Enhanced Name and Vote Separated E-voting System: An E-voting System That Ensures Voter Confidentiality and Candidate Privacy

---

Citation:
Haijun Pan, Edwin S.H. Hou, and Nirwan Ansari, "Enhanced Name and Vote Separated E-voting System: An E-voting System That Ensures Voter Confidentiality and Candidate Privacy," *Wiley Security and Communication Networks,* DOI: 10.1002/sec.944, vol. 7, no. 12, pp. 2335– 2344, Dec. 2014.

URL:
http://onlinelibrary.wiley.com/doi/10.1002/sec.944/abstract

E-NOTE: An E-voting System That Ensures Voter Confidentiality and Candidate Privacy

Haijun Pan, Edwin Hou, and Nirwan Ansari

Abstract—In this paper, we propose an improved E-voting system based on our previous work (Name and vOte separaTed E-voting system, NOTE). The proposed E-voting system, referred to as Enhanced NOTE (E-NOTE), is enhanced with a new protocol design and a watchdog hardware device to ensure voter confidentiality and voting accuracy. In our improved scheme, rather than Election Committee (EC) and Vote Counting Committee (VCC), an impartial third party, Ballot Distribution Center (BDC), is proposed to take the responsibility of distributing ballots. The votes and the candidates' names are separated into two parts while voters cast their votes. The watchdog device records all voting transactions during the election to prevent voting disputes and other malicious behaviors from voter frauds. Our proposed procedure addresses issues related to voter confidentiality and candidate privacy, voting frauds and voting accuracy, and will thus create a fair election.

Index Terms— watchdog device, cryptography, voter confidentiality, candidate privacy.

I. INTRODUCTION

Concerns and issues from previous political elections have spawned numerous studies regarding voter confidentiality, voting security and voting accuracy. Although various voting schemes have been proposed to improve the security and accuracy of Electronic Voting (E-Voting) system, many disputes happened in the past still have not been resolved while new challenges have continuously been emerging. As we know, the paper ballot based voting system inevitably yields a certain rate of physical device failures and human errors. In addition, the tally result may suffer from unavoidable delays and ballot feeding errors while election committee counts votes on paper or machine readable ballots. With recent advances in technology, it may be time to transition traditional voting methods to electronic ones. There have been many reports [1]-[5] focusing on E-Voting issues. Currently, the most widely used "Direct Recording Electronic" (DRE) voting system [6]-[7] focuses on facilitating voters to cast paperless ballots on specific voting machines at voting booths. Meanwhile, several research works have focused on the security issues on the data encryption process [10]-[12]. Online E-voting has raised legitimate concerns about the performance of the voting system in terms of scalability, trustworthiness, and reliability, if millions of voters exercise their voting rights through the Internet instead of going to regular voting booths. Some researchers are advocating for Internet based voting [8], and our previous work (NOTE) [9] was also tailored for the Internet voting environment. Many challenges about Internet based E-Voting systems still remain open. Jakobsson *et al.* [13]-[14] have reviewed the issues and concerns about E-Voting on voter registration, voting in an untrustworthy or trust path, voting manipulation, reliability of software, data transmission, database systems, confidentiality of electronic votes, vote buying, and other factors. These factors are aligned with the major concerns of internet attacks around the global.

II. BACKGROUND

In this section, we will summarize current proposed E-Voting systems into several categories. The first major type of E-voting systems is the punchscan system that was proposed by Chaum

[4],[5],[15] and the three-ballot voting scheme proposed by Rivest [16]. Punchscan allows an eligible voter to scan the ballot, and hold one part of the ballot after the vote is casted. The three-ballot voting system does not use cryptography but rather uses multi-paper ballot to achieve the same security level as other systems that use cryptography. The punchscan scheme has also inspired several E-voting systems in the past few years [17]-[24].

Blind signature based voting scheme was introduced by Chaum [25] in 1983. The merit of blind signature mainly lies on simplifying the algorithm used in the voting process and it could secure the voting data transmission. However, when blind signature is applied, its untraceability is the major issue as voters might not be able to track their votes. Homomorphic–based schemes [26] are the third type of systems used in Internet based voting systems while every vote is encrypted and added to the final tally result. The main idea focuses on the whole voting tally result rather than every single vote. Usually, there exists a homomorphism between two algebraic structures, i.e., a structure-preserving map between the two structures. This property is used to decrypt the final tally result while the information and identity of voters remain encrypted. As researchers have pointed out, this type of schemes suffers from poor scalability. The fourth type of E-voting is the mix-net scheme proposed by Chaum [27] in which each vote is encrypted with a series of cascaded encryption.

