Data Science and Pattern Recognition
Ubiquitous International

Volume **1**, Number **1**, February **2017**

A Review of Contemporary E-voting: Requirements, Technology, Systems and Usability

King-Hang Wang, Subrota K. Mondal, Ki Chan, Xiaoheng Xie

Department of Computer Science and Engineering
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong
{kevinw, subrota, kccecia, xiexiaoheng}@ust.hk

Abstract. *E-voting technology has been developed for more than 30 years. However it is still distance away from serious application. The major challenges are to provide a secure solution and to gain trust from the voters in using it. In this paper we try to present a comprehensive review to e-voting by looking at these challenges. We summarized the vast amount of security requirements named in the literature that allows researcher to design a secure system. We reviewed some of the e-voting systems found in the real world and the literature. We also studied how a e-voting system can be usable by looking at different usability research conducted on e-voting. Summarizes on different cryptographic tools in constructing e-voting systems are also presented in the paper. We hope this paper can served as a good introduction for e-voting researches.*
Keywords: Security, System, E-voting, Usability, Survey

1. **Introduction.** Voting is the core pillar to a democratic society. In an election it allows citizens to select their proxies to run the society. In a referendum it allows citizens to make critical decision. Many society resources have been spent to facilitate the exercise of this civil rights. For example, Hong Kong budgeted more than 700 millions for the legislative council election in 2016[1]. Unlike many other applications where information technology was widely adopted to make things efficient, electronic used in voting is not very common in many countries. In US, a country that is relatively open to adopt IT, only DRE and optical scan are adopted in the government election while electronic remote voting system is still running behind. According to Gibson *et al.'s* reviews [39] of the current situation of remote voting systems around the world, the fail of acceptance of e-voting is often due to security - either the system is indeed insecure or it is perceived as insecure by the people.

Secure electronic voting system has been studied in the literature for more than 30 years since David Chaum paper [22]. This topic can be considered as one of the most difficult problems in the security literature. The objective of this paper is to give a comprehensive review on this topic.

We begin with looking at why it is a difficult problem. E-voting involves so many requirements and the literature have not yet arrived on a common set of requirements. Even worst, these requirements are sometime contradicting to each other (for example, verifiable vs receipt-freeness). One of the goals in this paper is to summarize a list out requirements in e-voting. We try to categorize them into core requirements and additional requirements. We recommend anyone who wish to develop an e-voting system should

[1] `http://www.reo.gov.hk/pdf/20162017estimates/reo_estimates_1617-e.pdf`

consider all core requirements and cherry-pick some additional requirements under their environments.

Another reason makes e-voting difficult: an e-voting system is a big and complex system that has many roles, processes. Every role of the system should not be 100 percents trustworthy. Henceforth, any single point of corruption may ruin the system. We give a brief review in the roles and processes involved in an e-voting system by looking into several implementations.

In addition, how people perceive is also important. Apart from the sense of security, an e-voting needs to be usable in order to make it work. Recalling the 2000 US presidential election - the Florida punch hole system rang the alarm to the world about usability issues [2]. In this paper we review some standards in measuring e-voting usabilities.

The bright side is that cryptographers have been working out so many technologies to meet the security requirement individually. This paper review of the popular cryptographic tools, perhaps one may start crafting their scheme by selecting them as some basic building blocks.

The paper is organized as follows. We first look into the requirements of e-voting systems. It is followed by describing the roles, processes that usually involved in e-voting systems. After that we look at the usability issues and see how researchers are measuring it. We will also look at what cryptographic tools have been developed to achieve the security requirements. Then we review some e-voting systems before we conclude the paper.

2. Requirements.

The goal of introducing electronics computation in voting is to enhance the efficiency of traditional paper ballot without compromising existing security, privacy, or legal requirements. The question comes before every e-voting paper in the literature is what are the requirements then. We summarize papers mainly after the year of 2000 and enumerate the requirements they are *explicitly* stated in their papers. By looking at the majority intersection we will be able to learn what is the core requirement to an e-voting system. It is understood that most papers emphasis on the requirements they can achieve, and to highlight their contribution, also include some requirements those are not recognized as core requirements by other literatures. On the other hand, a requirement which is not mentioned by other papers could also mean it is important but hard to be achieved electronically, or it is an undiscovered problem, or it only applies to certain environment, or it is too trivial. Our intention is to provide researchers a general and comprehensive survey. We also recommend researchers to include all **core requirements** in their e-voting schemes, and cherry-pick the other **additional requirements** that fit their environments. The citations given at each of the requirement explicitly states the importance of that requirement in an e-voting system.

2.1. Core Requirements.

- **Correctness (Completeness and Soundness)**. [3, 24, 41, 43, 46, 47, 51, 55, 60, 61, 69, 71, 72, 78, 87] This requirement simply means that the votes should be correctly counted. It can be further broken down into two sub-requirements: completeness and soundness. Completeness [13,62,83,85] means all valid votes need to be counted and Soundness [59] means votes submitted by unauthorized or unauthenticated individual or the ballot itself is invalid should not be counted.
- **Privacy**. [3, 7, 13, 24, 27, 41, 43, 46, 47, 52, 54, 55, 59–63, 67, 69, 71, 72, 78, 83, 85–87] Throughout the voting process none of any voter's ballot choices is known to others except for the voter himself. More precisely, of course we cannot stop a voter to

[2] `http://danbricklin.com/log/ballotusability.htm`

reveal his option. This requirement only states if a voter can follow the protocol and has the ability to keep a secret (e.g. vote-receipt, private key) to himself, then no one including the authority should learn a voter's choices.

Sometime the terms anonymity will be discussed together with privacy as when a voter becomes perfectly anonymous during the voting process, his privacy can also be preserved. In most of the circumstances a voter needs to be authenticated and double voting needs to be prevented, it is unlikely a voter can be perfectly anonymous. For example, the identity of a voter will be authenticated before he receives an anonymous credential after registering with a polling station. It should be noticed that anonymity is different than privacy where privacy conceals only the choices of a voter, but the act of voting or the time of voting are not necessary concealed.

