A CASE STUDY FOR TURKEY: A SECURE PAPER-BASED ELECTRONIC VOTING SYSTEM

Oktay Adalıer
Tübitak UEKAE
41470, Kocaeli, Turkey
E-mail: oadalier@uekae.tubitak.gov.tr

Fatih Birinci
Tübitak UEKAE
41470, Kocaeli, Turkey
E-mail: fatih@uekae.tubitak.gov.tr

Süleyman Kardaş
Tübitak UEKAE
41470, Kocaeli, Turkey
E-mail: skardas@uekae.tubitak.gov.tr

Mehmet Sabır Kiraz
Tübitak UEKAE
41470, Kocaeli, Turkey
E-mail: m.kiraz@uekae.tubitak.gov.tr

─Abstract ─
There are several electronic voting systems proposed in the literature either paper-based method, using voter's computer and internet or direct-recording electronic (DRE) voting machine. These systems aim to satisfy the security properties like voter privacy, receipt-freeness, anonymity, verifiability, reliability, and usability. Besides, they mainly focus on the ballot tallying in order to solve the first conflict by achieving voter privacy and verifiability simultaneously. The most popular systems are based on homomorphic cryptosystems and mix-nets. These cryptographic e-voting schemes require all voters to have an advanced knowledge of mathematics. This requirement may not be realistic for many of the ordinary voters. Some suggestions require voters to indicate their intent to some voting devices (e.g. DRE machines). Prêt à Voter scheme, which is invented by Peter Ryan, is also another type of electronic voting scheme which is similar to paper-based systems. Although its backend uses advanced cryptographic mechanisms it is simple to understand for any ordinary voters. In the Prêt à Voter scheme all ballot forms are generated by some election authorities in advance under the supervision of some audits. So, the authorities have the ability to read the voter's choice directly from their receipts.

In this paper, we first describe the Prêt à Voter scheme and its cryptographic primitives. Next, we investigate the efficiency and the cost-effectiveness of referendums in Turkey by providing a case-study of the Prêt à Voter scheme. We conclude the paper by proposing the possible improvements and suggestions for Turkish elections.

Key Words: *Electronic voting, cryptographic protocols, Turkish elections*
JEL Classification: D72 - Political Processes: Rent-Seeking, Lobbying, Elections, Legislatures, and Voting Behavior

1. INTRODUCTION

1.1. Electronic Voting

Electronic voting is getting more and more popular in several countries including Turkey. Since the economical and sociological situations are getting better, voting is becoming very difficult in several aspects. For example, the mobility during the voting day is becoming an issue. As in the many countries the voting process in Turkey is address based, and the people away from home have to travel on the voting day. Hence, the current situation prevents mobility of the citizens on the voting day. Furthermore, Turkish citizens abroad cannot vote even in the embassies. They have to travel to customs to be able to vote. Because of the current laws, the postal voting procedure is not accepted by the supreme court of Turkey. Although many people focus on these kinds of problems when talking about e-voting, there are in fact many more advantages if it is carefully designed. The system could satisfies many security properties, e.g. , privacy, correctness, anonymity, verifiability, receipt-freeness, which do not exist in the traditional paper based voting systems [EV].

The current voting system in Turkey has some good properties [YSK]. Although paper based voting process and manual tallying, the registration and the authentication of the voters are performed online. During the registration the Turkish Identification Number (which is unique for every Turkish citizen) is used in order to authorize to the system. This ID allows ever voter to register to a single voting center and to vote only once. Besides, after the tallying is completed in the voting centers, the results are sent through the VPN tunnel to the Election Authority Center. Therefore, the complete counting process takes only several hours. Later on, the votes are shipped physically to the Election Authority Center, too. Although these good properties, current voting system in Turkey have still several deficiencies:

- It is not individual and universal verifiable, therefore there is no possibility for voters to be able to verify whether their vote is counted correctly.
- Since the voters must stamp in a small area the rate of the invalid votes are high [EV].
- The counting process is also very cumbersome.
- Overall, the cost of the current system is very high.