In the United States, the term "E-Voting" refers to voters who use electronic voting machines and cast electronic ballots by touch screen devices [28]. In this paper, we refer to the term "E-Voting" as any voting process being held through the Internet.

III. Our Proposal

Our previous work NOTE (Name and vOte separaTed E-voting system [9]) provides a solution to prevent mistake and collusion that may happen in the vote counting procedure during an election. In NOTE, candidates' names and voters' votes on the ballots have been isolated so that Vote Counting Committee (VCC) does not have the complete information on each ballot other than the part that contains votes. Our new proposed scheme provides an extra measurement to ensure the accuracy of the voting tally result, and it would prevent VCC from committing malicious acts.

Besides the issues addressed in NOTE, many other issues can arise when the voting procedure is held through the Internet. Voter confidentiality is one of the major issues in the presidential elections and many researchers have explored this issue for years. If Election Committee (EC) members collude and share the ballot distribution information, voter confidentiality may be compromised. If EC is corrupted, it can rebuild the relationship between a specific ballot and the voter who uses this ballot. To counter this potential vulnerability, we introduce a third authority: Ballot Distribution Center (BDC). BDC, VCC, and EC are independent from each other, and our proposed scheme will prevent these three independent authorities from collusion, thus creating a fair election.

This paper presents an enhancement to NOTE with two levels of privacy protection measurements so that the risk of privacy leakage, collusion among voting authorities, and vote counting mistakes could be mitigated. The enhanced model, which is referred to as Enhanced NOTE (E-NOTE), provides a new platform to ensure a fair E-voting environment. Another issue to be addressed is voter's voting fraud. In order to prevent voters from maliciously disputing their votes, we introduce a hardware watchdog device to record all voting transactions. In real

life, some banks offer online E-banking service for registered customers. Every customer will get a flash card or device which will be connected to their personal computer. Without this device, the customer could not logon and use the E-banking service. The watchdog device used in our scheme has similar functionalities and it is issued by EC to every eligible voter prior to the election.

The novelty of our work is to create a mutually restrictive relationship between voters and voting authorities. The outlined scheme also eliminates voters' voting frauds and protects both voter confidentiality and candidate privacy.

In this section, we illustrate our proposed scheme with an example by using paper ballot to help readers understand the concept of our scheme. Fig. 1 shows the information flow between voters and the voting authorities. There are three election authorities in our scheme which are EC, BDC, and VCC. BDC performs the duty of ballot distributing from EC. First of all, EC certifies a voter's eligibility by identifying the voter's watchdog device, then issues him/her an electronic certificate, and the eligible voter can obtain the ballot from BDC by using this electronic certificate. Other than the certificate, this voter does not have to show any other identification to the authority (BDC) to obtain the ballot. From this step, there is no linkage between the certificate and the voter's identity. Obviously this method ensures voter confidentiality and privacy.

The watchdog device records all transactions carried out during the voting procedure, and thus eliminate the possibility of voting frauds, such as requesting duplicated voting and ballot requesting.

Let us consider a small class election where Alice, Bob and Charlie are three candidates. We assume that there are three other students, A1, A2, and A3, representing three voting authorities, EC, BDC, and VCC, respectively. A1 is in charge of voter registration, A2 is in charge of ballot distribution, and A3 is in charge of vote counting. We could not identify the relationship among these three students and the three candidates. In other words, the three students acting as the voting authorities are not 100% trustable.

Suppose Jessica is one of voters in the class; her voting procedure is conducted as follows:

Step 1: Jessica goes to A1 for registration where she receives a certificate card from A1.

Step 2: Jessica then shows her certificate card to A2. Note that Jessica does not have to show her identity to A2 at this time. A2 generates 3! types of ballots (since we have 3 candidates), and each ballot has one of the 3! permutations and a marker indicating its type. A2 checks Jessica's certificate card to verify that she is an eligible voter and her thumb is not marked (indicating she has not voted. This step is equivalent to recording the transaction and setting a flag in the watchdog device). Then, Jessica will be given a plain ballot and her thumb will be marked at the same time to indicate that she has been assigned the ballot. These two steps are used to protect voter confidentiality and privacy, and we already know that there is no linkage between the certificate and the ballot.

