Survey on End-to-End Verifiable Cryptographic Voting Systems

Labeeb Ahmed Qubati
Computer Science Dept., Faculty Of Computer And Information, Cairo University, Egypt

Sherif Khattab
Computer Science Dept., Faculty Of Computer And Information, Cairo University, Egypt

Ibrahim Farag
Computer Science Dept., Faculty Of Computer And Information, Cairo University, Egypt

ABSTRACT
Electronic voting refers to the using of computers or computerized voting equipments to cast ballots in the election. The e-voting has been developed for more than 20 years. In the electronic voting, there are three stages: the registration stage, the voting stage, and the tally stage. Verifiable cryptographic voting systems use encryption technology to secure electorate's votes and to avoid coerce them to vote for any particular candidate or to buy their votes, and any another threats. This research aims to obtain an electronic voting system could be used easily in the third world countries. In this research ten of existing cryptography verifiable voting systems have been studied, and especially focused on End-to-End verifiable voting systems, which is considered as the newest class of voting systems. In addition this paper took a system from another type of verifiable voting systems for a comparison purpose. The comparison between these systems has done according to a set of public evaluation contexts that is followed in any voting system such as: properties, cryptographic building block, ballot format, and models. This paper discusses seven of E2E voting systems, which are closer to deal with in the developing communities in order to modify any one of those systems for using in third world countries. This study concludes that most of the modern voting systems currently in place are not usable in the third world countries (despite the many positive achievements in many aspects) but can be adjusted to fit with these countries. In the future, the most appropriate E2E voting system will be chosen among systems which are mentioned in this study to be adjusted in order to fit in the third world countries.

Keyword
Electronic voting, Usability of system, Third world societies.

1. INTRODUCTION
The governments around the world are working since a long time to replace the traditional election with electronic elections, due to several benefits that achieved by electronic elections, such as less cost, less time consumption, minimize the possibility of fraud and rigging and also the capability of verification for the authenticity and integrity of the electoral process either by the voters or by the global verification without losing the privacy of voters. The election is the process through which to choose a person or party to fill a specific function in a democratic manner to allow each eligible person to cast his vote to select suitable person or party.

The electronic elections based on several requirements that must be available in any electronic voting system, such as: use of system, system security, privacy, verification, and convenience. There are many properties that can be relied upon in any assessment process for an electronic voting system (whether the voting system achieves the whole characteristics or a part of them). The electoral process passes in three basic stages, the first stage is the registration stage, when the preparation of electoral is done, the second stage is the voting stage when the voters cast their votes, and finally the tallying stage when the votes are compiled and counted then announce the results. The e-voting system can be represent in two subsystems, the first one includes the registration stage and the second one includes the other two stages.

There are many electronic voting systems classified in several ways, for example, HAVA classification which voting systems are classified into four categories one of the four categories is E2E cryptographic-based, which is consider as the newest class of voting systems. The voting systems can be also classified according to the polling place, which some of voting systems require form the voters to attend actually in the polling place, and some of voting systems allow the voters to vote anywhere via communication tools.

The aim of this study is to identify modern voting systems that can be adapted to suit in the developing societies and achieve the required properties, especially the usability, flexibility, simplicity in the use of the system in addition to the required properties to secure the system and the ability to verify and prevent coercion and selling votes.

The purpose of this paper is to obtain an electronic voting system that is safe and usable by voters, including the illiterates and handicapped people via the adaptation of the latest currently available voting systems. Accordingly, ten of electronic voting systems have been selected, seven of them are E2E verification systems and three non-E2E systems from the another types according to HAVA classification. This paper also focuses on E2E verification systems because these systems are the latest and strongest in achieving the desired properties, especially security properties. The focus was on the selection of systems that can be adapted to suit the target group in this study (developing societies in the Third World). And the non-E2E systems has been chosen for the purpose of comparison only.

After the analytical study and comparison of the currently available voting systems it became clear that most of the voting systems currently available did not fit with some of the communities, especially developing communities, despite that this systems achieved many of the required properties for voting systems, but can be adapted with some adjustments to achieve the desired goal.

This study on voting systems differs than the another research those were published in the same field, because this research targets the developing countries and third world countries,

unlike the other researches which targets the advanced countries, which are almost free from illiteracy.

The next section introduces the definition and requirements of e-voting systems. Sec. 3 presents the classification dimensions for the e-voting protocols. Sec.4 presents the study and analysis for ten of the verifiable cryptographic voting systems. Sec.5 presents five tables of comparison between these systems and Sec.6 presents discussion about those tables. In Sec.7 presents the concluding remarks of this work and some future work.

2. E-VOTING DEFINITION AND REQUIREMENTS

The governments around the world are working to replace the traditional paper-based voting schemes with electronic voting systems. The election defines as: "a process to obtain accurate data representing a set of participant's 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. One or more votes are combined into a structure called a ballot.

An eligible, authenticated participant in an election is called a voter. Each question in an election is called a race, and therefore each race has a set of candidates, potentially receiving votes from voters. A voting scheme is a protocol which has a means of receiving votes as input, and produces an output which is a tally of the votes cast.

Therefore, it is a method for conducting an election. The tally may result in a decision. The decision can, for example, be the assignment of an individual to a public office, or the institution of a referendum. In the event of a referendum vote, the set of candidates would consist of (yes) or (no) [1]".

There are many electoral systems, plans and methods. They differ in the way that they work and their property, how are they counting votes, the declaration of the results, and how they interact with the voters in the voting process and the entire election. The details depend on a large extent on the history and culture of a group of voters, and the purpose of the elections and the tools that are available.

Electronic voting is a convenient and secure way to register and vote counting. It can be used for a variety types of elections, from small committees or on-line communities through to full-scale national elections. But this comes with the possibility of violations widely and manipulation. The procedures for detecting and avoiding manipulation in paper-based systems, such as public counting of votes and monitored transport of ballot boxes, do not work when everything is done electronically [2].

The Requirements and the technologies that should be available in the electronic voting systems, which make electronic voting solution possible and safe. Any e-voting system must meet an important set of requirements, and most important of these requirements are: ease of use, accuracy so that the system does not allow removal or change in any voter's vote, and does not allow to enter any vote from any ineligible person, and also prevent malicious parties, from stuffing the ballot boxes, while does not affect the privacy of voters. Requirement of democracy, which allows only for voters who are eligible for voting to vote and only once per voter. Privacy requirement, which includes the inability to detect voter's vote in order to avoid vote buying and to avoid intimidation of voters[1,3,4].

Verification requirement, which includes enabling the voter to verify that his voice has reached the final stage of counting, and enable any person or party of re-counting and verifying the accuracy of the final results of the voting. Security requirements, that does not allow any person or party from tampering with the operations, or information, or the results of this system. Convenience requirements are necessary to accept the voters and candidates for the system, and the flexibility to facilitate its use in different types of elections such as parliamentary and presidential elections, and with minimal equipment or special skills.

3. CLASSIFICATION DIMENSIONS

This section presents the stages of voting, where the voting process pass in three phases, namely the preparation stage, the voting stage, and the tally stage and the announcement of the results, and this paper will submit some cryptographic methods that used in cryptographic voting schemes, to achieve the properties of security to the voting scheme, and this research will address the properties that must achieved by voting scheme, and it will classify voting systems, according to the polling place, As well as, according to U.S. HAVA classification[1].

3.1 Voting Stages

The elections process consist of several stages executed by different agencies see fig.1. At each stage the parties involved either on the confidence of the agency that performs the stage or that there will be observers within the agency to protect the interests of the party.

In an optimal system, at the design of each stage must take into consideration the required characteristics that remind later, and spoil possible violations in the field of security and overcome the reasonably threat by authorities that are likely to be corrupt. [5] [6] The stages show as below:

i) Registration stage: At the stage of registration determines a person who is entitled to vote by the authorities, maintain a list of registered voters and provide them with the voting credentials, which is used later in the voting stage.

ii) Voting stage: At this stage, the voters cast their ballots after verifying the authenticity of the ballot cards that were given to them in the previous phase, and the voter did not cast his vote before. Here may ask, for example, voter identification number or password, and check voter lists and thus allow the voter to cast his vote in a certain way and through a particular system.

iii) Tallying stage: In the tally stage collect the ballots papers for each voter and therefore are collected votes obtained by each candidate through those cards and published. Accuracy and verifiability are most prominent at this stage and rely heavily on what has been achieved in the previous stages of security.

3.2 Cryptographic Building Blocks

This section will submit some cryptographic methods that used in cryptographic voting schemes.

1"In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA). HAVA created the U.S. Election Assistance Commission (EAC) and assigned to the EAC the responsibility for both setting voting system standards and providing for the testing and certification of voting systems."[47].

3.2.1 Commitments

In cryptography [7,8,9] a commitment scheme allows for one to commit to a chosen value (or chosen statement) while keeping it hidden of others. There are two kinds of commitment scheme. The first kind hides the committed value information theoretically from the verifier (unconditionally hiding) but is only conditionally binding. The second kind is only computationally hiding but unconditionally binding. The Commit is hiding given $comm(A)$, one has no idea about A, and the Commit is binding, it is hard to find A' such that $comm(A) = comm(A')$. There are commitment scheme employed zero-knowledge arguments or be zero-knowledge proof systems.