Electronic voting system is the most difficult problem for cryptographers since it is rather a difficult problem involving several research areas like society, physiology, politics, laws, information technology and security [EV]. It is also rather interesting and unique problem for cryptographers since any malicious behavior can be both from insider and outsider. For example, the system can cheat voters, voters can cheat systems, coercers can affect voters, and voters can fool coercers. Furthermore, the proposed system must be understandable and usable by the entire voting population, regardless of age or disability. Voters in general do not have the computing power and expertise. Therefore, the proposed e-voting systems should be user-friendly, understandable and scalable. Providing accessibility to such a diverse population is also an important engineering problem. If the security properties described-above are also satisfied, electronic voting might be a great improvement over traditional paper-based system.

Instead of traditional paper-based voting systems electronic systems like machine, internet and even mobile can be used. In this way, the voters generate the encrypted votes and they are published on the bulletin board. However, this might result in the following serious issues:

1. How can voters ensure that their intent has been transferred into encrypted votes correctly, and these votes are recorded in the election system correctly?
2. How can voters ensure that the voting device or election authorities will not leak the private information?

Most of the current cryptographic schemes have solved only the first issue. However, because voters need to indicate their intent to some voting device or election authorities, the voter privacy will be violated if the voting devices or election authorities are malicious. The first e-voting scheme solves both problems described-above by Prêt à Voter with re-encryption mixes, in which all ballots are generated by a number of election authorities in a distributed fashion [RS06]. Therefore, although some voting devices are still proposed, the voters no longer need to indicate their intent to the voting devices or some single authority.

1.2. Related Work

Although electronic voting is well-studied within the research community there are still specific issues for each of the proposed schemes. There might be several problems like incorrect use of cryptography, vulnerabilities to network threats and poor software development processes.

Maybe the most interesting and practical example is Estonia where Internet voting is used in parliamentary elections since 2005. Besides that, Norway will start to use internet voting in September 2011 in local governmental elections. The Internet vote is particularly attractive to those voters who spend considerable time to reach the polling station. For example, about half of the Internet voters in Estonia indicated that they would have spent half an hour or more to reach the polling station [EES]. Many of these voters might not live in their official residence, either living in another place or abroad. Internet based scheme for Norwegian case solve the above-mentioned issue by adding extra two independent pre and post-channels (pre-channel is postal service and post-channel is SMS) [NVS].

The Prêt à Voter is also interesting and attracts attention of the research community because of its simplicity, usability and understandability. It is simple and very close to paper voting since the voters are provided with a familiar-looking ballot form as it is important for people to be able to accept the system. There is still active research going on improvements of the Prêt à Voter scheme on several aspects [RS06]. We note that there are only a few research has been done about e-voting in Turkey [MA06, CC06, CC07, CD07]. Moreover, there are also not many case-studies for Turkish elections. The Prêt à Voter scheme is, therefore, is an interesting system to analyze whether it is suitable for Turkey.

1.3. Contributions

Election Authority and Turkish Government are interested in electronic voting systems to develop and use for future elections [YSK]. Therefore, in this paper, we are going to analyze applicability

of the Prêt à Voter scheme for referendums in Turkey. It should be noted that every election like referendums, parliament and local elections should be considered as a completely different project. Therefore, we will focus on only on referendum. This paper is interesting since it is the first paper that considers the Prêt à Voter scheme for Turkish elections. We analyze the efficiency and cost-effectiveness based on the latest referendum results done in September 2010. We summarize the results and conclude the paper by proposing possible improvements and suggestions for Turkish elections.

Roadmap: In Section 2, we describe the Prêt à Voter scheme. In Section 3, we describe the current situation of Turkey and the statistics of referendum in 2010. In Section 4, we analyze the efficiency and cost-effectiveness of the Prêt à Voter scheme. Section 5 concludes the paper.

2. Prêt à Voter Scheme

In this section we present the basic cryptographic primitives necessary for the electronic voting systems. A voting protocol consists of a set of sub-protocols which allows a set of voters to cast their votes securely. These protocols also enable a set of talliers to compute and communicate the final tally, which can be verified by a set of observers and auditors. The essential security requirements of must be achieved by the overall protocol.