Step 3: When Jessica marks and submits her ballot, a carbon copy of the vote is retained by herself (this is equivalent to recording the transaction in the watchdog device). The main purpose of this step is to prevent voter frauds [29]. If Jessica claims a problem with her vote, she must present the carbon copy ballot to the authority for further investigation. In the E-voting mode, the watchdog device is used to record all the transactions in the voting process.

Step 4: This is similar to the step discussed in [9]. Jessica tears the ballot into two parts and

casts them into two different boxes. The part containing Jessica's vote is given to A3 and the part containing the candidate's name is given to A1.

Step 5: A3 counts all received ballots once the voting is completed. Since there are 3! types of ballots and the received parts do not contain the candidates' names, A3 only tallies the result based on the ballot type.

Step 6: A3 publishes the tally results of each type of ballots to the public on the blackboard.

Step 7: A1 reveals the sequence of candidates' names on each type of ballot, and thus the final count for each candidate is obtained.

IV. System Model

In this section, we discuss the proposed scheme in the E-voting mode.

For the voting procedure in our scheme, the following assumptions are made:

a) Voters are not 100% trustable.
b) The voting authorities are independent from each other, but they are still not 100% trustable.
c) The voting data transmission is reliable. We only focus on the protocol design in this paper.
d) We do not focus on the development of new cryptographic methods. Three-pass protocol and RSA are the main cryptographic methods [30-31] used in this paper, and other encryption methods could be adopted to our scheme for future research.
e) Each voter obtains a watchdog device from EC when they register to vote prior to the election. This step is equivalent to having the voter register for voting in traditional election process. The device must be connected to a computer when E-voting transactions are carried out. The device's main function is to record voting transactions (such as certificate request and issuance, ballot request and issuance, and vote casting). Voters are unable to either review or modify the transaction history. It is assumed that the device is secure and any voting dispute will be investigated by checking the voting transaction history recorded in the device.

The proposed E-voting procedure is summarized in Fig. 2.

1. EC receives the registration request from the voter; EC verifies and determines whether the voter is eligible to receive the certificate. EC uses the three-pass cryptographic algorithm [30] to encrypt the certificate and sends it to the voter. The three-pass protocol is a framework which allows one party to securely send a message to the other party without exchanging encryption keys.
2. The voter uses the three-pass cryptographic algorithm again to encrypt the certificate with his/her own key. Then, the voter sends the encrypted certificate (which is encrypted twice with different keys from EC and voter) back to EC.
3. When EC receives the encrypted certificate from the voter, EC decodes it with EC's own key and then applies the BDC's public key (which is only shared by EC and BDC) on the encrypted certificate, and sends it back to the voter again.
4. The voter receives the certificate for the second time and uses his/her own key to decode the encrypted certificate. After this step, the certificate is only encrypted by the BDC's key.
5. The voter sends the encrypted certificate which is only encrypted with the BDC's key to BDC.

6. BDC uses its private key to decode the certificate and verifies whether the certificate is authentic and is issued by EC. If the verification result is positive, the voter is eligible to receive a ballot from BDC.
7. BDC uses the RSA algorithm [23] to encrypt the voting data. The ballot format is defined as *{c, t, f}* where the array $c = (c[1], c[2], \ldots, c[w])$ is the list of candidates at the voter side and w is the number of candidates, t denotes the marker (type) of the ballot the voter received, and f is the transaction flag recorded in the voter's watchdog device. BDC sends the encrypted ballot *{c, T, f}* to the voter where the marker t is encrypted as T, it remains hidden as it uses a key. Voters could not decrypt T either. The flag f is received at the voter side and it will be compared and recorded into the watchdog device. This step ensures there is no linkage between the specific voter and the assigned ballot. Meanwhile, the ballot request flag is recorded into the watchdog device to prevent further ballot requests from the same voter.
8. The voter's vote is represented by a binary array $d = (d[1], d[2], \ldots, d[w])$ (where a "1" denotes a YES vote; a "0" denotes a NO vote).
9. The voting data including the array d and the marker T is sent to VCC. The watchdog device records the vote submission transaction. VCC cannot decrypt the hidden marker T since it does not have the BDC's key. This step ensures that ballot types remain unknown to VCC. VCC generates a receipt L and sends it back to the voter. L is used by the voter to review and track his/her vote, and is recorded in the watchdog device as well.
10. VCC tabulates and publishes the results on a public bulletin for each type of ballots and sends them to EC. In the meantime, BDC will post its private key on the bulletin as well.
11. EC reveals the value of marker T on each type of ballots, and calculates the final tally results of the votes according to the candidates' names. There is no chance to manipulate the results since it is already published.