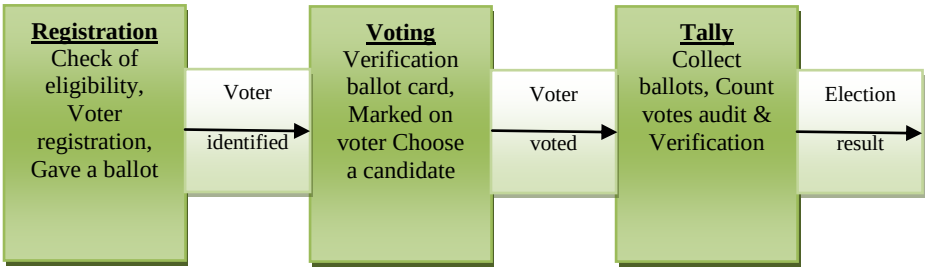

fig. (1) Three Voting Stages: Registration stage, Voting stage and Tally stage.

Cramer and Damgard describe a class of commitment schemes allowing to prove algebraic properties of the committed value. These include RSA-based and discrete-logarithm-based schemes for both kinds of commitment scheme. An example of a computationally binding and unconditionally hiding scheme based on the discrete logarithm problem is the one to Pedersen, Let ***p*** and ***q*** be large primes such that $p = 2q + 1$, and let g be a generator to subgroup of order q of Z_p^*. Let ***a*** be a random secret from Z_q, and $h = g^x \bmod p$. The values ***p, q, g*** and *h* are public, while ***x*** is secret. To commit to a message $x \in Z_q$ or $x \in \{1,...,q\}$, the sender chooses a random $r \in Z_q$ or $r \in \{1,...,q\}$, and sends the commitment $c = g^x h^r \bmod p$ to the receiver, while in order to open the commitment, the sender reveals ***x*** and ***r***, and the receiver verifies that $c = g^x h^r \bmod p$.

3.2.2 Zero-Knowledge Proofs

In zero-knowledge proof (ZKP) [10,11,12], A proof of knowledge is a protocol that enables a particular party to convince another party of the validity of a statement. In a zero-knowledge proof , this is achieved without revealing any information beyond the legitimacy of the proof. The Interactive Proof Protocol, Prover and verifier share common inputs, The protocol yields "Accept" if every response is accepted by the Verifier. Otherwise, the protocol yields "Reject".

The requirements of interactive Proofs: i) Completeness: if the statement is true, the honest verifier will be convinced of this fact by an honest prover. ii) Soundness: if the statement is false, the cheating prover can not convince the honest verifier that it is true, except with chances slim. iii) Zero-Knowledge: no information about the prover's private input (secret) is revealed to the verifier.

a. Proof of Knowledge (of discrete logarithm).

A prover tries to prove that he knows a discrete logarithm ***x.***

$$x = \log_g Y \bmod p, \quad (Y = g^x \bmod p)$$

Prover **verifier**

$t \in_R Z_q^*$

$R = g^t \bmod p \xrightarrow{R(Commitment)}$

$\xleftarrow{u(Challenge)} u \in_R Z_q^*$

$w = t - ux \bmod q \xrightarrow{w(Response)}$

$R \overset{?}{=} g^w Y^u \bmod p$

b. Proof of Equality of two discrete logarithms.

Prover tries to prove that two discrete logarithms are equal without revealing ***x.***

$$Y = g^x, z = c^x \ \& \log_g Y = \log_c z$$

Prover **verifier**

$t \in_R Z_q^*$

$R_1 = g^t \bmod p$

$R_2 = g^t \bmod p \xrightarrow{R_1, R_2(Commitment)}$

$\xleftarrow{u(Challenge)} u \in_R Z_q^*$

$w = t - ux \bmod q \xrightarrow{w(Response)}$

$R_1 \overset{?}{=} g^w Y^u \bmod p$

$R_2 \overset{?}{=} c^w Y^u \bmod p$

c. Non-Interactive Zero-Knowledge Proof.

Non-interactive Zero-knowledge (NIZK) proofs using Fiat-Shamir Heuristic.

$$x = \log_g Y \bmod p, \quad (Y = g^x \bmod p)$$

Prover **verifier**

$$t \in_R Z_q^*$$

$$R = g^t \bmod p \xrightarrow{(R,w)} \qquad u = H(Y,R)$$

$$u = H(Y,R) \qquad R \stackrel{?}{=} g^w Y^u \bmod p$$

$$w = t - ux \bmod q$$

3.2.3 Mix-Net

In 1981, David Chaum Published the paper, that introduced the idea of a mix-net, in addition to an electronic voting protocol together [13]. To create a channel anonymous for accept a set of inputs and anonymize them by a secret shuffling process using a mix-net, such that the output cannot be returned to their corresponding inputs. In electronic voting, the inputs for the application of a mix-net are encrypted votes, and the outputs are the corresponding plaintext votes.

Located between the input and output of a mix-net series of (Mix) Trustees, or Servers. [14] Each server decrypts each vote partially in a set with its own private key, then performs a secret shuffle to the set of decrypted votes partially. The server redirects all of the votes to the next server, who functions in a similar manner, until the last server in the mix-net has fully decrypted each vote. The result generates path cannot follow it from input to output see fig.(2). In the voting process, it is useful in the inability to rebuild the one-to-one correspondence between the voter and the vote, and thus achieved the non-disclosure of the identity of the voter.

In any mix-net scheme, must verifying of the actions of the servers in order to ensure integrity of the decrypted votes via an auditing process that must be available there, and the servers must produce proofs for correctness of their computations. This is achieved with the survival of maintaining the anonymity of the vote is not possible.

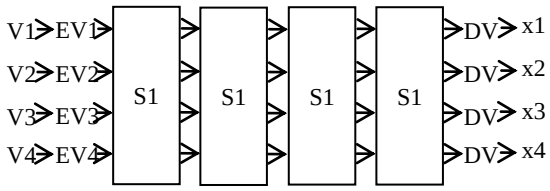

fig.(2) Show small mix-net to 4 mix servers (t=4) S1,…,St. the inputs (n=4) v1,…,vn are first privately encrypted by their providers using encryption function E. Each server Si transform and permute their inputs privately, and provide the result to the next server. The final stage decryption operation D generates a permutation version (x1,x2,...,xn) of the original input sequence, This stage may be integrated in the previous transforms.

3.3 Properties Of Elections

There are many characteristics that must be achieved by an integrated system of voting in order to meet the system requirements,[15] the desired election properties are classified into user interaction, security-related and system–related.

3.3.1 User Interaction Properties

Usability: The system must be easy to use, and should not be complicated system and difficult to use it by the users. Accessibility: Enable voters to easily access to the system, including the disabled people and do not prevent them from voting. Reliability: Generate confidence when voters in the whole voting process.

3.3.2 Security-Related Properties

The security-related properties are voter-related properties and voting-related properties.

a) Voter-Related Properties.

Ballot Secrecy: The system must not allow any third party to see the content of the ballot. Individual Verification: The system allows the voter that verify that his vote was really counted to favor the intended candidate. Coercion Resistant: a voter cannot to prove to coercer that he voted for certain candidate. Eligibility: The system allows for the eligible voters only to vote, and only once. User Anonymity: The system prevents the user from being linked to the ballot.

b) Voting-Related Properties.

Universal verifiability: The published result is the sum of all the votes really, and universal verifiability property divided into three properties are: i) Ballot Box Integrity: Show only votes of registered voters at the end of the voting process (before the counting process) without any modifications. ii) Tally Accuracy: The system does not allow any partial results, and the counting process of votes must be after the completion of the voting process. iii) Fairness: The early results are may affect the rest of the voters. The voting system must prevent early results. Auditability: The voting system allows for any third party to check on the workflow in the voting process without affecting on other security properties for authentication on the final results of the elections.

3.3.3 System-related properties

The system-related properties are integration properties and technical issues properties.

a) Integration Properties.

Integration: The system is capable of achieving different types of elections. "Ease of implementing/adapting the evaluated system as an independent verifier system for other voting infrastructures". Robustness: The voting system must be strong, secure and not subject to breakthrough by opponents and prevent any malicious behavior of voters, authorities, or others.

b) Technical Issues Properties.

Simplicity: The verification process is clear, explicit and simple. Availability: Prevent voters from casting ballots several times, and the ability of the voter to cast his vote in a specific period of time. Scalability: The effective voting systems must be scalable with respect to the needs of storage, calculation, and communication as part of the number of voters. The verifier system is scales mathematically. Flexibility: The possibility of using the voting system to deal with several types of electoral processes, and may also be in different languages.

3.4 Voting Models

This section will offer two classifications of voting models: first, according to the polling place, where voters must go to the polling place to vote, and the anther model according to the U.S. HAVA classification.