- **Unreusability**. [41, 46, 60, 61, 69, 78, 85, 87] Unreusability means no one shall cast a vote twice. This includes the cases that an attacker tries to clone and casts a ballot which was previously casted by another legitimate voter or a voter re-runs a voting protocol twice. This is sometimes referred to *preventing double-voting*.
- **Eligibility**. [41, 46, 60, 61, 63, 69, 72, 78, 85, 87] Eligibility mainly focus on that only authorized voters can vote. This property is usually implemented by suitable authentication mechanisms. Suffrage, or enfranchisement, the right to vote are definitely important but very seldom mentioned in the e-voting literature when eligibility is defined. For instance an e-voting system using fingerprint authentication may make some disables more difficult to vote.
- **Robustness**. [13, 47, 52, 54, 59, 60, 62, 71, 72, 83, 87] A system is said to be robust if it can properly function with certain amount of misbehaved voters or with partial failure of the system. Usually that would require a distributed system to support fault tolerant.
- **Verifiable**. [3, 7, 13, 24, 27, 40, 41, 46, 47, 52, 54, 59, 61–63, 67, 69, 71, 72, 78, 83, 85–87] Verifiable is an umbrella term to allow someone verifying a particular ballot has been counted. Without further specify, verifiability may be referred as *individual verifiable* such that a voter can verify his vote is being counted or not. More rigid definitions like universal verifiable or E2E verifiable will be described later.
- **Usability**. [2, 4, 9, 11, 14, 16, 26, 32, 36, 42, 46, 53, 64, 70, 73, 77, 81, 83] Usability plays a very important role in determining the success of a system. We gives a more comprehensive review in Section 4.

2.2. **Additional Requirements.**

- **Fairness**. [41, 54, 59–62, 69, 78, 85, 87] A system with fairness should ensure that no partial results will be computed before the end of election. In most of the paper-based ballot used nowadays, the voting boxes are locked. The authority would not be able to count the vote before the end of election. However, exit-poll surveys are legally allowed in some countries so that political parties can hint their supporters to vote strategically.
- **Uncoerability** [7, 24, 27, 41, 43, 46, 59–63, 69, 72, 78, 83, 86, 87] Coercion is about vote buying in the way that the vote buyer is convinced a voter sold his ballot and has voted for some designated choices. It is not restricted to e-voting environment where

chain voting[3] can also happen in paper ballot poll station voting. For mailing based voting coercion is a more severe problem and cannot be solved easily.

E-voting opens more opportunities for coercion owing to 1) voting is usually done remotely; 2) voting needs to be verifiable. Theoretically researchers have done many efforts in tackling the problem like designing scheme that is receipt-freeness (a voter neither obtain or construct a receipt to prove his vote, e.g [43]), coercion-resistant (it is receipt-free even if the vote seller disclose its private key, e.g. [51]), or having coercion-evident (a scheme that have evident that which person is selling votes [40]). However, neither these scheme can prevent if a vote seller simply sends a screen capture to an vote buyer, or letting a vote buyer sitting next to a him during the voting process, or even sells its private key to the vote buyer and let him vote directly. Adida [3] has even put a "coerce me!" button in his system that allows a voter to sell his vote, which highlights the problem of coercion and the difficulty in solving this problem.

- **Efficiency** [13,61,72,83,86] It is measured by the order of complexity of computation, communication especially considers the vast amount of voters and choices.
- **Mobility** [61] It states whether voting can be done using mobile devices. Mobile voting is a trend in nowadays, especially for the business investigation and promotion. At the mean time, it has greater demand for security.
- **Vote-and-Go** [24] It states whether a vote can go offline once after his ballot is casted. In fact some schemes require that all voters to compute at the same time, say generating random secrets [62].
- **Universal Verifiable** [3, 24, 27, 41, 52, 54, 59–61, 67, 69, 71, 72, 78, 83, 85, 87] A voting scheme is said to be universal verifiable if anyone can verify the final voting result is intact. That requirement implies verifiability. One of the way in doing that is to assume the existing of broadcasting channel (like a bulletin board) is available so that when a voter cast his vote, some messages will be sent to all participants and they can assemble the information and verify the result later.
- **E2E-Verifiable** [17, 18, 20, 27, 55, 74] An End-to-End (E2E) verifiable system produces a receipt to a voter that convinces a voter who he has voted without revealing the choice of the vote on the receipt. This is similar to individual verifiability which does not require the generation of receipt.
- **Practicality** [83] This feature requires the system not relying on assumptions that is difficult to realize in large scale scenarios. Some papers assume the existence of untappable channels e.g., [43], some assume all voters to compute at the same time e.g., [62], some assume the use of tamper-resistance devices e.g., [60], some assume an authentic universally accessible memory e.g., [51].

3. Backgrounds.

In this section we provide the backgrounds on what roles and processes are commonly found in an e-voting system.

3.1. Common Roles in e-voting system.

In this section, we show the summary of e-Voting protocol implementation based on the implementation in [6, 8, 29, 50]. The protocol requires the existence of voter, registrar, validator, tallier, and pollster modules. Additional modules may augment the system.

[3]Chain voting can be explained as a voter first smuggled an empty ballot from polling station and filled the ballot with designated choice. The ballot is given to another vote seller who votes the filled ballot. Later he returned the empty ballot that he claimed at the polling office to the vote seller. The vote seller is convinced that vote buyer has indeed casted the filled ballot.

The voter module is responsible for casting vote among the contesting candidates. The registrar is responsible for registering voters prior to an election. The validator is responsible for the validation task, and the tallier is responsible for the tallying and collection tasks. The pollster acts as a voter's agent performing all cryptographic and data transfer functions on a voter's behalf.

1. **Voter**
   A vote consists of selection, generally from a predetermined list of contesting 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. A person who chooses among the contesting candidates and cast vote is a voter. An coercer or adversary can pretend to be a voter. Thus, an authentication system verifies the validity of a voter's credentials attempting to vote and allows to vote who has not voted already.
2. **Registrar**
   The registrar takes a list of people eligible to register and a list of people who have applied to register and whose identities have been verified, and produce a list of registered voters.
   The main difficulty in implementing a registrar lies in verifying the identity of applicants, a task that may be impossible without a face-to-face meeting. The registrar implementation requires that each voter be sent a voter identification number (which need not be secret) and a secret token prior to the registration process.
   Eligible voters generate public/private key pairs and register to vote by sending the registration number and public key. The registrar verifies that the applicants have submitted the correct tokens and adds their identification number public keys to the registered voter list.
3. **Pollster**
   The pollster acts as a voter's agent, presenting human readable ballots to a voter, collecting the voter's responses to ballot questions, performing cryptographic functions on the voter's behalf, obtaining necessary validations and receipts, and delivering ballots to the ballot box.
   The pollster implementation has a simple text user interface. It can display (unvoted) ballots through web browser.
4. **Validator**
   The validator creates a blinded validation certificate by signing a blinded ballot. The voter then unblinds the validation certificate and submits it to the tallier with his or her ballot.
   The validator uses the registered voter list to obtain each voter's public key and check the signatures on their ballots. With this method no record is kept of the order in which ballots are validated.
5. **Tallier**
   Voters submit encrypted ballots signed by the validator to the tallier. The tallier checks the authenticity of the validation and verifies that the encrypted ballot is unique among the encrypted ballots received so far. If the ballot is valid and unique, the tallier issues a signed receipt to the voter. The voter then submits the ballot decryption key. The tallier uses the key to decrypt the ballot. After the election, the tallier publishes a list of encrypted ballots, decryption keys, and decryption ballots, allowing for independent verification of election results.