In the past, many contentious issues were raised during the vote counting period, and people have many concerns about the voting machines and their software. For example, in the 2000 presidential election, counting errors and recounting were the focus of debate in Florida [32]. Our proposed election process is a distributed E-voting system model. The three independent voting authorities, EC, BDC, and VCC, ensure the absolute fairness during the election. The plug-in watchdog device used in our implementation of E-NOTE can authenticate voter's communication with the voting authorities. The device can also provide voters with their own voting history and can be used as evidence in the event of a voting dispute. Our revised model E-NOTE can mitigate both of these concerns by utilizing a decentralized counting process that ensures voter confidentiality and voting accuracy.

V. Functional Details

In this section, we illustrate the mathematical formulation of our proposed method. Suppose there are n voters and w candidates:

A_i: Voter i's batch code
B_i: Voter i's date of birth
U_i: Voter i's identity number
G_i: Voter i's gender
D_i: Voter i's choice

$C_{i:}$ The name of Candidate i, where i is from 1 to n.

M: The certificate given to voters by EC; the voter needs to show this certificate to BDC to obtain the ballot from BDC.

Assume $r\ r'$ mod $(p\text{-}1) = 1$ and $s\ s'$ mod $(p\text{-}1) = 1$, where p is a large number and r is in the range from 1 to $(p\text{-}1)$ with $\gcd(r, p\text{-}1) = 1$. We denote r as the private key of EC and r' as the corresponding decryption key of EC. We also denote s as the private key of voter i, and s is in the range from 1 to $(p\text{-}1)$ with $\gcd(s, p\text{-}1) = 1$. s' is the corresponding decryption key of voter i.

Step 1: Voter i sends the data array (U_i, G_i, B_i, A_i) to EC to get the voter registration. After EC's verification, EC uses the three-pass encryption algorithm and sends the message:

$$(E(r, M), F) = (M^r \bmod p, F) \quad (1)$$

to Voter i. Prior to the election, the authorities will initialize every watchdog device with a set of data. These data are used for securing and monitoring voters' online voting behaviors and transactions. F is used for the watchdog device to verify that this packet is really from EC, and $E(.)$ is the encryption function. This step shows that EC sends the certificate M to Voter i. If F matches the data stored in the watchdog device which authenticates the packet, the voting process can then proceed. The voter does not have access to information stored in the watchdog device; only the authority can review and check the watchdog device upon request.

Voter i receives the packet from EC, and encrypts it with his/her own private key s, resulting in the following data:

$$(E(s, E(r, M)), F) = (E(r, E(s, M)), F) = ((M^r)^s \bmod p, F) = (M^{rs} \bmod p, F) \quad (2)$$

The packet is sent back to EC, and EC will decode it with own key r' by the decryption function $Z(.)$:

$$Z(r', E(r, (s, M))) = E(s, M) = M^s \bmod p \quad (3)$$

Denote Φ as the shared key from BDC to EC; Φ is in the range from 1 to $(p\text{-}1)$ with $\gcd(\Phi, p\text{-}1) = 1$ and Φ' is the corresponding decryption key of BDC. Then, EC uses the BDC's shared key Φ to encrypt the certificate again, and the certificate becomes:

$$E(\Phi, E(s, M)) = M^{s\Phi} \bmod p \quad (4)$$

Finally, EC sends this certificate to the voter again for BDC to identify eligible voters.

Step 2: Voter i receives and decodes the certificate with his/her key s' as

$$Z(s', M^{s\Phi} \bmod p) = M^{\Phi} \bmod p = E(\Phi, M) \quad (5)$$

and then sends $E(\Phi, M)$ to BDC to show that he/she has the certificate from EC, and it is encrypted with the key that is only shared between BDC and EC.

BDC uses the same method to decode

$$Z(\Phi', E(\Phi, M)) = M^{\Phi\Phi'} \bmod p = M \quad (6)$$

Then, BDC distributes one ballot to Voter i. This step protects the voter's identity.

Step 3: Denote $c[i]$ as the name of the i^{th} candidate and the array $c = (c[1], c[2], \ldots, c[w])$ as the packet containing the list of names of all the candidates. Denote $t \in X$ as the marker on the ballot, where $X = 1, 2, \cdots$ is a set of consecutive numbers, and $|X|$ is greater than $w!$.

BDC generates one set of data, the ballot identification along with the list of candidates. BDC encrypts marker t with BDC's key.