3.4.1 Site-Based Classification

There are three types of electronic voting systems, according to the polling place, namely: poll-site voting, booth voting and remote electronic voting. In the following, a short overview for each type: i) Poll-site Voting: Poll-site Voting are voting systems that require from voters to come to the polling place to cast their ballots through electronic devices

such as touch screen, and is verified the identity of the voter by traditional methods. ii) Booth Voting: In this type of the electronic voting systems are placed especially booths of the polling process in the public places such as schools , libraries or others and are secured to monitor security concerns and be under the supervision and control of election officials. Voting booths contain the electronic devices that used by voters to cast their ballots. iii) Remote Electronic Voting: The electronic voting system of this type allows for voters cast their ballots from anywhere through the tools of communications or via Internet. The methods, that can be used to determine the identity of the voter, such as: digital signature, PIN codes, biometrics, etc.

3.4.2 HAVA Classification

This classification issued by the U.S. Election Assistance Commission (EAC) see fig.(3), which was established by the Help America Vote Act of 2002 (HAVA).in the Volume 1, Appendix C of the 2005 VVSG divided the VIVSs (Voting Independent Verification Systems) into four types: [16,17,18] (i) process split-based VIVSs , the modular architecture is divided into two independent systems dealing with generation and casting operations, respectively. (ii) witness VIVSs are take a picture to a summary of the ballot during the voting phase of voters that can be used in the audit process. The voter will not be included in the image. (iii) Direct VIVSs are a voting systems that uses a scanner to scan the ballot after direct scrutiny by the voter for it, to generate an electronic record of the paper record. (iv) End-to-End encryption VIVSs systems are new voting systems (also known as receipt-based or universally-verifiable voting systems), which relies on cryptographic technologies to create an encrypted copy of the choices ballot voter, by issuing a receipt contains information does not allow to voter to prove to someone else that he voted for the particular candidate, but the voter can from through this information that verifies that his vote is used as intended and collected as defined (voter verification), and any party can verify that the votes are counted as collected (universal verification). An E2E system will provide the voter with a signed or stamped receipt of her vote.

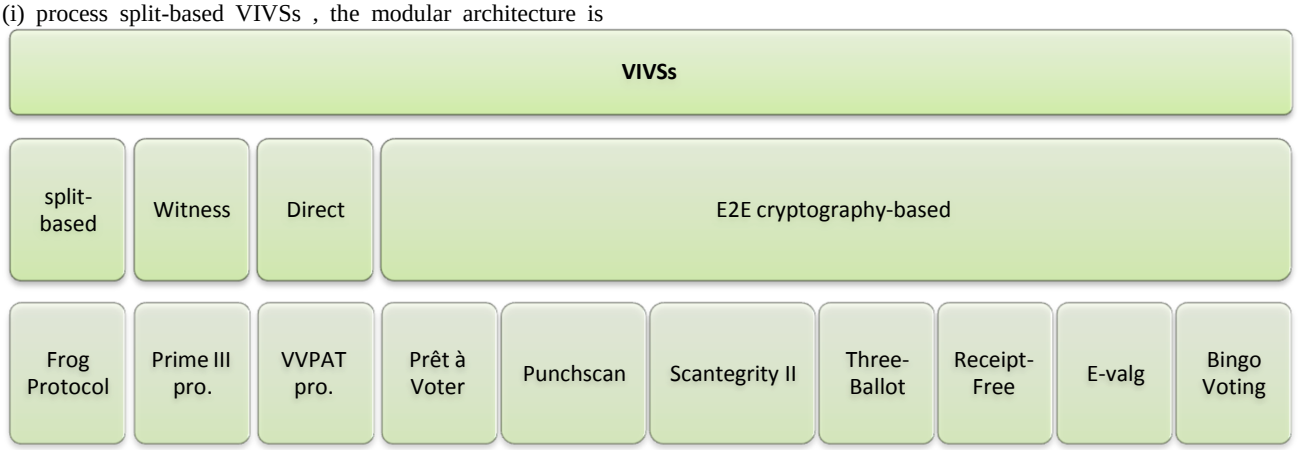

fig. (3) VIVSs Voting Independent Verification Systems according to HAVA classification.

4. STUDIED PROTOCOLS

There are many voting protocols, by the categories shown above, for election procedure and counting votes procedure in different ways. The conventional election ballots and ballot boxes become the most widely used method because the voter's privacy was mandatory for most elections.

There are verifiable voting schemes, which use cryptographic and there are many styles that provide the necessary information without compromising the privacy of the voter with different technologies those used and their properties.

As mentioned before there are cryptographic voting schemes those require the voters to go to the polling places to cast their ballots, other schemes where the voting can be of booths placed in the public places, and remote voting schemes (e.g. on the Internet), these schemes use certain techniques designed to get secure voting systems.

In addition, as mentioned above that voting systems classified by HAVA. This section gives a brief explanation of some voting protocols classified by HAVA classification and it focuses on the E2E cryptography protocols, which is considered the newest class of voting protocols.

4.1 Frog Voting

Bruck, Jefferson, and Rivest in 2001 submitted, modular voting architecture, "Frogs" where vote generation is performed separately from vote casting [19]. This scheme consists of a modular voting architecture. The basic idea here is that separates the voting procedure into two phases: vote-generation and vote-casting, where the voting process pass through three specific steps: Signing in, Vote generation and Vote casting.

Signing in: At this stage, the voter is identified by an elections official to make sure that he registered to vote. After that, election official gives empty Frog (ballots are named frogs, which are devices), and initializes it by writing some of the required information on the Frog, but The identity of the voter is not recorded.

Vote generation: The voter receives his Frog, which initialized, from the election official. After that, the voter Places his Frog into the "vote-generation" equipment. The "vote generation" equipment reads Frog style, provides the user interface to the voter to indicate his selections, (Here the voter fills the frog with his choices through a Direct-Recording Electronic (DRE) voting machine, and his choices are typed onto his Frog). The voters selections are written onto frog in a standard format.

Vote-casting: There is vote-casting equipment separates from vote-generation equipment. The voter removes his frog from vote-generation equipment, and inserts it into vote-casting equipment. After that, the voter sees frog contents displayed. If the content of the frog as intended, the frog is digitally signed, same signing key used for all votes, then frozen

(blocked against writing) and deposited in the frog bin which containing all of the cast votes. Finally, an electronic copy of vote is stored into a data memory unit and replicated in other memories for reliability.

After the election is over, the election officials publish the results on web, as two separate, unmatched lists in random order for each precinct, the first list , for names of all voters who voted, and the second list for all cast ballots (with digital signatures). Everyone can verify signatures on ballots, and compute elections' results. It is noted that this protocol achieves the user anonymity and integration of properties, but does not achieve ballot secrecy, coercion resistant, tally accuracy, fairness, and auditability. Also this protocol is weak in the accessibility and scalability, and mild in achieving the characteristics of usability and individual verification as well as the ballot box integrity, but strong in the flexibility.

4.2 VVPAT

The (VVPAT) [20] Voter-Verified Paper Audit Trail, verified paper record, is a system of independent verification of the voting machines (DREs) is designed to allow voters from verify that their vote was cast correctly, to detect election fraud possible or malfunction, and provide a way to audit the stored electronic results. VVPAT systems usually consist of a thermal printer connected to a DRE voting system with a spool of ballots enclosed within the machine.

The VVPAT creates a paper record, can be read by the human eye and visually checked by the voters, and how each vote was cast. This record can be either a ballot paper that has been deposited by the voter in the traditional ballot box, or voting system under the glass that keeps a record of paper inside the voting machine but allows voters to see it [21]. It can be said that the digital recording electronics with printed audit trails (DRE-VVPAT) is touch screen-based machines that produce a printout of each vote, verified directly by the voter, to maintain a physical and verifiable record of the votes cast.

The voting process is going through the following process: The voter determines a candidate who wants, and makes his choice in the DRE, a material paper ballot is printed of those choices and it is displayed under glass, the voter verifies that the content of the ballot paper identical to his choice, as in the DRE. Finally, voter accepts the ballot paper, if the paper is matching, and the system submits the paper ballot to the ballot box. Otherwise, the system eliminates the printed ballot paper, and repeat the process from the beginning. There is an opportunity with the voter to remove the paper record of the voting place at any moment. Therefore, all paper ballots serve as verification and audit trail of the elections. This protocol achieves the integration, tally accuracy, fairness, auditability, individual verification as well as the ballot box integrity of elections properties.

In 2009, Adolfo and Komminist presented the activities related to the development and formal verification of an e-voting system, called ProVote. ProVote is an end-to-end e-voting system with a VVPAT, resistant to security attacks and errors in user procedures [22].

4.3 Prime III

The Prime III is a secure, open-source, multimodal electronic voting system. The voter can vote by speak and touch interchangeably, Multimodal Interactions. The Voters must confirm ballot (touch or voice), and can change their vote at any time before casting the actual ballot.

This system creates video ballots, [23,24], and monitors the voting machines through video surveillance. The voter can review the captured video screen of their own voting process to verify the accuracy , this generates a voter-verified video audit trail (VVVAT). During an audit, the video and audio ballots are played back on a video player.