There are mainly three types of voting scheme: (a) Blind signatures, (b) Protocols based on homomorphism, (c) Mixnet protocols [ACDMTV05]. Blind signatures employ an anonymous channel to cast ballots thwart connection of votes and voters. Authentication is conserved through the use of blind signatures [DC83]. Protocols based on homomorphism are protocols where individual votes are split up among different tallying authorities in order that no single one of them can compromise the privacy of an individual voter. These protocols are based on homomorphic encryption and homomorphic secret sharing and allow for universal verifiability [RAD78]. Mixnet protocols are based on mixing each votes so that no one can relate a particular vote to a voter. In this scheme, there are no disconnecting talliers or observers. Prêt-à-voter is a good example of mixing protocols. The technical detail of the protocol is described in the next section.

2.1 The Voting Scheme

Prêt-à-voter is an electronic voting system invented by Peter Ryan [RS06]. The main purpose of this scheme is to provide guarantees of accuracy of the tallying and ballot privacy, which are independent of software, hardware etc. In the electronic voting, transparency of the process is very important. To achieve the transparency, Prêt- à-Voter maintains ballot privacy and allows voters to confirm that their vote accurately and also it avoids dangers of coercion or vote buying.

In addition, in order to keep ballot privacy, the Prêt à Voter approach encodes the vote using a randomized candidate list. The randomizations of the candidate list on each ballot form make certain the secrecy of each vote. By the help of this way, it also removes any biasness towards the top candidate that can occur with a fixed ordering.

Figure 1: A typical Prêt à Voter ballot form

Ayşe Demir	
Mustafa Yılmaz	
Bora Yıldız	
Erol Kaya	
	e1Tg37

In Figure 1, a typical ballot form is shown and the value printed on the right bottom of the form is the key to extraction of the vote. Buried cryptographically in this value is the information needed to reconstruct the candidate order and so extract the vote encoded on the receipt. This information is encrypted with secret keys shared across a number of tellers. Thus, only a set of tellers acting together are able to interpret the vote encoded on the receipt.

After the election, voters can visit the Web Bulletin Board (WBB) and confirm their receipts appear correctly. Once the voting is over, the tellers take over and perform anonymising mixes and decryption of the receipts. All the intermediate stages of this process are posted to the WBB and are audited later.

In this paper, we consider the Prêt à Voter system with re-encryption mixes. This scheme consists of four distinct operations: ballot generation, vote casting, vote processing and auditing. Each operation is described in detail in the next sections.

2.2 Ballot Generation

Ballot forms are generated by a set of clerks that each clerk contributes to the entropy of the crypto seed in an encrypted way. The candidate order is derived from the secret seed. In order to determine the seed values, all the clerks have to cryptographically collude in a predefined threshold scheme.

In the ballot generation, it is assumed that a set of decryption tellers hold secret key shares for a threshold ElGamal primitive with public key (p, α, β_T). Each teller is responsible for the final decryption stage after anonymising, re-encryption mix phase that are explained in section 3.3 and 3.4 in detail. There also a set of registrars with threshold secret key shares corresponding to the public key (p, α, β_R) that are known to the clerks and will be used to generate the ballot forms.

First of all, each clerk C_j generates a batch of initial seeds s_i^j. These seeds are randomly drawn from a binomial distribution with zero mean and standard deviation σ which is chosen as the order of n, the number of candidates. The clerk C_0 first encrypts each s_i^0 in the form of $\gamma^{-s_i^0}$ where γ is a generator of Z_p^* under the registrar key and teller key as follows. This form of encryption allows

us to perform re-encryption mixes and transformations in the vote processing and auditing. Let x_i^0 and y_i^0 be drawn randomly from Z_p^*. Then, the ElGamal encryptions are:

$$(\{\gamma^{-s_i^0}\}_{PK_R}, \{\gamma^{-s_i^0}\}_{PK_T}) = ((\alpha^{x_i^0}, \beta^{x_i^0}{}_R.\gamma^{-s_i^0}), (\alpha^{y_i^0}, \beta_T^{y_i^0}.\gamma^{-s_i^0}))$$