Let

$$\alpha = (k-1)(k'-1) \tag{7}$$

where $z = kk'$, and k, k' are large numbers.

BDC chooses $1 < h < \alpha$ such that $\gcd(h, \alpha) = 1$. h' is chosen to satisfy the following:

$$(hh' \bmod \alpha) = 1,$$

where h' is the multiplicative inverse of $h \bmod \alpha$.

The marker t is encrypted as follows:

$$T = t^h \bmod \alpha \tag{8}$$

T is the encrypted data received at the voter side with BDC's key, h. BDC holds the private key exponent h' and VCC does not have the specific key to decrypt the marker T.

Step 4: When the voter has decided on the choice $d[i]$, the system will send the vote packet $(d[1], d[2], \ldots, d[w])$ with the marker T to VCC. The array d is a binary array generated at the voter side.

Step 5: VCC receives the array d, and then the votes are tallied for each type of ballot based on T. L is the voter's voting receipt to ensure that the vote is counted properly.

While VCC does not have the private key h',

$$\begin{aligned} TALLY_T &= (\sum(d[1], d[2], \ldots, d[w]), T) \\ &= ((\sum d[1], \sum d[2], \ldots, \sum d[w]), T) \end{aligned} \tag{9}$$

$$VER_T = ((\sum L), T) \tag{10}$$

Here, $TALLY_T$ is the tally of the ballots with the same encrypted marker T. $\sum(d[1], d[2], \ldots, d[w])$ represents the sum of the votes for every candidate, i.e., where $\sum d[j]$ represents the number of votes casted for candidate j. For example, if there are three types of ballots in the sequences of candidates "Alice, Bob, Charlie", "Alice, Charlie, Bob" and "Charlie, Alice, Bob", VCC will summarize the result of each individual type of ballots with the same sequence marked by T. $\sum d[1], \sum d[2], \ldots, \sum d[w]$ represent the number of votes that each candidate receives for one type of ballot. VER_T is the summary of all L with the same type T of the ballot. It will be stored in a database which allows voters to visit and track the votes they casted.

Step 6: After VCC finishes counting the votes, each $TALLY_T$ with the same marker T is published to the public.

Step 7: At the same time, BDC chooses a random number along with EC's public key to encrypt BDC's own private key to generate a new encrypted data packet, and then publishes on the

bulletin board to the public as well. We do not set up the secure channel between BDC and EC because we assume BDC and EC have no way to exchange data and key.

Step 8: EC uses its own private key to decrypt the encrypted key to obtain BDC's private key. Then, it decrypts $t = T^{h'} \bmod \alpha$ and tallies the final results.

After the content of the marker for each ballot type is reviewed and published, the final tally result can be calculated accurately by EC under the public's scrutiny.

VI. SECURITY AND EVALUATION DISCUSSION

Since E-NOTE is an Internet based voting system designed for future elections, one of the goals is to make the E-voting system as easy to use as any e-business or e-banking systems.

In this paper, we focus our research on the voting procedure so as to avoid potential mal-behaviors among election authorities. Our scheme is also set up to prevent VCC or other possible hackers from manipulating the vote results.

Consider an example where bribed authorities/hackers try to subvert or manipulate the election results. We define x as the event that the malicious authority or the hacker guesses the location of their favorite candidate on the ballot correctly. Define $P(x)$ as the probability that this can be done. If there are w candidates, there are w outcomes for this event and $P(x)$ is $1/w$.

We define y as the event that the malicious authority or the hacker guesses the sequence of candidates on the ballot correctly. Define $P(y)$ as the probability that this can be done and there are $w!$ types of ballots, and therefore

$$P(y) = \frac{1}{w!} \tag{11}$$

The entropy of X and Y,

$$H(X) = -\sum_w p(x) \log\ p(x) \tag{12}$$

$$H(Y) = -\sum_{w!} p(y) \log\ p(y) \tag{13}$$

Using the definition in information theory [33], we know that the mutual information relationship is defined as follows:

$$I(X,Y) = H(Y) - H(Y|X) \tag{14}$$

$$I(X,Y) = H(X) - H(X|Y) \tag{15}$$

From our definition and assumption, if the permutation of the list of candidates on the ballot is guessed successfully by VCC or other hackers, VCC's favorite candidate's position on the ballot will be known. The conditional entropy is:

$$H(X|Y) = 0 \tag{16}$$

This conditional entropy is 0 since the order of the candidates on the ballot is already known. Since $H(X|Y)=0$,