The voting process begins when a voter access to polling place, and conduct the necessary operations to check and assigned the polling booth to voter by poll worker. the poll worker will load the ballot using his poll worker ID, and the voter will enter the booth and use the touch screen or the headset, to cast his votes. For voting through the touch screen there large touch screens, where the ballot layout be for one race per screen. The voter touches the screen to make selection, and confirms ballot twice before it is recorded.

For voting through the headset, the system speaks to the voter through the headset, and the conversation is confidential no one can hear the machine's speech except voter itself. The system generates random numbers (may be pre-recorded) for each candidate or party and read it to the voter, and hence, the voter speaks the number for the intended candidate, and confirmation is verbal. The eavesdroppers can hear the voter but they cannot hear the machine, therefore they are not able to linked this number with the corresponding candidate.

After the completion of the voting process, the voter's ballot will be stored on the hard drive and closes the ballot application. Each Prime III machine is attached to 1 or 2 separate video recorders, where the video recorder is active when activity occurs, and sleeps otherwise. The video recorder monitors each Prime III machine, and all transactions are recorded (audio/video), where the voter and voter's voice are not recorded on video, only the screen and Prime III's audio (Voter remains anonymous). The photos are taken from the ballot paper from the video with its corresponding audio for production a video ballot, and audio read ballot.

The video recorder provides an easy way to recount. The screen review being with yellow background to distinguish it about the other video frames that containing background neutral, for helping auditors to find the ballot frames easily, and prints the number that represents the sequence of ballots (from 1 to n where the n is the total number of ballots on the video) on the bottom right corner of the ballot video.

This protocol achieves the simplicity properties, but does not achieve ballot secrecy, user anonymity, coercion resistant, individual verification, tally accuracy, fairness, and ballot box integrity. Also this protocol is weak in the flexibility and scalability, and mild in achieving the characteristics of accessibility and as well as the auditability, but strong in the usability.

4.4 Prêt à Voter

in 2004, [25] David Chaum feet a new type of receipt allows voters to verify the results of the elections even if all election computers and records were compromised. This approach applies on set of re-encryption of the votes of the Russian nesting dolls, to decrypt votes using decrypting mix-net to provide ballot privacy and anonymity, respectively.

The Prêt-à-Voter [26,27,28] is a paper-based integral voting system, the Prêt-à-Voter ballot divided into two parts, left part contains a list of candidate names arranged randomly, and the right part a custom to voters choices, and ballot identifier that corresponds to the encryption of the randomized candidate-names order, and this encryption be a form of "onion skin

layers"(public key encryptions, based on a threshold scheme). The series of onion layers generate the final ballot ID which is used by the mix-net, which in every step of partially decrypt for each vote (remove the skin from the "onion").

The voting steps of through this protocol is as follows: At first, the voter authenticates himself and registers at the polling station. He is invited to select, at random, a ballot form. The voter now enters a booth with his ballot form. The voter puts his choice (mark x) in the cell corresponding to the candidate that he wants to vote for him. Then, the ballot separates into two halves left and right (LH & RH strips). The LH strip removes, and feeds the RH strip into the voting device, in order to checks that the ballot strip is unused and read the position of voter's x and the value of onion. After that, the device marks on this strip (RH) as having been used, and return it to the voter to becomes the voter's receipt.

Once the election has been closed, the digital receipts posted on the web bulletin board. The voter visits a bulletin board and verifies that his receipt is correctly posted, and therefore be properly inserted into the screening process at a later time. In the tally process, the officials elections decrypt votes in a certain way to hide the link between specific ballot receipts and the resulting decrypted votes, in order to provide voter anonymity.

It is noted that this protocol achieves the user anonymity, ballot secrecy, individual verification, integration, and all security-voting-related properties, but does not achieve coercion resistant. Also this protocol is weak in the accessibility and scalability, and mild in achieving the flexibility, but strong in the usability.

4.5 Punchscan

The Punchscan system [29,30,31], which was provided by David Chaum, in 2005, is a receipt based voting system, that combines paper ballots and a cryptographically secure electronic tabulation process, and it is a hybrid paper/electronic system. Punchscan employs a two-layer ballot and receipt, a cryptographic tabulation system called a Punchboard. Where the Punchboard is specially constructed anonymity network, the back-end of the Punchscan system, which translates voter marks into voter choices.

The Punchscan ballot is composed of two paper layers, top layer and bottom layer. The top layer contains a list of candidate names, with a code next to each candidate name. These names and coding random order, also contain circular holes. The bottom layer contains the same codes in random order, visible through holes in the top layer see fig. (4).

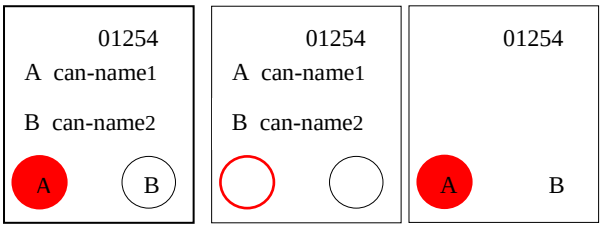

Fig. (4) A Punchscan ballot with a vote marked for can-name1. The left shows the ballot with the top and the bottom layers superimposed. The right shows the top and the bottom layer separated.

The voter marks through the hole on the code of the candidate who wants to vote for him using a marker that leaves a mark on both top layer and bottom layer. After that, the voter selects either the top layer or the bottom layer. The layer that chosen by the voter is scanned at the polling place and returned to the voter as receipt, (During the scanning process for the ballot, the voter verifies that the scanning process has done correctly). The other layer of the ballot (which was not chosen by voter) is destroyed by a cross-cut paper shredder. When the ballot layers are separated neither reveals the original vote.

The election with Punchscan system go through four phases [29], the first phase for defining ballot paper and election parameters, posting the results ballot definition file on the web server, also creating the punchboard with the specified number of ballots, questions and choice permutations. The punchboard stored on the recordable media is published on the web server. All data in this phase is encrypted.

In the second phase, The Auditors perform a Pre-Election Audit by choosing half the ballot ID numbers listed in the Punchboard, and Election Officials decrypt the whole rows of the Punchboard, which conformity for chosen ballot ID numbers. The partially decrypted Punchboard is send to the web server, and conducts the process of data validation by auditors and observers, to ensure the health of the specified processes. Also in this phase is issued the ballot images ready for print, for each ballot ID number were not chosen to audit, stored on discrete storage device and send it to the printer to print them, and finally send the printed ballots to the polling place.

The third stage is the stage of voting, where voters go to cast their votes. After the voter determines his preferred candidate on the ballot, the ballot is scanned (for the layer that chosen by the voter), the ballot is returned to the voter and an electronic copy is prepared, encrypted and send to the web server, and save copy of it on a removable storage device. The voters can visit the election website to verify that ballots published correctly. The Punchboard is filled with data obtained from each encrypted ballot, and is extracted votes by processed each ballot mark through the Punchboard's Decrypt table. The updated Punchboard and vote totals are send to the web server.

The fourth phase, the results are published online, and the auditors carrying out a Post-Election Audit, and decrypt the chosen half of the decrypt table to reveals half of the ballot mark translation process.

This protocol achieves the user anonymity, ballot secrecy, individual verification, and all security-voting-related properties, but does not achieve coercion resistant. Also this protocol is weak in the accessibility and scalability, and mild in achieving the flexibility, but strong in the usability.

4.6 Scantegrity & Scantegrity II

As is well known from before, that Punchscan ballots consist of two layers of paper, and Prêt à Voter ballots randomize candidate name order. Scantegrity [32] is an improvement of Punchscan combining the draw of the two layers in a layer.

The Scantegrity uses with optical scan voting systems, (only voter-verifiable system with familiar optical-scan user interface). Scantegrity is the first independent E2E verification mechanism that saves optical scan as the primary voting system and does not inconsistent with a manual recount.

The Scantegrity ballot is an optical scan ballot with randomly assigned code letters next to each candidate's name, and contains perforated chit in the corner contains a serial number written in human and computer readable forms see fig. (5).

When the voter casts his vote, The voter marks the circle adjacent to the candidate favorite, and registers the random code letter for this candidate on his ballot card, and feeds ballot into an optical precinct scanner.

The receipt in Scantegrity, a voter cuts a perforated corner of the ballot, called a ballot chit, that contains a serial number, also writes down the randomly assigned code letter listed next to the selected candidate. This a receipt delivers to voter to verify that his vote as intended after the counting of votes. The Scantegrity uses the permutation to recover the vote while hiding the link between serial number and vote, to anonymity.

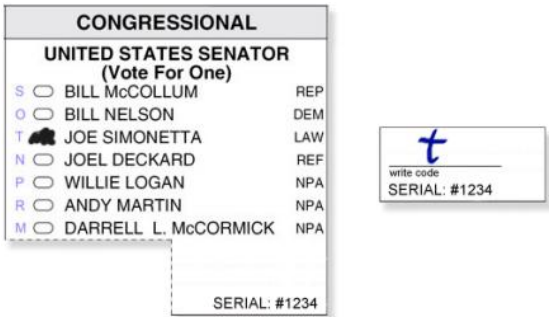

Fig. (5) Scantegrity Ballot and Receipt."Scantegrity uses an optical scan ballot with randomly assigned code letters located next to each choice (left). The perforated chit in the corner contains a serial number and a space for the voter to write down a code. The chit is torn off and kept by the voter as a receipt (right)" The source of [46].