For maximum security and privacy, the validator and tallier modules might be run on separate machines and the pollster module might not be run on a machine that houses any of the other modules.

3.2. **Generic Electronic Voting Phases/Stages.** There exists a wide variety of voting/electoral processes. The electoral process is all that concerns to the realization of an election. The end-to-end voting process is divided into several phases or stages [29, 50] which are identified as follows:

1. **Registration/Preparation:** This phase involves compiling a list of people eligible to vote. In addition, the ballots are prepared and all the logistics arrangements or the activities needed for the election are accomplished.
2. **Validation:** Involves verifying the credentials of the voters attempting to vote and only allowing the registered voters who have not already voted to proceed.
3. **Collection:** Involves collecting the voted ballots.
4. **Verification:** The validity of the ballots are verified. Only the valid ballots are used in the tallying phase.
5. **Tallying:** This phase involves in counting the valid votes. At the end the tally is published.
6. **Claiming:** All the claims (if any) are investigated. In addition, in this phase auditing is done. At the end of this phase the final results are published.

The above are the generic phases followed by most of e-voting systems. There might be e-voting schemes that may have stages more or less. It is essential to consider ways in which the phases mentioned above can be carried out accordingly while designing and implementing an e-voting system without sacrificing voters' privacy or introducing opportunities for corruption. In addition, it is important to ensure or satisfy all desirable standard polling system properties or requirements [29, 50].

4. **Usability.** Different technical innovations have been actively investigated and implemented while researchers demonstrated that the proposed approaches can fulfill the technical requirements and hence are the prominent solutions for successful e-voting systems.

Besides these important technical aspects, another important issue is the voter's perceptions towards e-voting systems. As indicated in Voluntary Voting System Guidelines (VVSG) [33] and a report from the U.S. Vote Foundation [32], usability, i.e. the user's willingness to use a system or not, is one of the most important requirements for voting systems. Accessibility and usability requirements are also listed in the development specification in the Norwegian E-vote 2011 project. The importance of usability testing on voting systems are also agreed by various researchers [11, 26, 42, 70, 81].

Problems with usability in voting systems have led to controversy in the US presidential election in year 2000 [11] and the re-elections of the Finnish municipal elections on the 26th October, 2008 [35]. Therefore, the ability of voters to vote as they intend is one of the factors influencing the election outcomes. Since then there were raising concerns in different governments on usability and accessibility issues, for example, Help America Vote Act (HAVA) in the United State and the Norwegian Discrimination and Accessibility Act. Besides, both VVSG and WCAG (Web content accessibility guidelines) [**?**] mentioned the needs of improving the accessibility for the disabled on e-voting systems and web-based systems respectively. In VVSG, it is explicitly indicated that the usability tests have to be performed on voting systems, while minimizing the cognitive, perceptual, interaction difficulties of the voting process.

4.1. **ISO 9241-11 Standard: Guidance on Usability.** Volkamer et al. [82] discussed the importance of evaluating e-voting system according to international standards to enhance the trust of voters. ISO 9241-11 [48] has been frequently employed to evaluate e-voting systems' usability. It is recommended in the National Institute of Standards and Technology (NIST)'s report to US Congress on voting systems [58]. The ISO 9241-11 standard defines the usability as:

> The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

According to the NIST's report, there are three components of usability:

- Effectiveness - the accuracy and completeness that users can achieve specified goals
- Efficiency - the resources for users to achieve the goals accurately and completely
- Satisfaction - the users' subjective comfort and acceptability of the results

Olembo and Volkamer [70] have summarized the commonly used measurements for the three components. Error rate measuring the percentage and accuracy of completed user tasks is used for effectiveness. Time required by users on performing the tasks are commonly used for measuring efficiency. Some other approaches are also adopted to measure efficiency, such as the mental or physical efforts, materials or financial costs required for the user tasks. For example, the average number of interactions between the user and the voting systems such as the number of clicks required for users to vote on a remote voting system can be a measure of efficiency [80]. For measuring satisfaction, subjective satisfaction questionnaires, such as Software Usability Measurement Inventory (SUMI) [56], System Usability Scale (SUS) [10], and Questionnaire for User Interface Satisfaction (QUIS) [23] can be employed.

Since ISO 9241-11 was published in 1998, the rapid development of web and information technologies and the change in users' requirements have led to the need of revising the standard. According to Bevan et al. [12], the revision will need to consider the three components of usability as outcomes of interaction with the system rather than just as measurements. Also, they mentioned that the revision will include more specific aspects of outcomes. The revision of ISO 9241-11 may affect the evaluation of usability for e-voting systems in the future.

4.2. **Usability Testing Methods or Techniques.** Various methods and techniques can be employed in evaluating usability. Many of these come from the commonly used techniques in human computer interaction (HCI). Some examples are expert review, focus group interviews, personas, user testing. Focus group interviews can be carried under certain scenarios or prototypes. Expert review can be either a cognitive walkthrough or heuristic review. User testings can be lab studies, i.e. under a controlled environment or field studies, i.e. under an uncontrolled environment. Usually, data for the studies or the testings are collected from observations, such as audio or video recording, data from log files and questionnaires.

4.3. **Related Works.** Various researches have been carried in studying and evaluating the usability of e-voting systems.

Important usability issues are identified by comparing different e-voting systems. Through these comparison studies, usability issues, such as the relation between voters' efforts and satisfactions, the confidence of voters, can be discovered.

Bederson et al. [11] compared several direct recording electronic (DRE) systems through the analysis from expert reviews, the comments from close observations and the questionnaires from field studies. The questionnaire they used consists of six questions in a scale

of 1 to 9. Voters were asked about their overall impression, the comfortness, the easyness to use and the trustyness of the systems.

Conrad et al. [26] compared six e-voting systems with different design approaches such as ATM-style touch screens, zoomable interface, optical scan. The six systems are Diebold AccuVote-TS and Avante Vote-Trakker, UMD Zoomable, Hart Intercivic eSlate, Nedap LibertyVotey and ES&S Model 100. They measured the process, accuracy and satisfaction with 42 participants which they specifically oversampled participants with limited computer experience and older in age. Process is measured by the number of voting actions and the time required to cast a vote. Accuracy is measured by the error between voters' intentions and the actual casted votes. Satisfaction was again measured by questionnaires on the ease, comfort of use, readability, confidence, etc.