After that, the remaining clerks then perform re-encryption mixes and transformations on this batch of onion pairs. Each j-th clerk takes the output pair of previous clerk and performs a combined re-encryption along with an injection of fresh entropy into the seed values. In other words, j-th clerk generates new random values x_i^{j-1}, y_i^{j-1} and s_i^{j-1}. Next, it computes the encryption pair $((\alpha^{-s_i^{j-1}}, \beta_R.\gamma^{-s_i^{j-1}}), (\alpha^{-s_i^{j-1}}, \beta_T.\gamma^{-s_i^{j-1}}))$ and multiplies it with previous output pairs using homomorphism property of the ElGamal encryption (E(x).E(y) = E (x.y)). Then the final output pair after l-1 mixes will be in the following form:

$$((\alpha^{x_i}, \beta^{x_i}{}_R.\gamma^{-s_i}), (\alpha^{y_i}, \beta_T^{y_i}.\gamma^{-s_i}))\text{, where } x_i = x_i^l, y_i = y_i^l, s_i = s_i^l.$$

The final output s_i values will have the binomial distribution with zero mean and standard deviation $\sigma\sqrt{l}$. The first onion is referred to the "Registrar onion" or "booth onion" whereas the second onion is referred to "Teller onion".

The use of two onions on a ballot form allows us to detect any corruption on the form. The candidate order is enclosed in the seed value, which is then encrypted with public key in the ballot form. These onions can now printed on the ballot form freely because the encryption avoids the any clerk to reveal the candidate list order. Fortunately, if all the Registrars get together on a threshold scheme, then they can decrypt the first onion, then they will able to reveal the order of the candidates.

2.2 Vote Casting

The voters in the booth have a common Prêt à Voter ballot form which consists of the candidate list and the associated right hand (teller) onion. The voters can easily mark and X against the candidate of their choice. The left hand strip is removed and destroyed. Then, the voter leaves the booth and casts his/her vote in the presence of an official and the machine record the vote as (r, onion) where onion is the teller onion of the form and r is the index value of the position of the X. The vote is then digitally signed and a copy of the receipt is also given to the voter.

An adversary can classify the votes according to the r index value. In order to overcome this problem, r index value can be absorbed into onion value. This is done as follows. Assume that we use a single choice election system and base ordering of the candidate list can only be reordered by simple cycle shifting. For example, we have 5 candidate and only 5 re-ordering candidate lists is possible by the help of cycle shift operation. Then, let s_i be the shift of the candidate list for i-th ballot form. The r index value can be absorbed in to onion value as follows: $(\alpha^y, \beta_T^y.\gamma^{r-s_i})$. It is

easily seen that this is a simple ElGamal encryption in which $r - s_i$ modulo n is encrypted as message and this gives the voter's the original candidate choice in the base ordering.

As soon as the election has closed, the copies of the digitized receipts will be posted to the Web Bulletin Board (WBB). The voters can also visit WBB and verify whether their vote is posted to WBB.

2.3 Vote Processing

ElGamal encryption mechanism allows re-randomization and so the mixing votes are done by the help of re-encrypting votes. Once the election has closed and all digitized votes are posted to Web Bulletin Board, the votes are processed by a conventional re-encryption mix by a set of mix tellers [JCJ02]. These mix tellers do not hold any secret keys, however; gets a batch of ElGamal terms from the WBB, re-encrypt each of them and then post the resulting terms in random order to the WBB. As soon as a large enough number of such anonymising re-encryption mixes are done, a threshold set of decryption tellers come together and extracts the plain text values.

It is seen that the anonymising and decryption phases are separated out in re-encryption mixes. In order to tally the votes, this will result in decrypted terms of the form: $\gamma^{r-s_i} \pmod p$ and computing $r - s_i$ is difficult as much as the taking discrete log of γ^{r-s_i}. Since we know s values are drawn from a binomial distribution with $\sigma\sqrt{l}$, we can search the space efficiently. For instance, we can construct a large enough look-up table for the logs of some multiple of $\sigma\sqrt{l}$.