David Chaum, et al. [33,34] submitted proposed Scantegrity II, a variant of Scantegrity that allows disputes to be handled through an online (as opposed to in-person) protocol. Where, The receipt, aforementioned, creation is unsupervised, it is possible for disputes to occasionally arise between voters and election officials over which confirmation code is correct.

The ScantegrityII addresses this point in a more advanced manner than its predecessor. The ScantegrityII Integrates traditional opscan with modern cryptographic (end-to-end) methods, and uses Invisible ink for "confirmation codes (CC's)" , web site, and crypto (back end).

The ballots can be scanned by ordinary scanners, and can be recounted by hand. The application of Scantegrity II requires changes in the software and in the information managed by the voting procedure. This information consists of four tables), which provides permutation and randomization to unlink voting preferences of casted ballots (i.e., mixing) to provide ballot privacy and ballot anonymity. The voter marks ballot as in conventional opscan, but uses a special pen for reveal the invisible ink.

The Scantegrity II ballot consists of two parts one for voting and other for receipt see fig. (6), each ballot with unique ID number. The voting part of the ballot includes the ballot's ID and a list of candidate names with an optical mark recognition field, referred to as a bubble, beside each candidate name, where the bubble contains a confirmation code (sequence of randomly generated alphanumeric characters) printed in invisible ink.

The confirmation code reveals, when the voter marks the bubble for candidate with a special decoder pen and the receipt part includes the ballot's ID, and area for writing a confirmation code for the candidate by voter. The officials workers also post revealed CC's, and the voters can confirm posting (uses ballot serial number for lookup, ID), and protest if incorrect.

The protocol steps: i) check in, by voter's name and address and then the voter is giving a card to vote. ii) the voter is getting ballot and verification card. iii) the voter marks ballot, (optionally) marks a receipt. iv) the voter casts ballot and inserts ballot into scanner. V) after polls close, verify vote online by ballot serial number. Because the code numbers are randomly chosen for each ballot, they will not reveal how the voter voted.

This protocol achieves the user anonymity, ballot secrecy, individual verification, coercion resistant, integration, simplicity and all security-voting-related properties. Also this protocol is weak in the accessibility and scalability, and mild in achieving the flexibility, but strong in the usability.

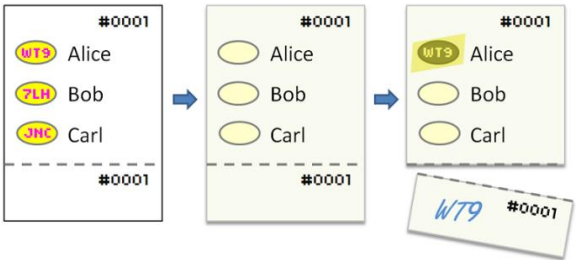

Fig. (6) ScantegrityII Ballot and Receipt, " Left: Printable ballot image with invisible regions specified by a false-color mapping)magenta and yellow). Middle: Printed paper ballot. The confirmation codes, printed in invisible ink, are initially not visible. Right: Marked paper ballot and receipt. Marking a bubble with the decoder pen causes the confirmation code to become visible", the source of [34].

4.7 ThreeBallot

In 2006, Rivest [35] proposed a system for voting on paper that protects the auditability of the count by ordinary voters and still guarantees ballot secrecy. The ballot in this system is a multi-ballot (three ballots) in the same shape (each of these ballots contains the same list of candidates with an op-scan bubble next to the name of each candidate that can be filled in by the voter) and differ only in the ID ballot. The ballot ID number on the bottom of each ballot is unique, as shown in fig(7).

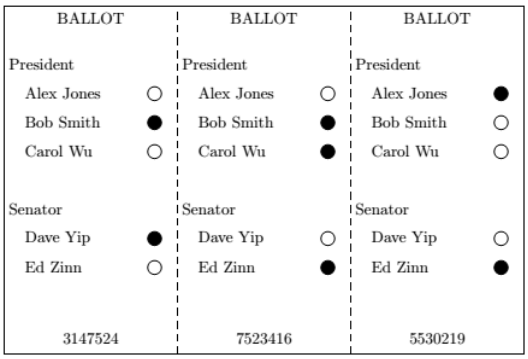

Fig. (7) "Filled-out version of multi-ballot, showing a vote FOR Smith for President and a vote FOR Zinn as Senator, since the rows for these candidates have two filled-in bubbles (marks) each. All other rows have exactly one mark. (There are many other ways such choices could have been indicated.) Note that ballot 7523416, when viewed as a conventional ballot, looks like an over vote for President", the source [35].

In the ThreeBallot system, Each voter identifies herself at the poll site, and then gets a paper consists of three ballots as in fig (7) "multi-ballot" to vote. After that, to vote for the desired candidate, the voters must choose a candidate in two of the three ballots, and to vote against a candidate unwanted (the equivalent of leaving blank vote on other systems), the voters must choose a candidate in one vote only.

After the end of the selection in the multi-ballot, the voter inserts the multi-ballot in the checker machine for verification. The checker checks of that each row in a multi-ballot has one or two marks. In other words, no candidate may be left blank on all ballots in ThreeBallot system, and no candidate can be selected on all three ballots that should be applied by a trusted authority, which could be a mechanical device to prevent multiple vote fraud.

The voter takes home copy of arbitrarily-chosen one (any one of a three ballots) as receipt, this receipt does not indicate how he voted. After that, the voter puts a three original ballots separately into the ballot box to casting three ballots. After the completion of the election process, the cast ballots are scanned and it posted on the bulletin board, in addition to the publication of the names of all the voters who participated in the elections.

The tally in ThreeBallot system, each candidate receives *n* votes (*n* the number of participating voters) added to the number of votes obtained by the candidate , but election outcome is unchanged. Where the vote totals for each candidate can be calculated by subtracting the number *n* from the total number of marks for that candidate.

In 2007, [36] Rivest and Smith presented a proposal VAV Like ThreeBallot, where each voter casts three ballots and takes home copy of one as a receipt, but VAV works for any vote-tallying system (e.g. IRV), not just plurality, approval, and range-voting. The idea is that one ballot may cancel another ballot. This means that the three cast ballots, two of them must cancel each other. VAV (Vote, Anti-Vote, Vote), two ballots are V(Vote) and one ballot is A (Anti-Vote). The canceling be between two ballots identical except for A/V notations, while the remaining V contains the voter's preferences. The remaining ballots are tallied to determine election results. VAV handles any voting system, and also provides end-to-end security.

Also, The authors used floating receipts. When a voting system employs floating receipts, voters take home the receipt of another voter. The voter cannot use take-home receipt to sell his vote, because it is copy of some other voter's ballot. The voter places his receipt into the bin, and receives a copy of some previous voter's receipt from the bin. The idea of use a bin to toss one's receipt and take another's receipt randomly. They imagine that the poll-site has a bin of preprinted blank ballots, and that the voter randomly selects three to form his multi-ballot.

In 2008, [37] Santin, Costa, and Maziero submitted a proposal to develop three-ballot scheme to provide a full electronic solution. This proposed is fully computerized architecture, it was built using the following entities: a registration agent, a voting console, a voting manager, an electronic ballot box, and an electronic election bulletin board. The voting process consists of three stages: i) The registration phase, where the voters go to the registration agent to get a credential that qualifies them to vote, and also to obtain the corresponding ballot IDs and uses them to build credentials that are returned to the voters. ii) Voting phase, once authentication the voter, the voter casts his vote during the voting console and it stores in the electronic ballot box while the voting console gives a voting receipt back to each voter. iii) The vote counting, here the votes are counted and published in a bulletin board.

It is noted that this protocol achieves the all security-related properties and availability. Also this protocol is weak in the usability and flexibility accessibility, and mild in achieving the scalability.

4.8 E-valg 2011

Norwegian Ministry started e-Valg 2011 project in August 2008, remote electronic voting at municipal elections in 2011. In 2009, been chosen ErgoGroup and Scytl to provide electronic voting solution to the Norwegian municipal elections [38]. These parties made solutions to meet all security requirements using encryption techniques, and different systems are designed to support two types of voting poll site-based and remote voting which meets the system requirements specification of the E-valg 2011 project [39].

The E-valg 2011 has been designed specifically to work remotely, in addition to that it supports polling models uncensored. Thus, this system contains two options, so that the voters can choose the way that they want for vote, either through a computer at the voting site or vote through the Internet. Where the workflow in the system for both cases are the same, with the difference that the latter case is exposed to certain risks. At elections [40] , sending voting cards to voters via email, note that the voting cards contain Vote Card ID, and list of candidates names (Voting options) next to each candidate's name the return code random.