In a paper by U.S. Vote Foundation [66], usability is one of the three major requirements for internet voting. They compared three internet voting systems, namely, Helios, Star-Vote 1, and Star-Vote 2. They interviewed a focus group of 27 participants. The interviews were audio recorded, process were screen captured and questions were asked. They identified some challenges and issues in internet voting systems, for example, voter verification was not understood or cared by voters.

Some other researches focused on evaluating the usability on one particular system. Besselaar et al. [81] evaluated an e-voting system by performing field experiments in different environments, including in Orsay of Paris, at Carpenters Estate in London, and in different community networks in Italy, Milan and Finland. Through the questionnaires collected, they demonstrated that issues other than technical ones have to be considered. They showed that poor design, in particular on insufficient usability, may lower the participation.

Prosser et al. [73] recognized the importance of user's acceptance towards and their ability to use a two-stage e-voting. They evaluated the procedures by three aspects. First, they traced the number and types of help requests from votes. Second, they recorded the number of votes using the recovery function. Finally, they obtained voter's user experience from a web questionnaire of five questions. Four questions are in Likert scale to collect voters' perception, e.g. whether it is easy to use and how confident they have voted correctly. The fifth question is an yes/no question to see if the voter has used the help information or not.

Recently, more and more researches are adopting the ISO 9241-11 standard in evaluating all the three components of usability. Acemyan et al. [2] compared three E2E voting systems in measuring both the voting and the verification process. Campbell et al. [16] compared a smartphone voting system against traditional voting platforms. Budurushi et al. [14] evaluated the EasyVote voting scheme in complex elections while Holmes et al. [44] evaluated the Vote-By-Phone, an interactive voice response (IVR) system. All of them evaluate the efficiency by measuring the time spent in specific voting processes and the satisfaction by SUS. For effectiveness, Acemyan et al. measured the inability of votes to cast a vote or verify the vote, the per-contest error rate and overall ballot error rate. Budurushi et al. observed the number of users who are able to complete the tasks while Holmes et al. and Campbell et al. measured the error rates.

When most of the studies on usability only focused on the general public, Fuglerud et al. [36] carried user testing including a wide range of disabled user groups with errors and subjective impressions collected.

5. **Technologies used in constructing E-voting system.** Most of the e-voting technologies we found in the literature are based on cryptography. Each of them may have different constructs to fit different requirements and features. Usually researchers [43, 54, 60]

classify them into three main categories as *Mix-net*, *Homomorphic Encryption*, and *blind signature*. Sometimes the taxonomies will also include *ring signature* [24, 62] or *secret sharing* [62]. In fact an e-voting system can be rather complicated and requires more than one cryptographic tools. We introduce some of these tools as follows.

5.1. **Mix-net.** Mix-net proposed by Chaum in 1981 [22] is always cited as the pioneer in E-voting in the literature. Subsequently works including [1, 3, 13, 21, 40, 49, 51, 54, 59, 60, 68, 86] have used Mix-net or its varient in their constructs. The idea of a mix-net, or more specific, a re-encryption mix-net, is to perform a re-encryption over a set of ciphertext and shuffle the order of those ciphertext. By means of re-encryption, the mix-net (or a shuffle agent) needs not decrypt the ciphertext, but to use the authority public key and transform the ciphertext into another number where the decryption of this ciphertext remains unchange. By cascading several shuffle agents, the original order of the ciphertext would not be known and thus the authorithy will be unable to trace the originality of the ciphertext. In the e-voting context, ballots are treated as ciphertext and be collected by different shuffle agents. These agents collect and mix the ballot and the authority is therefore unable to relate a ballot to a voter. It should be noticed that there is an assumption in using a mix-net – at least one shuffle agent is trustworthy in the sense that they would not collude to relate voters and their ballots. We say a mix-net is *robust* if it can provide evident to convince a voter to his ballot is indeed re-encrypted rather than being discarded or replaced. However, such a evident may not bring the system be not *receipt-freeness* and allow voters to reveal their ballot to vote buyers.

5.2. **Homomorphic Encryption.** The term homomorphic encryption has two meanings in the e-voting literature. The first one [24,43] means a *homomorphism* of a ciphertext, or with our terminology, a re-encryption. The second one [54, 62], which we are using here, allows one to aggregate ciphertexts without decrypting them [38]. Take a oversimplified example, a ciphertext encrypted using RSA $C_1 = m_1^e \ mod \ n$ aggregates with another ciphertext $C_2 = m_2^e \ mod \ n$ by $C_1 \times C_2 = (m_1 m_2)^e \ mod \ n$ so that the new ciphertext is indeed the aggregation of two and the decryption of this ciphertext would be $m_1 m_2$. The homomorphic property allows each encrypted ballot to be aggregated by an agent before tallying at the authority [28,31,54]. In the above oversimplified example, one may encode each candidate's number as a prime larger than 2. It is possible to aggregate at most k ballots such that $g^k < n$ where g is the largest prime used by the candidates. Since ballots are aggregated without decryption, we may have an agent to aggregate the ballots before submitting the ballots to the authority.

5.3. **Secret Sharing.** If homomorphic encryption is to conceal a ballot by *adding up*, secret sharing is to do it by *breaking down*. Secret sharing [76], sometime referred to a threshold system, is a cryptographic tool that allows a group of at least k members holding shares to decrypt a cipher while group less than k member would be unable to decrypt it. Take an oversimplified example, the y-intersect of a $k-1$-degree polynomial is the private key to decrypt a message. Each member holds one unique coordinate of the polynomial. It would be impossible to reconstruct the polynomial and compute the private key unless there are at least k members work together. Secret sharing is commonly used in a multiple agents or multiple authorities setting [30, 41, 47, 60, 62, 67, 78, 83, 87]. It is rested on the assumption that these agents/authorities would not all collude together in the middle of the election to partial tally, or to reveal an individual ballots.

5.4. **Blind Signature.** Schemes [37, 46, 50, 63] use blind signature to assert the inclusion of a ballot while maintaining the voter's privacy. A blind signature [37] assumes interactions between a requester and a signer. A requester may demand a signature from

a signer on a document where the content of the document is concealed to the signer. When it is used in e-voting context, a voter will demand the authority to blindly sign on a concealed ballot. The voter then casts the unblinded ballot anonymously. In the tally phasing all anonymous vote will be published. If a voter cannot find his vote under a possibly exclusion of his vote, he can present an evident of the blinded ballot was signed by the authority.

