in cryptology – EUROCRYPT '97. LNCS, vol. 1233. Springer-Verlag; 1997. p. 103–18.
- [33] Chaum D. Blind signature system. In: Advances in cryptology – CRYPTO '83. Plenum Press; 1984. p. 153.
- [34] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public key cryptosystems. Communications of the ACM 1978;21:120–6.
- [35] D Sandler, K Derr, D. Wallach. VoteBox: a tamper-evident, verifiable electronic voting system. In Proceedings of the 17th conference on Security symposium USENIX Association Berkeley, 2008.
- [36] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing 1989; 18:186–208.
- [37] Blum M, De Santis A, Micali S, Persiano G. Non-interactive zero knowledge. SIAM Journal of Computing 1991;20(6):1084–118.
- [38] Shamir A. How to share a secret. Communications of the ACM 1979;22(11):612–3. Stinson DR. Cryptography: theory and practice. 2nd ed. CRC Press; 2002.
- [39] Chandramathi S. An overview of visual cryptography. In International Journal of Computational Intelligence Techniques, ISSN: 0976–0466 & E-ISSN: 0976–0474 Volume 1, Issue 1, PP-32-37, 2010.
- [40] P.S.Revenkar. Survey of Visual Cryptography Schemes. In International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.
- [41] Chaum D. Secret-ballot receipts: true voter-verifiable elections. IEEE Security & Privacy Magazine Feb 2004.
- [42] Chaum D. Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. In: Advances in cryptology – EUROCRYPT '88. LNCS, vol. 330. Springer Verlag; 1988a. p. 177–82.
- [43] Boyd C. A new multiple key cipher and an improved voting scheme. In: Advances in cryptology – EUROCRYPT '89. Springer-Verlag; 1990. p. 617–25.
- [44] Sako K, Killian J. Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth. In: Advances in cryptology – EUROCRYPT '95. LNCS, vol. 921. Springer-Verlag; 1995. p. 393–403.
- [45] Pedersen T. A threshold cryptosystem without a trusted party. In: Advances in cryptology – EUROCRYPT '91. LNCS, vol. 547. Springer-Verlag; 1991. p. 522–6.

- [46] Cohen (Benaloh) JD, Fischer MJ. A robust and verifiable cryptographically secure election scheme. In: Proceedings of 26th symposium on foundation of computer science 1985. p. 372–82.
- [47] Cohen (Benaloh) JD, Yung M. Distributing the power of a Government to enhance the privacy of voters. In: ACM symposium on principles of distributed computing 1986. p. 52–62.
- [48] Benaloh J. Verifiable secret-ballot elections, Ph.D. thesis, Yale University; 1987.
- [49] Iverson KR. A cryptographic scheme for computerized general elections. In: Advances in cryptology – CRYPTO '91. LNCS, vol. 576. Springer-Verlag; 1992. p. 405–19.
- [50] Sako K, Killian J. Secure voting using partially compatible homomorphisms. In: Advances in cryptology – CRYPTO '94. LNCS, vol. 839. Springer-Verlag; 1994. p. 411–24.
- [51] Cramer R, Franklin M, Schoenmakers B, Yung M. Multi-authority secret ballot elections with linear work. In: Advances in cryptology – EUROCRYPT '96. LNCS, vol. 1070. Springer Verlag; 1996. p. 72.
- [52] Hirt M, Sako K. Efficient receipt-free voting based on homomorphic encryption. In: Advances in cryptology – EUROCRYPT '00. LNCS, vol. 1807. Springer-Verlag; 2000. p. 539–56.
- [53] Baudron O, Foque PA, Pointcheval D, Poupard G, Stern J. Practical multi-candidate election system. In: Proceedings of the 20th ACM symposium on principles of distributed computing. ACM Press; 2001. p. 274–83.
- [54] Damgård I, Jurik M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In: Proceedings of public key cryptography, fourth international workshop on practice and theory in public key cryptography, PKC 2001, LNCS, vol. 1992. Springer-Verlag; 2002. p. 119–36.