$$H(Y) - H(Y|X) = H(X) \tag{17}$$

$$H(Y|X) = H(Y) - H(X) \tag{18}$$

From Eqs.(15)-(16), we have:

$$H(Y|X) = H(Y) - H(X) \tag{19}$$

$$= -\sum_{w!} p(y) \log\ p(y) - \left(-\sum_{w} p(x) \log\ p(x)\right)$$

$$= w * \frac{1}{w} log \frac{1}{w} - w! * \frac{1}{w!} log \frac{1}{w!}$$

$$= log \frac{1}{w} - \log \frac{1}{w!} = log\ (w-1)!$$

Fig. 3 shows the relationship between the number of candidates and the conditional entropy. The conditional entropy can be interpreted as how likely the malicious authority VCC or the hackers can guess the permutation of the candidates set on the ballot if the position of their favorite candidate on the ballot is known. The number of candidates varies from 2 to 50 in Fig. 3 and a larger value in the conditional entropy indicates that there is more uncertainty to determine the permutation of the candidates on the ballot.

Consider the extreme case when there are only 2 candidates running in the election, i.e., w is 2. After VCC or hackers guess the position of their favorite candidate successfully on one ballot, the position of the other candidate on the ballot is also known. This means that the conditional entropy $H(Y|X) = 0$ as shown in Fig. 3.

In large-scale elections where there are a large number of ballots, we can consider the probability of picking any ballot type as being equal. If we have η types of ballot, the probability of any specific type ballot being selected is $1/\eta$.

Consider the case that the malicious authority VCC or the hacker guesses their favorite candidate on one of the ballots successfully. When the malicious authority or the hacker obtains the next ballot, let τ be the event that the same favorite candidate can be guessed successfully in this ballot and the probability $P(\tau)$ of that happening is:

$$P(\tau) = \frac{1}{w!} * 1 + \left(1 - \frac{1}{w!}\right) * \frac{1}{w} \tag{20}$$

$$= \frac{w + w! - 1}{w(w!)}$$

A plot of Eq. (20) is shown in Fig. 4 and the values of $P(\tau)$ for selected values of w are tabulated as Table 1.

In the worst case scenario where the cryptography method has been hacked by the malicious authority or the hacker, our E-NOTE scheme can still protect the candidate's privacy. $P(\tau)$ will drop from 1 to 0.04 if there are 25 candidates in the election.

Other than the presidential candidates, a national election ballot will also have candidates of senators, governor and local officers. The total number of choices in a ballot can be around 25 and we can add another 25 "virtual candidates" in the actual communication packet to decrease the probability of the ballot being guessed to 0.02.

VII. Conclusion

We have proposed a new E-voting system, E-NOTE, that ensures voter confidentiality, candidate privacy and voting accuracy, and E-NOTE thus plays an important role for future fair elections. Our scheme can reduce the possibility of having the list of candidates being guessed or hacked from 1 to $1/w$ by shuffling the names on every ballot. If the encryption scheme used in the election is hacked by malicious parties, the shuffling of the candidates' names on the ballot provides an additional protection to secure the privacy and fairness of the election.

References

[1] C.-H. Chen, "A practical voting system for small-scale election," *Proc. IEEE 3rd International Conference on Information Technology: Research and Education (ITRE 2005)*, Hsinchu, Taiwan, 27-30 June 2005, pp. 322-326.

[2] M.D. Byrne, K.K. Greene, and S.P. Everett, "Usability of voting systems: baseline data for paper, punch cards, and lever machines," in *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, San Jose, California, USA, April 28 - May 03, 2007,pp.171-180.

[3] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the Internet," *Proc. Third International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS 2001),* San Jose, CA, USA, 2001, pp.188-190.

[4] D. Chaum, (2006, Oct 15). *Punchscan*. Available at: *http://www.punchscan.org.*

[5] S. Popovenuic and B. Hosp, "An Introduction to Punchscan," Oct 15, 2006.

[6] N. Ansari, P. Sakarindr, E. Haghani, C. Zhang, A.K. Jain, and Y.Q. Shi "Evaluating electronic voting systems equipped with voter-verified paper records," *IEEE Security and Privacy*, vol. 6, no. 3, pp. 30-39, May 2008.

[7] T. Kohno, A. Stubblefield, A.D. Rubin, and D.S. Wallach, "Analysis of an electronic voting system," *Proceedings 2004 IEEE Symposium on Security and Privacy*, Oakland, California, USA, 9-12 May 2004, pp. 27-40.