In the voting process, The voter uses a computer to cast his vote, by provides his card ID credentials to the voting application for authenticates the voter to the voting server. The voter marks on the preferred candidate on the list of candidates that displayed by the client application (ballot). Vote encrypt by e.g. ElGamal encryption. Further, it signs the encryptions using voter's "vote-card-ID", and generates one zero-knowledge proof per encryption. After that, the values generated in this step are sent to the vote collector server (VCS). VCS verifies the voter's zero-knowledge proofs and the signatures (Operated Encrypted Vote). If accepted, all received values, and with the values generated in this step are sent to return code generator (RCG).

RCG performs the same verification steps as VCS, and verify VCS's computations. If accepted, computes a return code which must that corresponding to the voting card for same voter, and create the receipt contains this code that send to the voter via SMS. It also sends a voting receipt to VCS to confirm that the vote is accepted and the SMS has been sent. Upon reception, VCS stores the vote and forwards the voting receipt to the voter for confirmation. RCG saves its voting receipt for the purpose of verification during the tallying stage. After that, the voter compares the codes which sent to him by SMS with the values on his voting card.

After that, the electronic ballot boxes which collected in the VCS, digitally signed to ensure the authentication and integrity, which contains the encrypted votes and encryption proofs are transferred securely to new system in a safe place, and digital receipts are saved for each votes to enable voters to make sure that their votes were counted at the counting stage, and are also validate digital certificates.

After that, the verification of digital signatures to ensure their authenticity and integrity. Then, the digital signatures for the votes are removed to be anonymous. The anonymous votes

addressed through re-encryption mix-net, so that the outputs from this process is all the votes re-encrypted and shuffled and a set of zero knowledge proofs for verifying the correct mixing process. After that, the Electoral Council being the digital signature on list of all decrypted votes and announcement of the election result.

It is noted that this protocol achieves the all security-related properties and availability. Also this protocol is weak in the flexibility accessibility, and strong in achieving the scalability, accessibility, and usability.

4.9 Receipt-Free

In 2006, [41] Tal Moran and Moni Naor submitted a proposal for the first universally verifiable voting system based on a general assumption that can be based on any non-interactive commitment. And also it is first Receipt-Free Voting Scheme with Everlasting Privacy, and it uses a voting machine to receive the voter's choice and generate receipt. As well as, this protocol contributes with a formal definition of receipt-freeness and uses secure (integrity) proofs in the Universal Composability Model (Security against arbitrary coalitions "for free").

This scheme is somewhat similar to non-electronic voting systems, where voters cast their vote at the polling stations. The votes are scheduled for each station separately and the final count is calculated by aggregating the results of each stations. In this system, there are three requirements from the voters: The voter sends a short message to the DRE, verification of the match between two strings, one chosen by the voter himself, and chose a random string.

The basic idea is that the machine voting prints the commitment for the candidate chosen by the voter and then proves that the content of this commitment is the name of this candidate , using a zero-knowledge proof. The Moran-and-Naor's voting scheme includes a great advantage is that it requires almost no specific preparation. In this system requires the provision of public bulletin board, so that all the parties in the system can reading from the board and all messages are transferred from DRE to the bulletin board.

The protocol consists of three stages: Casting, Tallying, and Universal Verification. At the casting stage, the voter communicates with DRE over a private channel. The voter cannot access the bulletin board from the voting booth, so they assumed that there will be a separate channel between the DRE and voters and also with the printer. The outputs of the DRE are messages to the printer (print the receipt) and to the bulletin board. Thus the voter checks that the contents of his receipt and the contents of the bulletin board are identical. Also in the cast stage, the system encrypts votes and put the commitments to them, for the purpose of not to reveal confidential information contained in the vote, and to ensure that the content of the vote is as intended.

The steps of casting are as follows: The voter chooses the candidate that intended to vote for him, The DRE encrypts the voter's vote by calculating the commitment and attends proof that this commitment holds with his choice. This step consists of computing masked copies of the real commitment. The voter enters random words (dummy challenges) for each of the other candidates , The DRE converts each challenge to string of bits using a certain algorithm (e.g., by hashing), and generates a commitments in response to this challenges for the other candidates different to the voter's choice [41]. The DRE now computes a commitment *x* to everything and prints *x* on the receipt. After that, the voter enters random words (real challenge) for his candidate, and also the DRE translates this challenge into string of bits, and the DRE computes the answers to the challenges and saves the answers. Then, the DRE prints the voter name and the names of the candidates with the corresponding challenges for each them.

The voter checks of the challenges printed on the receipt, if not identical to the previous challenges (his choosing) cancels this process by pressing the ESC, and in case of conformity picks OK to accept receipt. If the voter accepts the receipt, the DRE prints a "Receipt Certified" on the receipt. After that the voter takes his receipt and leaves. The DRE sends a copy of receipt to the bulletin board, along with the answers to the challenges and information to open the commitment *x*. The voter can verify that his receipt posted on the bulletin board correctly.

The tally stage, in this phase the election officials takes the first commitment of each receipt and uses a shuffle of known content to prove that the tally corresponds to the content of these commitments without giving any additional information about the choice of a single voter (for purpose anonymity voter).

The Universal Verification, This stage to ensure that the DRE sends required messages well formed, and opened all commitments correctly. Where in the final tally phase, the verifier checks that all commitments were opened correctly according to the challenge bit.

In 2007. Feet T. Moran and M. Naor improve for this scheme, Instead of owning the keys that are used to open the commitments by a single party (the DRE), they used the threshold scheme for distribution the key between several parties. This has been improved this system (Receipt-Free) and get a new scheme (Split-Ballot voting scheme) [42].

This protocol achieves the all security-related properties except eligibility and auditability, and it achieves the robustness and integration. Also this protocol is weak in the accessibility, usability and mild in achieving the scalability, accessibility, and flexibility.

4.10 Bingo Voting

In 2007, [43] The Bohli, Muller and Rohich submitted a proposal for voting protocol (Bingo Voting). They focus on split the relationship between voter and ballot, avoid vote buying, coercion resistant, and universal verification.

In this protocol used some of cryptographic building blocks as commitment, zero knowledge proofs, receipts, and bulletin board. Also used the trusted random number generator. The basic idea of bingo voting is that each voter will cast his vote on the ballot and take a copy of the ballot as a receipt. After the election closed all ballots are published so that each voter can verify that his vote counted correctly.

The protocol is described in three stages as follows: i) Pre-Voting stage, before election day, the voting machine generate, for each voter, one random number per candidate, generating a pair of random number and candidate. For voter v_i and candidate c_i, such a pair would look like $(r_{i,j}, c_j)$ (dummy vote pairs for the candidate c_j). Thus, for n voters and *m* candidates, the voting machine generate $n \times m$ pairs, and keep these dummy vote pairs secret, but publish commitments to these dummy vote pairs.

ii) Voting stage, The voter selects his candidate by pressing the according candidate's button on the voting machine. The

TRNG generates a fresh random number, and sends it to voting machine, this fresh random number is assigned for the candidate of the voter's choice. All other candidates are assigned one of the previously generated random numbers (of the pool of dummy votes for the respective candidate). The voter verifies of that the fresh random number is given to his candidate. After that, The voter is given a receipt, on which the candidate of his choice is assigned the freshly generated random number. To ensure that the receipt cannot be used to sell his vote, all other candidates are assigned one of dummy votes. The voter leaves the booth and takes out the receipt.

iii) Post-Voting stage, the voting machine calculates the result and sends it to a public bulletin board with a proof of correctness. The published data consists of digital copies of all handed-out receipts, list of all unused pairs(dummy votes) and is opened, proof to prove that all unopened commitments (unused dummy votes) are indeed used on one receipt, and also proof to prove that each candidate received the same number of the dummy votes.

The final result is then given by the unused dummy votes pairs. Note that an abstaining voter leaves one unused dummy vote per candidate. Hence, the abstaining voters can be deducted from the tally, if necessary. The voter can verify that his receipt is included in the list and therefore was counted for the tally[44,45].

This protocol achieves the all security-related properties except eligibility and auditability, and it achieves the integration. Also this protocol is weak in the accessibility, usability and mild in achieving the scalability, and flexibility.