2.4 Auditing

In the previous section, we introduce the mechanisms allowing the distributed generation of ballot forms, just-in-time decryption of the candidate list and printing of the ballot forms. The use of such mechanism removes the need to trust a single entity to keep ballot form information secret and avoid chain of custody issues. In order to pre-audit the ballot forms, the approach of Ryan and and Peacock can be incorporated [RP09]. In this approach, a ballot form has two independent pairs of onions. One printed on the one side of the form, the other on the flip side. The left hand onion on each side could be decrypted in the booth and the corresponding candidate list printed in the left hand column. Then, two independent ballot forms, printed on each side, depicted in the following figure.

Figure 2: Prêt à Voter ballot form

Ayşe Demir		----------
Mustafa Yılmaz		----------
Bora Yıldız		----------
Erol Kaya		----------
	7rJ93M	

Side 1

Erol Kaya		----------
Ayşe Demir		----------
Mustafa Yılmaz		----------
Bora Yıldız		----------
	1EJo6L	

Side 2

These two ballot forms could be considered as rotated around a vertical axis. Hence, the third column of side 1 would oppose the candidate list of side 2. Note that each side has independent randomization of the candidate order along with cryptographic onion values. The voters use only one side of the ballot form and make an arbitrary choice between the sides. For example, let a voter chooses side 1 and wants to cast a vote for Ayşe Demir. The voter places X against Ayşe Demir on side 1 and she/he destroys the left hand strip that shows the candidate order for side 1. The results of this process on the forms are depicted in Figure 3.

Figure 3: Both sides of a Prêt à Voter ballot receipt

X	----------	Erol Kaya	
	----------	Ayşe Demir	
	----------	Mustafa Yılmaz	
	----------	Bora Yıldız	
7rJ93M			**1EJo6L**

vote encoding side (Side 1) **auditable side (Side 2)**

Now, the information on the both sides can be recorded and posted to the WBB. The flip side can be audited and checked to make sure that the candidate list printed by the booth correctly corresponds to the onion value. Such checks could be carried out immediately at the time of casting in order to detect any problems as soon as possible.

3. PRÊT À VOTER SCHEME AND REFERENDUM IN TURKEY

3.1. Social Situation for Electronic Voting in Turkey

In Turkey, classical paper based voting is used for both in general election and in referendum. These system used inherently have some drawbacks such as invalid votes because of the stamp on the ballots (for example smearing of the ink), on purposely misreading a ballot, changing the ballot box illegally etc. Note that these problems are not specific to Turkey and are believed to be solved easily with e-voting systems.

Classical paper based elections are being used for centuries and people get used to trust it. Voters should also rely on the e-voting system used. Otherwise the people will not accept the system and voting system will not to be used. This situation was unfortunately experienced in several countries like Austria, the Netherlands and USA [Aus09, Sch04, Net06]. To gain confidence of people overall development and certification of the system should be open to everyone. Besides that, the voting process itself and the post processes should be easy and understandable. Some of the back processes of the Prêt à Voter Scheme such as tallying are fairly complex. Since these processes will be open to everyone, universities, research institutes and non-governmental organizations can examine them. In case sufficient examinations are performed from different part of organizations, the society might put trust to the system.

Most of the voters in Turkey are either primary school or high school graduates. In rural areas illiterate rate is higher than in urban areas (see Figure 4).

Figure 4: Statistics of Turkey

Distribution of Population according to Education (15 +age) - 20091			
Turkey			
Education	Total	Male	Female
No Education (illiterate)	4.645.638	908.628	3.737.010
Literate but no school completed	3.222.987	1.279.284	1.943.703
Primary School	18.523.823	8.937.271	9.586.552
Elementary Education	6.324.830	3.408.312	2.916.518
Junior high school	2.795.917	1.786.153	1.009.764
High School	10.379.231	6.002.688	4.376.543
Bachelor	4.320.813	2.534.434	1.786.379
Master	279.268	166.285	112.983
PhD	95.500	61.301	34.199
Unknown	2.962.823	1.626.257	1.336.566
Total	53.550.830	26.710.613	26.840.217
Foreign people are not considered			

Computer and Internet usage is low compared to the other OECD countries. However computer and Internet usages are increasing, particularly among young voters. Percentage of households with Internet access has increase to % 41.6 in 2010[2].