5.5. **Anonymous Submission.** An anonymous submission scheme allow someone to contribute its input in a vector without letting other knowing where it is submitted to. This technique was borrowed in e-voting [62, 85]. Before the voting starts, voters jointly run a protocol to obtain an unique *position* in a vector for each voter. The position obtained by each voter is confidential to the others. The voter then casts its real ballot into its position and dummy ballot into other positions. At the tally stage, each voter can verify the decryption of its position is indeed its own ballot.

5.6. **Zero-knowledge Proof.** Zero-knowledge Proof has been used extensively in e-voting schemes [24, 30, 40, 52, 54, 55, 68, 78, 83] for verification purposes. A zero-knowledge proof protocol allows a prover to demonstrate a statement is indeed what it is claimed without revealing any addition knowledge about it. Taken into e-voting context, a proof needs to be zero knowledge for different reasons. For example, a voter verifies its vote is being counted but no additional info he can receive to prove to his vote buyer. For example, in a blind signature based system the authority requires the voter to prove the blind ballot is valid/confined with certain format.

5.7. **Deniable Signature / Designated Verifier Signature.** Deniable Signatures [61, 79] allow a signer to send a signed message to a designated verifier who can be convinced that the message is composed by the signer and the signer can later deny the signature to other verifiers by composing another entirely different message but with the same signature. Designated Verifier Signatures (DVS) [45] share similar logic as deniable signature while in a DVS scheme the verification of message requires the secret key of a designated verifier. This technique allows a voter to convince an authority a ballot is indeed sent by this voter while the voter can deny this ballot to any vote buyers to prevent any sort of coercion. Hirt [43] differentiated the incoercibility and the *deniability* of a denialable signature or a DVS which "only allows a voter to lie about his vote, but it cannot help against a voter who wants to make his encryption undeniable." Designated Verifier Re-encryption Proof [43, 59] is a variant of DVS used in the literature that allows only a designated verifier to validate a message is indeed a re-encryption of another ciphertext.

6. **Review of Electronic Voting Systems.** In this section, we briefly show the analysis of some existing e-voting systems. In general, this review helps us to know which e-voting system uses which technology in its implementation, which requirements are satisfied, and what are the limitations. In particular, it reveals us which e-voting system is the ideal to employ/adopt or how we can satisfy almost all the requirements of an ideal e-voting system in an easier manner of implementation.

1. **DRE:** One of the present-day e-voting systems is the touch screen system, referred to as Direct Recording Electronic Systems (DRE) [5]. DRE is considered the first full computer based e-voting system. A DRE machine implements most of steps in the voting process from registration to tallying. DRE systems consist of buttons and areas on the touch screen. Voters get a PIN or smart card by showing their ID to the election authority. They access the DRE machine by using the PINs or smart cards. Voter makes his/her choice and after that DRE machine shows the

choices on the screen and finally gives the voter an opportunity to change his/her choice or submit the choice. 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 e-voting machines [57]. 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 [65, 84].

2. **Sensus:** A well known e-voting protocol presented by Cranor *et al.*. [29]; a security-conscious e-voting system over computer networks. It uses blind signatures to ensure that only registered voters can vote and that each registered voter only votes once, while at the same time maintaining voters' privacy, but does nothing to prevent a voter from proving that he or she voted in a particular way. Sensus allows voters to verify independently that their votes were counted correctly and anonymously, but it is not possible for any interested party to verify that all votes were counted correctly. Even satisfying most of the security requirements of an e-voting system, Sensus suffers from a vulnerability issues that allows one of the entities involved in the election process to cast its own votes in place of those that abstain from the vote.
3. **REVS:** Robust Electronic Voting System (REVS) [50] is a voting system that was designed for distributed and faulty environments, namely the Internet. REVS is an e-voting system that accomplishes the desired characteristics of traditional voting systems, such as accuracy, democracy, privacy and verifiability. REVS also deals with failures in real world scenarios, such as machine or communication failures, which can lead to protocol interruptions, allowing a secure voting process even in a faulty environment. REVS defends failures by keeping a distributed loosely-coupled state. Each voter keeps a local state in mobile non-volatile storage allowing to stop and resume the election anytime and anywhere.
4. **Civitas:** Civitas [25] is the first e-voting system that allows voters to vote securely from the remote client of their choice, while providing universal verifiability, voter verifiability, anonymity, integrity, and coercion resistance. It utilizes a publicly viewable log service such as a bulletin board to record all the information needed for verifiability of the election. A variety of zero-knowledge proofs are used to enforce the compliance of protocol execution. In order to resist coercion, a voter has to use his designated private key and run an algorithm to generate fake credentials. The voter provides these fake credentials in case of coercion from adversaries. All the votes submitted through fake credentials are eliminated, and the re-voting depends on the policy specified by the supervisor. Civitas can scale up to a large number of voters, with a low marginal computational cost per voter.
5. **PunchScan:** It is an optical scan, cryptographic voting system [17] that is easy to use by the voter as well as by election officials [34]. The system offers voter-verifiability, integrity, privacy, and transparency. It provides an end-to-end audit mechanism and issues a ballot receipt to each voter while retaining/preserving voter-privacy, ballot-secrecy, integrity, coercion resistance and so on.
6. **Scantegrity:** Scantegrity [20] is a successor of PunchScan [17] that meets industry standard by providing end-to-end verifiability of election results. It uses privacy preserving confirmation codes to allow each voter to prove that the vote is included unmodified in the final tally.

   An enhanced version of Scantegrity is introduced and named as Scantegrity II [19]. It increases election integrity, improves usability, and disputes resolution through the novel use of confirmation codes printed on ballots in invisible ink. Unlike in

Scantegrity, dispute resolution neither relies on paper chits nor requires election officials to recover particular ballot forms. Scantegrity II works with either precinct-based or central scan systems.