[8] A. Kiayias, M. Korman, and D. Walluck, "An internet voting system supporting user privacy," *Proc. 22nd Annual Computer Security Applications Conference (ACSAC '06),* Miami Beach, FL, USA, Dec. 2006, pp. 165-174.

[9] H. Pan, E. Hou, and N. Ansari, "Ensuring voters and candidates' confidentiality in E-voting systems, " *34th IEEE Sarnoff Symposium* Princeton, NJ, May 3-4, 2011.

[10] C. Orhan and A. Doganaksoy, "Pseudo-voter identity (pvid) scheme for e-voting protocols," *Proc. The Second International Conference on Availability, Reliability and Security (ARES 2007)*, Vienna, Austria, 10-13 April 2007, pp. 1190-1196.
[11] X. Li *et al.*, "An Elementary Electronic Voting Protocol Using RFID," *Proc.* 2007 *IEEE SMC Information Assurance and Security Workshop (IAW '07)*, 20-22 June 2007, pp. 234-238.
[12] O. Cetinkaya, "Analysis of security requirements for cryptographic voting protocols," *Proc. Third International Conference on Availability, Reliability and Security (ARES 08)*, Barcelona , Spain, 4-7 March 2008, pp. 1451-1456.
[13] M. Jakobsson and A. Juels, "DIMACS workshop on electronic voting theory and practice," DIMACS Center, CoRE Building, Rutgers University, Piscataway, NJ, May 26- 27, 2004.
[14] C.-K. Wu and R. Sankaranarayana, "Internet voting: concerns and solutions," *Proceedings of First International Symposium on Cyber Worlds, 2002*, Tokyo, Japan, November 6-8, 2002, pp. 261-266.
[15] B. Hosp and S. Popovenuic, "Punchscan Voting Summary," Feb 13, 2006, Available at: *http://home.gwu.edu/~bhosp/punchscan/article.pdf*
[16] Ronald L. Rivest. "The Three-Ballot Voting System," Oct. 2006, Available at: *http://theory.csail.mit.edu/_rivest/Rivest-TheThreeBallotVotingSystem.pdf*
[17] P.Y.A. Ryan and S. A. Schneider, "Prêt à voter with re-encryption mixes," in *ESORICS*, Lecture Notes in Computer Science, Springer, 2006.
[18] J. Graaf, "Voting with Unconditional Privacy by Merging Prêt-à-Voter and PunchScan," *IEEE Transactions on Information Forensics and Security*: Special Issue on Electronic Voting, vol. 4, no. 4, pp. 674-684, December 2009.
[19] B. Adida and Ronald L. Rivest, "Scratch & vote: self-contained paper-based cryptographic voting," in *WPES '06: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society*, New York, NY, USA, 2006, pp. 29–40.
[20] B. Adida, "Helios: web-based open-audit voting," in *SS'08: Proceedings of the 17th Conference on Security Symposium*, USENIX Association, Berkeley, CA, USA, Jul 28- Aug 1, 2008, pp. 335–348.
[21] D. Chaum, et al., "Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes," *Proceedings of the conference on Electronic Voting Technology*, San Jose, CA, July 28-29, 2008, pp. 1-13.
[22] T. Moran and M. Naor, "Split-ballot voting: everlasting privacy with distributed trust, In P. Ning, S. De Capitani di Vimercati, and P. F. Syverson, editors, *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007*, ACM, 2007, pp. 246–255.
[23] R.L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21(2), Feb. 1978, pp. 120-126.
[24] J.L. Papaianni, "Concerns raised about new voting machines now in use," *The coaster*, Oct 16, 2008. [Online]. Available at: http://thecoaster.net/wordpress/2008/10/16/concerns-raised-about-new-voting-machines-now-in-use/
[25] D. Chaum, "Blind signature for untraceable payments," *Advances in Cryptology, CRYPTO82*, Plenum Press, New York, pp.199-203, 1983.

[26] J. Benaloh, "Secret Sharing Homomorphisms: Keeping shares of a secret secret," *Proc. 1986 Advances in Cryptology (CRYPTO' 86)*, Springer-Verlag, New York, pp. 251-260, 1987 (year of publication).
[27] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM* Vol 24, no. 2, pp. 84-90, Feb. 1981.
[28] S.P. Everett et al,. "Electronic voting machines versus traditional methods: improved preference, similar performance," *Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems*, Florence, Italy, Apr. 2008, pp. 883-892.
[29] L. Hope (Mar 24, 2011). ABC Chicago local news.
Available at: *http://abclocal.go.com/wls/story?section=news/politics&id=8032912*.
[30] A. Konheim, Cryptography: A Primer, John *Wiley* & Sons Inc, 1981, pp.346-347.
[31] Rivest, R, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM,* vol. 21, no. 2, pp.120–126, 1978.
[32] Wikipedia, "United States presidential election in Florida, 2000"
Available at:
http://en.wikipedia.org/wiki/United_States_presidential_election_in_Florida,_2000
[33] Gray, R.M., "Entropy and Information Theory," Springer-Verlag, New York, NY, 1990, pp. 17-46.