- [55] Lee B, Kim K. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In: ICISC '02. LNCS, vol. 2587. Springer-Verlag; 2002. p. 389–406.
- [56] Schoenmakers B. A simple publicly verifiable secret sharing scheme and its applications to electronic voting. In: Advances in cryptology – CRYPTO '99. LNCS, vol. 1666. Springer-Verlag; 1999. p. 148–64.
- [57] Kiayias Aggelos, Yung Moti. Self-tallying elections and perfect ballot secrecy. In: Proceedings of public key cryptography, fifth international workshop on practice and theory in public key cryptosystems, PKC 2002. LNCS, vol. 2274. Springer-Verlag; 2002. p. 141–58.
- [58] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. In: Advances in cryptology – AUSCRYPT '92. LNCS, vol. 718. Springer-Verlag; 1993. p. 248–59.
- [59] Baraani-Dastjerdi A, Pieprzyk J, Safavi-Naini R. A practical electronic voting protocol using threshold schemes. In: Proceedings of the 11th annual computer security applications conference 1995. p. 143–8.
- [60] Okamoto T. Receipt-free electronic voting schemes for large scale elections. In: Proceedings of the workshop on security protocols '97. LNCS, vol. 1361. Springer-Verlag; 1997. p. 25–35.
- [61] Juang W, Lei C, Liaw H. A verifiable multi-authority secret election allowing abstention from voting. The Computer Journal 2002; 45(6):672–82.
- [62] Ogata W, Kurosawa K, Sako K, Takatani K. Fault-tolerant anonymous channel. In: Proceedings of the ICICS '97. LNCS, vol. 1334; 1997. p. 440–4.
- [63] Jakobsson M. A practical mix. In: Advances in cryptology – EUROCRYPT '98. LNCS, vol. 1403. Springer Verlag; 1998. p. 449–61.
- [64] Abe M. Universally verifiable mix-net with verification work independent of the number of mix-servers. IEICE Transactions on Fundamentals July 2000; E83-A(7). p. 1431–40.
- [65] Golle P, Zhong S, Boneh D, Jakobsson M, Juels A. Optimistic mixing for exit-polls. In: ASIACRYPT '02. LNCS, vol. 2501. Springer-Verlag; 2002. p. 451–65.
- [66] Lee B, Boyd C, Dawson E, Kim K, Yang J, Yoo S. Providing receipt-freeness in mixnet-based voting protocols. In: Proceedings of the ICISC '03, 2003. p. 261–74.
- [67] Kiayias Aggelos, Yung Moti. The vector-ballot e-voting approach. In: Financial cryptography. LNCS, vol. 3110. Springer-Verlag; 2004. p. 72–89.
- [68] Acquisti A. Receipt-free homomorphic elections and write-in ballots. Cryptology ePrint Archive, Report 2004/105, <<http://eprint.iacr.org/>>; 2004.
- [69] Ari Juels, Dario Catalano & Markus Jakobsson. Coercion-resistant electronic elections. In Proc. Workshop in Privacy in the Electronic Society, 2005.
- [70] Ari, Juels, Dario Catalano and Markus Jakobsson, Coercion-Resistant Electronic Elections, Towards Trustworthy Elections - New Directions in Electronic Voting, LNCS 6000, 2010.
- [71] Jefferson D, Rubin AD, Simons B, Wagner D. A security analysis of the secure electronic registration and voting experiment (SERVE). Technical Report available online at <http://servesecurityreport.org/>; 2004.
- [72] Kohno T, Stubblefield A, Rubin AD, Wallach DS. Analysis of an electronic voting system. IEEE symposium on security and privacy; May, 2004.
- [73] Simons B. Electronic Voting Systems: the Good, the Bad, and the Stupid. ACM queue, Vol. 2, No. 7; 2004. p. 20–26.