7. **VoteBox:** VoteBox [75] is a complete e-voting system with minimized software stack that follows DRE-style voting system with additional security measures. It utilizes a distributed broadcast network and replicated log for providing robustness and audit-ability in case of failure, misconfiguration, or tampering. The system supports end-to-end verifiability which assures voters that votes are cast as intended and counted as cast. In addition, the vote decryption key can be broken into shares and can be distributed to several mutually-untrusted parties, such as representatives of each candidate, driving them to cooperate to view the final tally. VoteBox is receipt free and allows voters to verify their votes. In addition, coercion resistance and privacy are achieved.
8. **Prêt à Voter:** It is an end-to-end auditable e-voting system devised by Ryan *et al.* [74]. Uses paper based ballot forms that are converted to encrypted receipts to provide accuracy of the count and ballot privacy, at the same time avoids the dangers of vote buying. In this approach, vote is encoded using a randomized candidate list. The randomisation of the candidate list on each ballot form ensures the secrecy of each vote whilst getting rid of any bias towards the top candidate that can occur with a fixed ordering. A voter can visit the Web Bulletin Board (WBB) after the election and confirms the receipt appear correctly. All the stages in this approach are posted to the WBB and can be audited.
9. **Helios:** It is a web based cryptographic auditing voting system [3]. In this system voters casts their votes using web browsers. It protects the secrecy of a vote. Vote is encrypted inside the browser, before it is even sent to the server. This scheme assures anonymity of ballots using mixnets. It also ensures verifiability; voters can verify that ballots are received and tallied appropriately. It further preserves universal verifiability which is called open-audit in their paper. Note that Helios does not take any attempt to solve the coercion problem; is meant only for low coercion elections.
10. **M-SEAS:** Mobile Secure E-voting Applet System (M-SEAS) presents a mobile implementation of an e-voting system [15]. The authors show the portability of an e-voting protocol based on the Sensus protocol [29] and already defined for polling from a fixed location [8] on mobile devices. M-SEAS has fixed the well-known vulnerability issues of Sensus protocol. They use 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 further uses a formal verification technique to validate the security properties of the system.

A quick summary of the technologies used by each of the system is shown in Table 6

7. **Conclusion.** In this paper, we have presented a comprehensive review on the current state of the art of e-voting systems. In order to make e-voting systems be more adoptable in real world, we believe persistent force needs to be exerted in several directions. From cryptography there are many rooms to improve and meet this high dimension multiple constraints problem. In particular, enabling strong privacy notion with uncoercibility is a very challenging task. From system implementation perspective, a robust and verifiable paradigm needs to be established. The system needs to be examined to be secure and usable, without too many unnecessary assumptions or hardware supports. Once it is in place, it may first be used in some causal environment as to educate people and also to gain trust from people. We believe with the effort from the research community, large scale of e-voting adoption will happen in the future.

TABLE 1. A summary of some e-voting systems and the core technologies being used. Some of the system are working towards improving existing paper-based or DRE based voting while some implement remote voting systems.

System Name	References	Core Technologies
DRE	[5, 57, 65, 84]	By proprietary
Sensus	[29]	Blinded Signature
REVS	[50]	Blinded Signature
Civitas	[25]	Mixnet
PunchScan	[17, 34]	Punching Paper
Scantegrity	[19, 20]	Invisible Ink on Paper Ballot
VoteBox	[75]	Homomorphic Encryption
Prêt à Voter:	[74]	Mixnet
Helios	[3]	Mixnet
M-SEAS	[15]	Blind signature

REFERENCES

[1] M. Abe and F. Hoshino, "Remarks on mix-network based on permutation networks," *Lecture Notes in Computer Science*, pp. 317–324, 2001.

[2] C. Z. Acemyan, P. Kortum, M. D. Byrne, and D. S. Wallach, "Usability of voter verifiable, end-to-end voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II," *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, vol. 2, pp. 26–56, 2014.

[3] B. Adida, "Helios: web-based open-audit voting," *The International Conference on Security Symposium*, pp. 335–348, 2008.

[4] M, Al-Ibrahim and J, Al-Ostad, "The usability, creditability and security of e-voting system in education sector," *The International Conference on e-Education, e-Business, e-Management and e-Learning IPEDR*, vol. 27, pp. 111-115, 2012.

[5] A. A. Altun and M. Bilgin, "Web based secure e-voting system with fingerprint authentication," *Scientific Research and Essays*, vol. 6(12), pp. 2494–2500, 2011.

[6] R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," *IEEE International Conference on E-Commerce Technology and IEEE International Conference on Enterprise Computing, E-Commerce and E-Services*, pp. 382–392, 2007.

[7] M. Backes, M. Gagné, and M. Skoruppa, "Using mobile device communication to strengthen e-voting protocols," *ACM workshop on Workshop on Privacy in the Electronic Society*, pp. 237–242, 2013.

[8] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli, "Seas, a secure e-voting protocol: design and implementation," *Computers & Security*, vol. 24(8), pp. 642–652, 2005.

[9] D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna, "An experience in testing the security of real-world electronic voting systems," *IEEE Transactions on Software Engineering*, vol. 36(4), pp. 453–473, 2010.

[10] A. Bangor, P. T. Kortum, and J. T. Miller, "An empirical evaluation of the system usability scale," *International Journal of Human–Computer Interaction*, vol. 24(6), pp. 574–594, 2008.

[11] B. B. Bederson, B. Lee, R. M. Sherman, P. S. Herrnson, and R. G. Niemi, "Electronic voting system usability issues," *The SIGCHI Conference on Human Factors in Computing Systems*, pp. 145–152, 2003.

[12] N. Bevan, J. Carter, and S. Harker, "ISO 9241-11 Revised: What Have We Learnt About Usability Since 1998?," *Lecture Notes in Computer Science*, pp. 143–151, 2015.

[13] D. Boneh and P. Golle, "Almost entirely correct mixing with applications to voting," *ACM Conference on Computer and Communications Security*, pp. 68–77, 2002.

[14] J. Budurushi, K. Renaud, M. Volkamer, and M. Woide, "An investigation into the usability of electronic voting systems for complex elections," *Annals of Telecommunications*, vol. 71(7), pp. 309–322, 2016.