5. TABLES

Table 1: List of symbols are used in the tables 2, 3, 4 and 5

Ballot format	
E	Electronic
P	Paper
HAVA Classification	
SB	Separation-based
WB	witness-based
D	Direct
E2E	E2E cryptography-based

Location-based classification	
PS	Poll-site Voting
K	Kiosk Voting
RE	Remote Electronic Voting
Encryption	
AES	public-key cryptography (AES (Advanced Encryption Standard) with a 128-bit key size)
PKE	PKE, pased on threshold scheme

Anonymity	
SAN with RPC	Specialized Anonymity Network with Randomized Partial Checking (RPC)
RPC	Randomized Partial Checking
Properties	
S	Strong
M	Moderate
W	Weak

Table 2: The voting model for cryptography voting verifiable systems

protocols	Ballot format	Voting Models		Voting Stages	
		HAVA Classif.	Location-based	Registration	Voting &Tallying
VVPAT	**P**	D	**PS**		☑
Prime III	**E**	WB	**PS**		☑
Frog	**E**	**SB**	**PS**		☑
Prêt à Voter	**P**	E2E	**PS**		☑
Punchscan	**P**	E2E	**PS**		☑
Scantegrity II	**P**	E2E	**PS**		☑
ThreeBallot	**E**	E2E	**PS**	☑	☑
Receipt- Free	**E**	E2E	**PS**		☑
Bingo Voting	**E**	E2E	**PS**		☑
E-valg	**E**	E2E	**RE**	☑	☑

Table 3: The cryptographic building blocks for cryptography voting verifiable systems

protocols	cryptographic building blocks					
	Encryption	Anonymity	Receipts	Bulletin board	ZKPs	Digital signatures
VVPAT						
Prime III						
Frog		randomization	✓	✓		✓
Prêt à Voter	PKE	Mixnet or reencryption	✓	✓		
Punchscan	AES	CAN with RPC	✓	✓		✓
ScantegrityII	Commitment	RPC	✓	✓		
ThreeBallot	RSA	Mixing(hash)	✓	✓		✓
Receipt- Free	commitment	remasking+ permutation	✓	✓	✓	
Bingo Voting	commitment	remasking+ permutation	✓	✓	✓	
E-valg	ELGamal	multiplicative homomorphic	✓	✓	✓	✓

Table 4: The security-related properties of cryptography voting verifiable systems

protocols	Security-related Properties of Elections								
	Voter-related					Voting-related			
	Ballot Secrecy	User Anonymity	Coercion Resistant	Individual Verification	Eligibility	Universal verification			Auditability
						Ballot Box Inte.	Tally Accuracy	Fairness	
VVPAT				✓		✓	✓	✓	✓
Prime III									M
Frog		✓		M		M			
Prêt à Voter	✓	✓		✓		✓	✓	✓	✓
Punchscan	✓	✓		✓		✓	✓	✓	✓
Scantegrity II	✓	✓	✓	✓		✓	✓	✓	✓
ThreeBallot	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt- Free	✓	✓	✓	✓		✓	✓	✓	
Bingo Voting	✓	✓	✓	✓		✓	✓	✓	
E-valg	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 5: The user interaction and system-related properties of cryptography voting verifiable systems

protocols	User Interaction and system-related Properties of Elections								
	User Interaction			system-related					
	Accessibility	Usability	Reliability	Robustness	Integration	Simplicity	Availability	Scalability	Flexibility
VVPAT					✓				
Prime III	M	S				✓		W	W
Frog	W	M			✓	✓		W	S
Prêt à Voter	W	S			✓			W	M
Punchscan	W	S						W	M
Scantegrity II	W	M			✓	✓		W	M
ThreeBallot		W				✓	✓	M	W
Receipt- Free	W	W		✓	✓			M	M
Bingo Voting	W	W			✓			M	M
E-valg	M	M				✓	✓	M	W

6. DISCUSSION

This survey analyzes ten verifiable cryptographic voting systems, which were classified into four types according to the HAVA classification as described in Subsection 3.4, and compares these systems in terms of their achieving of 18 desired election properties described in Subsection 3.3. The table 4 and table 5 summarize this comparison.

From Table 4 can be concluded that E2E verification systems (seven from the ten studied systems) achieve three of the voter-related security properties, namely ballot secrecy, user anonymity, and individual verification, but the eligibility property was not covered as required in five systems. The coercion-resistance property was not covered in two systems, namely Prêt-à-Voter and Punchscan. On the other hand, non-E2E systems (VVPAT, Prime III, and Frog) did not achieve the voter-related security properties except the Frog system, which achieved user anonymity and individual verification, and VVPAT, which achieved individual verification.

From Table 4 also can be concluded that E2E verification systems (seven of the ten studied systems) achieve three of the voting-related security properties, namely ballot box integrity, tally accuracy, and fairness. The auditability property was not covered as required in two systems, namely Receipt-Free and Bingo-Voting . On the other hand, non-E2E systems (Prime III and Frog) did not achieve two of the voting-related security properties, namely tally accuracy and fairness. The ballot box integrity property was not covered in Prime III, and the auditability was not covered in Frog. The VVPAT achieves all the voting-related security properties.

Also, From Table 5 also can be concluded that E2E verification systems did not cover the user interaction and system related properties as required. The robustness property was covered in Receipt-Free system only. The integration property was not covered in three systems, namely Punchscan, ThreeBallot and E-valg. The simplicity property was not covered in four systems, namely Punchscan, Prêt-à-Voter, Receipt-Free, and Bingo-Voting. The Scantegrit II, Punchscan, and Prêt-à-Voter are weak in the scalability property, While Receipt-Free, Bingo-voting, E-valg, and three-ballot are medium. The scantegrit II, Punchscan, Prêt-à-Voter, Receipt-Free, and Bingo-voting are medium in the flexibility property, and the ThreeBallot and E-valg are weak in this property. On the other hand, non-E2E systems (VVPAT and Frog) achieve the integration property. The simplicity property was not covered in the VVPAT system. The PrimeIII is weak in the scalability and flexibility properties. The Frog is strong in the flexibility property but weak in the scalability property.

The user interaction given that all voting verifiable systems use DREs to emit votes. Table 5 shows that Prêt-à-Voter and Punchscan of the E2E verification systems are strong in the usability property, and Receipt-Free, Bingo-voting, and ThreeBallot are weak in the usability property, and scantegrit II and E-valg are medium. The E2E verification systems are weak in the accessibility property except the E-valg system is medium. On the other hand, non-E2E systems, the PrimeIII system is strong in the usability property and medium in the accessibility property. The Frog system is medium in the usability property and weak in the accessibility property. For the reliability property differs if it measured with a society where illiteracy abound, especially in the field of electronic technology.

From Table 5 also can be concluded that verifiable cryptographic voting systems did not cover user-interaction properties as required to suit with users in developing communities, the security-related properties have been well addressed in E2E verification systems . Also observed deficiencies in the coverage of the system-related properties.

Table 2 classified the verifiable cryptographic voting systems according to HAVA classifications and location-based classifications, and the stages of the voting systems (Registration, Voting, and tallying). From Table 2 can be concluded that the voting systems independent of the preparation of voter lists and electoral registers as well as verifying the identity of voters and checking whether the voter has voted before, for reduction of repeat voting, except the ThreeBallot and E-valg.

Table 3 presents a summary of the cryptographic building blocks, which were used in cryptographic voting systems. The E2E systems were used zero knowledge proofs for correctness in three systems, namely Receipt-Free, Bingo-Voting, and E-valg. Also, the E2E systems were used digital signatures in

three systems, namely Punchscan, threeballot, and E-valg. In addition, it was noted that E2E systems used the receipts and bulletin boards.

The E2E systems were used cryptography algorithms to encryption and anonymity. For encryption, the Prêt-à-Voter was used (PKE) public key encryptions passed on threshold scheme, the Punchscan was used AES (Advanced Encryption Standard) with a 128-bit key size), the Scantegrity II, Receipt-Free and Bingo-Voting were used commitment scheme, the ThreeBallot was used RSA algorithm, and the E-valg was used ELGamal encryption. For anonymity, the Prêt-à-Voter was used "Mixnet or reencryption Mixnet", Punchscan was used "CAN with RPC " (Specialized Anonymity Network with Randomized Partial Checking (RPC)), the Scantegrity II was used "RPC", the ThreeBallot was used additive homomorphic cryptography to guarantee voter anonymity (hash Mixing), the Receipt-Free and Bingo-Voting were used "remasking with permutation", and the E-valg was used "multiplicative homomorphic with mixing".

On the other hand, the Frog system (non-E2E systems) used the digital signatures, receipts, and bulletin boards. as well as Frog system used simple randomization algorithm to guarantee voter anonymity. While the rest of the non-E2E systems cannot be reliable because they were not as far enough in this aspect.

7. CONCLUSIONS

This paper presents a comparative study of verifiable cryptographic voting systems, requirements of voting systems and cryptographic building block, which used in the voting system. In addition, this paper has studied ten of voting systems, which is the closest to deal with developing communities for the purpose of modifying any one of these systems for use in third world countries, and this research focused on E2E cryptographic voting systems, and it compared between them to determine similarities and differences between the electronic voting systems, and coverage those systems for the properties and requirements of voting systems. This study shows that the voting systems are useful for dealing with handicapped and illiterate people. In addition to that use of electronic voting systems reduces the economic costs and logistics of the elections, as well as the it reduces the fraud and vote rigging.

Through this study, can be concluded that access to an electronic voting system, commensurate with the human absorption and fits with the third world countries based on what has been achieved in the electronic voting systems currently in place, requires a focus on the ability of voters (third world countries) to deal with voting systems and acceptance of the system, which is not enough in the current voting systems (are used in the developed countries), but can be adjusted to fit with the target group in this study. The focus in the future will be through the development of one of E2E voting systems has been described in the research, to enable voters in the third world countries to use the electronic voting in the elections.