Tabel 1. The effect of w on the probability $P(\tau)$.

w	5	10	20	25	30	50
$P(\tau)$	0.26	0.10	0.05	0.04	0.03	0.02

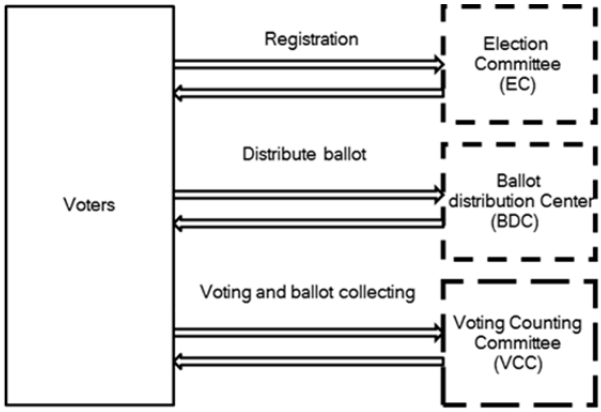

Fig. 1. Flow diagram illustrates how voter interacts with the voting authorities.

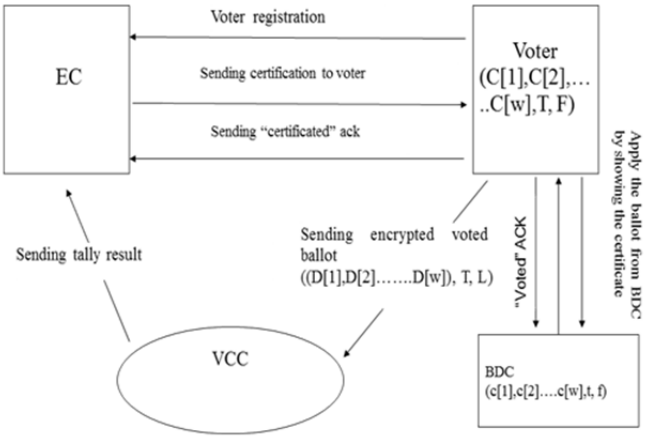

Fig. 2. The block diagram of the E-voting process.

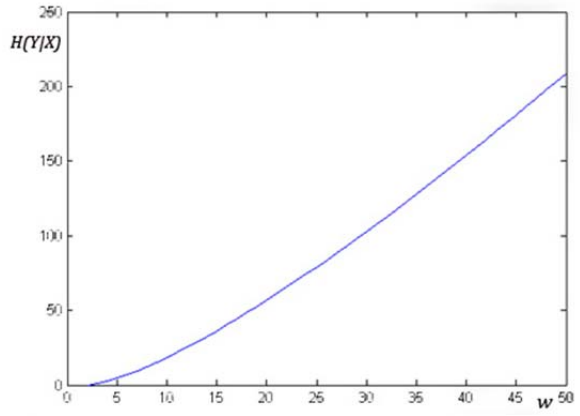

Fig. 3 The plot of $H(Y|X)$ with different w.

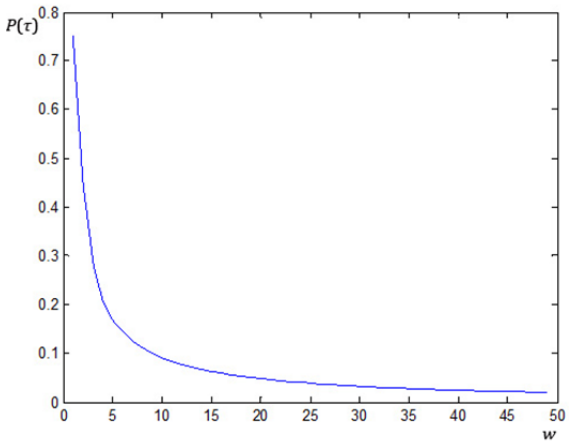

Fig. 4 The relationship between $P(\tau)$ and w.