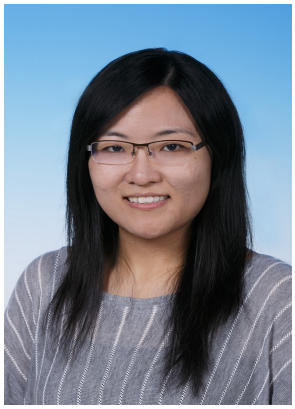
[15] S. Campanelli, A. Falleni, F. Martinelli, M. Petrocchi, and A. Vaccarelli, "Mobile implementation and formal verification of an e-voting system," *The International Conference on Internet and Web Applications*, pp. 476–481, 2008.
[16] B. A. Campbell, C. C. Tossell, M. D. Byrne, and P. Kortum, "Toward more usable electronic voting testing the usability of a smartphone voting system," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 56, pp. 973–985, 2014.
[17] R. T. Carback, S. Popoveniuc, A. T. Sherman, and D. Chaum, "Punchscan with independent ballot sheets: Simplifying ballot printing and distribution with independently selected ballot halves," *The IAVoSS Workshop on Trustworthy Elections*, 2007.
[18] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *CryptoBytes*, vol. 7(2), pp. 13–26, 2004.
[19] D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. Ryan, E. Shen, and A. .T Sherman, "Scantegrity ii: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes," *EVT*, vol. 8, pp. 1–13, 2008.
[20] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, "Scantegrity: End-to-end voter-verifiable optical-scan voting," *IEEE Security & Privacy*, vol. 6(3), pp. 40–46, 2008.
[21] D. Chaum, P. Y. Ryan, and S. Schneider, "A practical voter-verifiable election scheme," *European Symposium on Research in Computer Security*, pp. 118–139, 2005.
[22] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol.24(2), pp. 84–90, 1981.
[23] J. P. Chin, V. A. Diehl, and K. L. Norman, "Development of an instrument measuring user satisfaction of the human-computer interface," *SIGCHI Conference on Human Factors in Computing Systems*, pp. 213–218, 1988.
[24] S. S. Chow, J. K. Liu, and D. S. Wong, "Robust receipt-free election system with ballot secrecy and verifiability," *The Network and IT Conference: NDSS*, vol. 8, pp. 81–94, 2008.
[25] M. R. Clarkson, S. Chong, and A. C. Myers, "Civitas: A secure voting system," *Technical report*, Cornell University, 2007.
[26] Frederick G. Conrad, Benjamin B. Bederson, Brian Lewis, Emilia Peytcheva, Michael W. Traugott, Michael J. Hanmer, Paul S. Herrnson, and Richard G. Niemi, "Electronic voting eliminates hanging chads but introduces new usability challenges," *International Journal of Human Computer Studies*, vol. 67(1), pp. 111–124, 2009.
[27] V. Cortier, "Formal verification of e-voting: solutions and challenges," *ACM SIGLOG News*, vol. 2(1), pp. 25–34, 2015.
[28] R. Cramer, R. Gennaro, and B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," *The annual International Conference on Theory and Application of Cryptographic Techniques*, pp. 103–118, 1997.
[29] L. F. Cranor and R. K. Cytron, "Sensus: A security-conscious electronic polling system for the internet," *The Hawaii International Conference on System Sciences*, vol. 3, pp. 561–570, 1997.
[30] I. Damgård, M. Jurik, and J. B. Nielsen, "A generalization of paillier's public-key system with applications to electronic voting," *International Journal of Information Security*, vol. 9(6), pp. 371–385, 2010.
[31] J. Dossogne and F. Lafitte, "Blinded additively homomorphic encryption schemes for self-tallying voting," *The International Conference on Security of Information and Networks*, pp. 173–180, 2013.
[32] S. Dzieduszycka-suinat, J. Murray, J. R. Kiniry, D. M. Zimmerman, D. Wagner, P. Robinson, A. Foltzer, and S. Morina, "The future of voting: End-to-end verifiable internet voting - specification and feasibility study," Technical report, U.S. Vote Foundation, July 2015.
[33] Election Assistance Commission (EAC), Voluntary voting system guidelines, 2015. `http://www.eac.gov/testing_and_certification/voluntary_voting_system_guidelines.aspx` (Accessed on 8th September, 2016).
[34] A. Essex, J. Clark, R. Carback, and S. Popoveniuc, "Punchscan in practice: An e2e election case study," *The Workshop on Trustworthy Elections*, 2007.
[35] E. Felten, "Finnish court orders re-vote after e-voting snafu," Accessed on 8th September, 2016.
[36] K. Skeide F. and T. H. Røssvoll, "An evaluation of web-based voting usability and accessibility," *Universal Access in the Information Society*, vol. 11(4), pp. 359–373, 2012.
[37] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," *Advances in Cryptology-AUSCRYPT*, pp. 244–251, 1992.
[38] C. Gentry, "A fully homomorphic encryption scheme," PhD thesis, Stanford University, 2009.

[39] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of e-voting: the past, present and future," *Annals of Telecommunications*, pp. 1–8, 2016.
[40] G. S. Grewal, M. D. Ryan, S. Bursuc, and P. Y. Ryan, "Caveat coercitor: Coercion-evidence in electronic voting," *IEEE Symposium on Security and Privacy*, pp. 367–381, 2013.
[41] R. Haenni, R. Koenig, S. Fischli, and E.c Dubuis, "TrustVote: A proposal for a hybrid e-voting system," Technical report, Bern University of Applied Sciences, Höheweg, August 2009.
[42] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, and M. Traugott, "The importance of usability testing of voting systems," *The USENIX/Accurate Electronic Voting Technology Workshop*, pp. 3–3, 2006.
[43] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 539–556, 2000.
[44] D. Holmes and P. Kortum, " Vote-by-phone usability evaluation of an ivr voting system," *The Human Factors and Ergonomics Society Annual Meeting*, vol. 57, pp. 1308–1312, 2013.
[45] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Efficient strong designated verifier signature schemes without random oracle or with non-delegatability," *International Journal of Information Security*, vol. 10(6), pp. 373–385, 2011.
[46] M. S. Hwang, Y. C. Lai, and C. T. Li, "A verifiable electronic voting scheme over the internet," *International Conference on Information Technology: New Generations*, pp. 449–454, 2009.
[47] S. Iftene, "General secret sharing based on the chinese remainder theorem with applications in e-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, pp. 67–84, 2007.
[48] British Standards Institution, "Ergonomic requirements for office work with visual display terminals (vdts).: Guidance on usability," Standard, 1998.
[49] M. Jakobsson, A. Juels, and R. L. Rivest, "Making mix nets robust for electronic voting by randomized partial checking," *USENIX security symposium*, pp. 339–353, 2002.
[50] R. Joaquim, A. Zúquete, and P. Ferreira, "REVS–a robust electronic voting system," *IADIS International Journal of WWW/Internet*, vol. 1(2), pp. 47–63, 2003.
[51] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," *ACM workshop on Privacy in the Electronic Society*, pp. 61–70, 2005.
[52] J. Katz, S. Myers, and R.l Ostrovsky, "Cryptographic counters and applications to electronic voting," *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 78–92, 2001.
[53] G. E. Kennedy and Q. I. Cutts, "The association between students' use of an electronic voting system and their learning outcomes," *Journal of Computer Assisted Learning*, vol. 21(4), pp. 260–268, 2005.
[54] A. Kiayias and M. Yung, "The vector-ballot e-voting approach," *The International Conference on Financial Cryptography*, pp. 72–89, 2004.
[55] A. Kiayias, T. Zacharias, and B. Zhang. "Demos-2: scalable e2e verifiable elections without random oracles," *ACM SIGSAC Conference on Computer and Communications Security*, pp. 352–363, 2015.
[56] J. Kirakowski and M. Corbett, "Sumi: the software usability measurement inventory," *British Journal of Educational Technology*, vol. 24(3), pp. 210–212, 1993.
[57] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," *IEEE Symposium on Security and Privacy*, pp. 27–40, 2004.
[58] S. J. Laskowski, M. Autry, J. Cugini, W. Killam, and J. Yen, "Improving the usability and accessibility of voting systems and products," Technical report, National Insitute of Standards and Technology, 2004.
[59] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Providing Receipt-Freeness in Mixnet-Based Voting Protocols," *Lecture Notes in Computer Science*, pp. 245–258, 2003.
[60] B. Lee and K. Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," *The International Conference on Information Security and Cryptology*, pp. 389–406, 2002.
[61] C. T. Li, M. S. Hwang, and C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile ad hoc networks," *Computer Communications*, vol. 31(10), pp. 2534–2540, 2008.
[62] H. Li, Y. Sui, W. Peng, X. Zou, and F. Li, "A viewable e-voting scheme for environments with conflict of interest," *IEEE Conference on Communications and Network Security*, pp. 251–259, 2013.
[63] L. López-García, L. J. Dominguez Perez, and F. Rodríguez-Henríquez, "A pairing-based blind signature e-voting scheme," *The Computer Journal*, vol. 57(10), pp. 1460-1471, 2013.
[64] D. M. Namara, J. P. Gibson, and K. Oakley, "The ideal voting interface: Classifying usability," *Journal of eDemocracy and Open Government*, vol. 6(2), 2014.
[65] R. T. Mercuri, "Electronic vote tabulation checks and balances," Dissertation, University of Pennsylvania, 2001.