- [74] Evans D. Election security: perception and reality. IEEE security and privacy, Vol. 2, No. 1; 2004. p. 24–31.
- [75] Grove J. ACM statement on voting systems. Communications of the ACM, Vol 47, No. 10; (2004). p. 69–70.
- [76] Armen C. E-voting and computer science. Proceedings of the 10th annual SIGCSE conference on Innovation and technology in computer science education; 2005. p. 227.
- [77] Baoyuan Kang. Cryptanalysis on an e-voting scheme over computer network. International conference on computer science and software engineering. Vol. 3; 2008. p. 826–29.
- [78] Y Lee, S Park, M Mambo, S Kim. Towards Trustworthy e-Voting using Paper receipts. In Computer Standards &

- Interfaces, Elsevier, Volume 32, Issues 5–6, Pages 305-311, October 2010.
- [79] OO Okediran, SO Olabiyisi .A Survey of Remote Internet Voting Vulnerabilities. In *World of Computer Science and Information Technology Journal (WCSIT)* Vol.1, Issue 7, pages 297-301, 2011.
- [80] Barbara Ondrisek. E-Voting System Security Optimization. In *proceedings of the 42nd Hawaii International Conference on System Sciences*, 2009.
- [81] Carback, Richard T., Stefan Popoveniuc, Alan T. Sherman, and David Chaum. Punchscan with independent ballot sheets: Simplifying ballot printing and distribution with independently selected ballot halves. In *Proceedings of the 2007 IAVoSS workshop on trustworthy elections (WOTE 2007)*.
- [82] Essex, Aleks, Jeremy Clark, Richard Carback, and Stefan Popoveniuc. Punchscan in practice: An E2E election case study. In *Proceedings of the 2007 IAVoSS Workshop on trustworthy elections (WOTE 2007)*.
- [83] Chaum, David, Aleksander Essex, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, and Poorvi L. Vora. Scantegrity: end-to-end voter-verifiable optical-scan voting. *IEEE Security & Privacy*, 6(3):40–46: IEEE Computer Society 2008.
- [84] Chaum, D., R.T. Carback, J. Clark, A. Essex, S. Popoveniuc, R.L. Rivest, P. Ryan, E. Shen, A.T. Sherman, and P.L Vora. Scantegrity II: End-to-end verifiability by voters of optical scan elections through confirmation codes. *IEEE transactions on information forensics and security* 4(4):611–627, Special Issue on Electronic Voting, 2009.
- [85] Chaum, D., A.T. Sherman, R.A. Fink, R.T. Carback. Scantegrity III: Automatic Trustworthy Receipts, Highlighting Over/Under Votes, and Full Voter Verifiability. In *Proceedings of the 2011 conference on Electronic voting technology/workshop on trustworthy elections EVT/WOTE'11, USENIX Association Berkeley, CA, 2011.*
- [86] Michael Clarkson, Stephen Chong, Andrew Myers. Civitas: Toward a Secure Voting System. In *Proc. IEEE Symposium on Security and Privacy*, 2008.
- [87] PYA Ryan., T. Peacock. Prêt á Voter: a Systems Perspective.2005. Available online at [www.cs.ncl.ac.uk/publications/trs/papers/929.pdf](http://www.cs.ncl.ac.uk/publications/trs/papers/929.pdf)
- [88] Ryan, P.Y.A., D. Bismark, J. Heather, S. Schneider, and Zhe Xia. Prêt á Voter: A voter-verifiable voting system. *IEEE transactions on information forensics and security* 4(4), Special Issue on Electronic Voting, 2009.
- [89] Adida, Ben. Advances in cryptographic voting systems. PhD diss., Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2006.
- [90] C. Stefano, A. Falleni, F. Martinelli, M. Petrocchi, and A. Vaccarelli. Mobile implementation and formal verification of an evoting system. In *Proceedings of the 2008 Third International Conference on Internet and Web Applications and Services*, Washington, DC, USA: IEEE Computer Society, 2008.