8. REFERENCES

[1] Staub, Julie Ann, "An Analysis of Chaum's Voter-Verifiable Election Scheme" (2005).

[2] Delaune, Stéphanie and Kremer, Steve and Ryan, Mark, "Verifying privacy-type properties of electronic voting protocols", Journal of Computer Security 17, 4 (2009), pp. 435--487.

[3] Haenni, Rolf and Koenig, Reto and Fischli, Stephan and Dubuis, Eric, "TrustVote: A Proposal for a Hybrid E-Voting System", Bern University of Applied Sciences, Höheweg 80 (2009).

[4] Sastry, Naveen K, "Verifying security properties in electronic voting machines" (2007).

[5] Rosner, Ilana Mushinsky and Rosner, Gedon, "Electronic Voting Protocols and Schemes", The Hebrew University of Jerusalem, Israel (2002).

[6] Backes, Michael and Hritcu, Catalin and Maffei, Matteo, "Automated verification of remote electronic voting protocols in the applied pi-calculus", in Computer Security Foundations Symposium, 2008. CSF'08. IEEE 21st (, 2008), pp. 195--209.

[7] Menezes, Alfred J and Van Oorschot, Paul C and Vanstone, Scott A, Handbook of applied cryptography (CRC press, 1996).

[8] Cramer, Ronald and Damgrd, Ivan, "Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free?", in Advances in Cryptology — CRYPTO'98(1998), pp. 424--441.

[9] Pedersen, Torben Pryds, "Non-interactive and information-theoretic secure verifiable secret sharing", in Advances in Cryptology—CRYPTO'91 (, 1992), pp. 129--140.

[10] Fiat, Amos and Shamir, Adi, "How to prove yourself: Practical solutions to identification and signature problems", in Advances in Cryptology—CRYPTO'86 (, 1987), pp. 186--194.

[11] Goldrech, O, "Foundations of Cryptography Teaching Notes", Citeseer (2001).

[12] Aggelos Kiayias, Notes by S. Pehlivanoglu, J. Todd, and H.S. Zhou. Cryptography Primitives and Protocols.

[13] Chaum, David L, "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of the ACM 24, 2 (1981), pp. 84--90.

[14] Jakobsson, Markus and Juels, Ari and Rivest, Ronald L, "Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking.", in USENIX security symposium (, 2002), pp. 339--353.

[15] Delaune, Stéphanie and Kremer, Steve and Ryan, Mark, "Verifying properties of electronic voting protocols", in in" Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE'06 (, 2006).

[16] United States ,Election Assistance Commission. 2005. Voluntary voting system guidelines. http://www.eac.gov/assets/1/workflow_staging/Page/124.PDF.

[17] Pujol-Ahulló, Jordi and Jard́ı-Cedó, Roger and Castellà-Roca, Jordi, "Verification Systems for Electronic Voting: A Survey", Electronic Voting 2010 (EVOTE2010) (2010), pp. 163.

[18] Roger Jard´ı-Ced´o, Jordi Pujol-Ahull´o, Jordi Castell`a-Roca,and Alexandre Viejo, "Study on poll-site voting and verification systems", Computers Security, pp. 989--1010, Elsevier 2012.

[19] Rivest, Ronald L and Jefferson, David and Bruck, Shuki, "A Modular Voting Architecture (" Frogs")", August (2001).

[20] Goggin, Stephen N and Byrne, Michael D, "An examination of the auditability of voter verified paper audit trail (VVPAT) ballots", in Proc. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 07) (, 2007).

[21] Mercuri, Rebecca T, "Electronic vote tabulation checks and balances", (2001).

[22] Villafiorita, Adolfo and Weldemariam, Komminist and Tiella, Roberto, "Development, formal verification, and evaluation of an E-voting system with VVPAT", Information Forensics and Security, IEEE Transactions on 4, 4 (2009), pp. 651--661.

[23] Cross, EV and Rogers, G and McClendon, J and Mitchell, W and Rouse, K and Gupta, P and Williams, P and Mkpong-Ruffin, I and McMillian, Y and Neely, E and others, "Prime III: one machine, one vote for everyone", On-Line Proceedings of VoComp (2007).

[24] Goggin, Stephen N and Byrne, Michael D and Gilbert, Juan E and Rogers, Gregory and McClendon, Jerome, "Comparing the Auditability of Optical Scan, Voter Verified Paper Audit Trail (VVPAT) and Video (VVVAT) Ballot Systems.", EVT 8 (2008), pp. 1--7.

[25] Chaum, David, "Secret-ballot receipts: True voter-verifiable elections", CryptoBytes 7, 2 (2004), pp. 13--26

[26] Chaum, David and Ryan, Peter YA and Schneider, Steve, A practical voter-verifiable election scheme (Springer, 2005).

[27] Ryan, Peter YA, "A variant of the Chaum voter-verifiable scheme", in Proceedings of the 2005 workshop on Issues in the theory of security (, 2005), pp. 81--88.

[28] Ryan, Peter YA and Schneider, Steve A, Prêt à voter with re-encryption mixes (Springer, 2006).

[29] Fisher, Kevin and Carback, Richard and Sherman, Alan T, "Punchscan: Introduction and system definition of a high-integrity election system", in Proceedings of Workshop on Trustworthy Elections (, 2006).

[30] Essex, Aleks and Clark, Jeremy and Carback III, Richard T and Popoveniuc, Stefan, "The Punchscan voting system", VoComp. http://www. vocomp. org/teams. php (2007).

[31] Popoveniuc, Stefan and Hosp, Ben, "An introduction to Punchscan", in IAVoSS Workshop On Trustworthy Elections (WOTE 2006) (, 2006), pp. 28--30.

[32] Chaum, David and Essex, Aleks and Carback, Richard and Clark, Jeremy and Popoveniuc, Stefan and Sherman, Alan and Vora, Poorvi, "Scantegrity: End-to-end voter-verifiable optical-scan voting", Security & Privacy, IEEE 6, 3 (2008), pp. 40--46.

[33] Chaum, David and Carback, Richard T and Clark, Jeremy and Essex, Aleksander and Popoveniuc, Stefan and Rivest, Ronald L and Ryan, Peter YA and Shen, Emily and Sherman, Alan T and Vora, Poorvi L, "Scantegrity II: end-to-end verifiability by voters of optical scan elections through confirmation codes", Information Forensics and Security, IEEE Transactions on 4, 4 (2009), pp. 611--627.

[34] Chaum, David and Carback, Richard and Clark, Jeremy and Essex, Aleksander and Popoveniuc, Stefan and Rivest, Ronald L and Ryan, Peter YA and Shen, Emily and Sherman, Alan T, "ScantegrityII: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes", EVT8 (2008), pp.1-13.

[35] Rivest, Ronald L, "The ThreeBallot voting system, October 1 2006", Draft online available at time of writing http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf

[36] Rivest, Ronald L and Smith, Warren D, "Three voting protocols: ThreeBallot, VAV, and Twin", in Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology vol. 16, (, 2007).

[37] REGIVALDO, G and ALTAIR, O and CARLOS, A, "A ThreeiBallotiBased Secure Electronic Voting System", (2008).

[38] Norwegian Ministry of Local Government and Regional Development, December 2009. E-vote 2011: Contractor solution specification. Online Feb. 2010.

[39] Norwegian Ministry of Local Government and Regional Development, October 2009. E-vote 2011: System requirements specification. Online Feb. 2010.

[40] Spycher, Oliver and Volkamer, Melanie and Koenig, Reto, "Transparency and technical measures to establish trust in Norwegian Internet voting", in E-Voting and Identity (Springer, 2012), pp. 19--35.

[41] Moran, Tal and Naor, Moni, "Receipt-free universally-verifiable voting with everlasting privacy", in Advances in Cryptology-CRYPTO 2006 (Springer, 2006), pp. 373--392.

[42] Moran, Tal and Naor, Moni, "Split-ballot voting: everlasting privacy with distributed trust", ACM Transactions on Information and System Security (TISSEC) 13, 2 (2010), pp. 16.

[43] Bohli, Jens-Matthias and Müller-Quade, Jörn and Röhrich, Stefan, "Bingo voting: Secure and coercion-free voting using a trusted random number generator", in E-Voting and Identity (Springer, 2007), pp. 111--124.

[44] Bohli, J-M and Henrich, Christian and Kempka, Carmen and Muller-Quade, J and Rohrich, S, "Enhancing electronic voting machines on the example of Bingo voting", Information Forensics and Security, IEEE Transactions on 4, 4 (2009), pp. 745--750.

[45] Bär, Michael and Henrich, Christian and Müller-Quade, Jörn and Röhrich, Stefan and Stüber, Carmen, "Real world experiences with Bingo Voting and a comparison of usability", in IAVoSS Workshop On Trustworthy Elections (WOTE 2008) (, 2008).

[46] Aleksander Essex, Cryptographic End-to-end Variability for Real-world Elections, PHD Thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Doctor of Philosophy in Computer Science, Canada, 2012.

[47] The U.S. Election Assistance Commission, Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems,2010, http://www.fvap.gov/resources/media/eacroadmap.pdf.