[66] J. Murray and K. Instone, "The future of voting: End-to-end verifiable internet voting - usability study report," http://www.usvotefoundation.org/E2E-VIV/usability-study.pdf (Accessed on 8th September, 2016).
[67] D. G. Nair, V. P. Binu, and G. S. Kumar, "An improved e-voting scheme using secret sharing based secure multi-party computation," *Computing Research Repository*, abs/1502.07469, 2015.
[68] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," *ACM conference on Computer and Communications Security*, pp. 116–125, 2001.
[69] T. A. T. Nguyen and T. K. Dang, "Enhanced security in internet voting protocol using blind signature and dynamic ballots," *Electronic Commerce Research*, vol. 13(3), pp. 257–272, 2013.
[70] M. M. Olembo and M. Volkamer, "E-voting system usability: Lessons for interface design, user studies, and usability criteria," *Human-Centered System Design for Electronic Governance*, pp. 172–201, 2013.
[71] K. Peng and F. Bao, "A design of secure preferential e-voting," *The International Conference on E-Voting and Identity*, pp. 141–156, 2009.
[72] C. Porkodi, R. Arumuganathan, and K. Vidya, "Multi-authority electronic voting scheme based on elliptic curves," *International Journal of Network Security*, vol. 12(2), pp. 84–91, 2011.
[73] A. Prosser, K. Schiessl, and M. Fleischhacker, "E-voting: Usability and acceptance of two-stage voting procedures," *The International Conference on Electronic Government*, pp. 378–387, 2007.
[74] P. Y. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, "Prêt à voter: a voter-verifiable voting system," *IEEE Transactions on Information Forensics and Security*, vol. 4(4), pp. 662–673, 2009.
[75] D. Sandler, K. Derr, and D. S. Wallach, "VoteBox: A tamper-evident, verifiable electronic voting system," *The International Conference on Security Symposium*, pp. 349–364, 2008.
[76] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22(11), pp. 612–613, 1979.
[77] M. A. Smith, S. S. Monfort, and E. J. Blumberg, "Improving voter experience through user testing and iterative design," *Journal of Usability Studies*, vol. 10(4), pp. 116–128, 2015.
[78] O. Spycher, R. Haenni, and E. Dubuis, "Coercion-resistant hybrid voting systems," *Electronic Voting*, pp. 269–282, 2010.
[79] H. M. Sun, K. H. Wang, S. Y. Chang, and L. Wan, "An authentication protocol combining deniability and forward secrecy for resisting adaptive attacks," *Information Security Conference*, 2006.
[80] S. J. Swierenga and G. L. Pierce, "Accessible voting systems usability measures," *Journal on Technology and Persons with Disabilities*, pp. 146–154, 2013.
[81] P. V. d. Besselaar, A. M. Oostveen, F. D. Cindio, and D. Ferrazzi, "Experiments with e-voting technology: experiences and lessons," *Building the Knowledge Economy: Issues, Applications, Case Studies*, pp. 719–726, 2003.
[82] M. Volkamer, O. Spycher, and E. Dubuis, "Measures to establish trust in internet voting," *The International Conference on Theory and Practice of Electronic Governance*, pp. 1–10, 2011.
[83] S. Weber, "A coercion-resistant cryptographic voting protocol-evaluation and prototype implementation," *Darmstadt University of Technology, http://www.cdc.informatik.tudarmstadt.de/reports/reports/StefanWeber.diplom.pdf*, 2006.
[84] K. Weldemariam and A. Villafiorita, "A survey: Electronic voting development and trends," *Electronic Voting*, pp. 119–131, 2010.
[85] X. Zou, H. Li, Y. Sui, W. Peng, and F. Li, "Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties," *IEEE Conference on Computer Communications*, pp. 136–144, 2014.
[86] A. Zúquete and F. Almeida, "Verifiable anonymous vote submission," *ACM symposium on Applied computing*, pp. 2159–2166, 2008.
[87] A. Zwierko and Z. Kotulski, "A light-weight e-voting system with distributed trust," *Electronic Notes in Theoretical Computer Science*, vol. 168, pp. 109–126, 2007.

King-Hang Wang received his PhD from the National Tsing Hua University and BEng from the Chinese University of Hong Kong. He worked in the Hong Kong Institute of Technology in 2010 as a lecturer. He joined the Hong Kong University of Science and Technology since 2015. His research focus is cryptography, mobile security, and provable authentication.

Subrota K. Mondal received the BSc degree in computer science and engineering from Khulna University of Engineering and Technology, Bangladesh and the PhD degree at The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. His research interests include cloud computing, network security, and SDN.



Ki Chan received her PhD degree in Systems Engineering and Engineering Management from the Chinese University of Hong Kong in 2010. She is currently a Lecturer of the Department of Computer Science and Engineering at the Hong Kong University of Science and Technology. Her research interests are text mining and information extraction, in particular, entity resolution and relation extraction.

Xiaoheng Xie received the BSc degree in computer science and engineering department from Renmin University of China, Beijing, China, and the PhD degree in computer science and engineering department from Hong Kong University of Science and Technology, Hong Kong. Her research interests include Data security, entity resolution, deep web data deduplication.