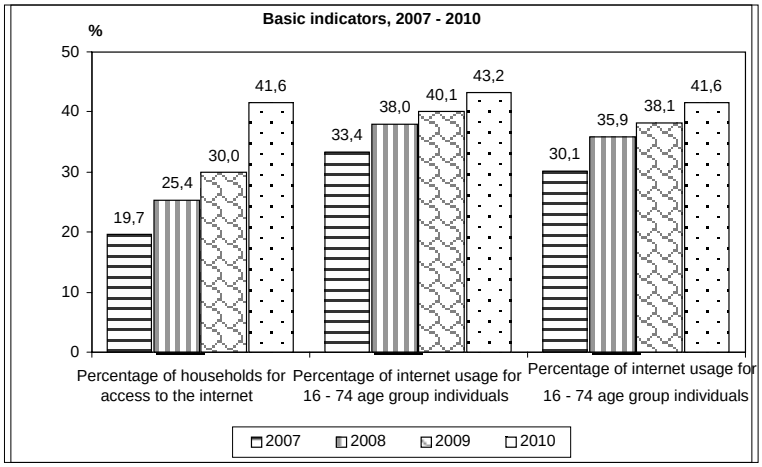
According to the research results, computer and Internet usage between 16-74 age groups are 53.4% and 51.8% for males, 33.2% and 31.7% for women respectively. These rates for the previous year are 50.5% and 48.6% for men, 30.0% and 28.0% for women respectively.

One of the obstacles in the use of the e-voting system in Turkey is the low computer literacy rate. However, India is known to have an overall lower literacy rate than Turkey[3]. Encouraging from India, e-voting might also be promising to be successfully used in Turkey. Apart from activities by private sector like e-banking, Turkey has given a considerable support on e-government and there are many formal operations can now be performed online. Hence, the rate of computer literacy of the society will be the expected level. However, if we consider the current literacy and level of computer literacy in Turkey, the suggested e-voting scheme should be very simple and

[1] Turkish Statistical Institute (TÜİK), ADNKS Data Base, National Education Statistics Database, 27.05.2010
[2] TÜİK News Bulletin -148, 18 August 2010
[3] UNESCO Institute for Statistics, National literacy rates for adults (15+), available from UIS website, http://www.uis.unesco.org (accessed 23 February 2011)

understandable. Preferably, it can resemble or be in parallel to the current classical voting scheme in Turkey.

Figure 5: Both sides of a Prêt à Voter ballot receipt



3.2. Cost-Efficiency and Cost-Effectiveness of Referendums in Turkey

It should not be considered that e-voting will bring cost advantages immediately. There will be initial costs such as development, deployment and certification of the system. During the voting process additional IT personnel should be hired to fix computer or system incidences. If Prêt à Voter is considered, apart from ballot boxes, printers and scanners will be needed in the voting processes. However, these equipments will be re-used for future elections and referendums as well and the securely storage and re-usage of these equipments will bring extra costs.

Maintenance, machine storage, servers, overhead,

Figure 5: 2010 Referendum in Turkey (Foreign people are not considered)

Item	**Total**
Voters	49.446.269 o 24 million Men o 25 million Women
Competent served people	1.061.137
Ballot box	150.000
watermarked paper	70 tons
Envelopes	50.965.853
Cost (including the voting and whole maintenance)	TL 154.989.528 (1 Euro = 2.2 TL)

Tallying process will be cost advantageous in e-voting. In e-voting, however, cost advantageous precautions can be taken to ensure the authenticity of the ballot boxes before and after the voting processes.

Now, let us look at the cost of using Prêt à Voter scheme in a referendum. First of all, for each of provinces, there would be some tellers and registrars who are able to decrypt the encrypted votes. These tellers and registrars are chosen from a variety independent parties and government. For technical requirements, we need a number of server-side voter centers in which whole digitized votes are gathered from small vote center periodically or real-time. The number of vote centers can be the numbers of cities in the country so 81 vote centers are required in the Turkey. Each vote center consists of many small vote centers that in each small vote center there are 5 booths on average. At each booth, 400 votes can be processed in a day time, so 50.000.000/400 = 125.000 booths are required. Since on the average 5 booths can be merged, 25.000 small vote centers are required. In each small vote center, a computer and a scanner is needed. These hierarchies are summarized in Figure 6.

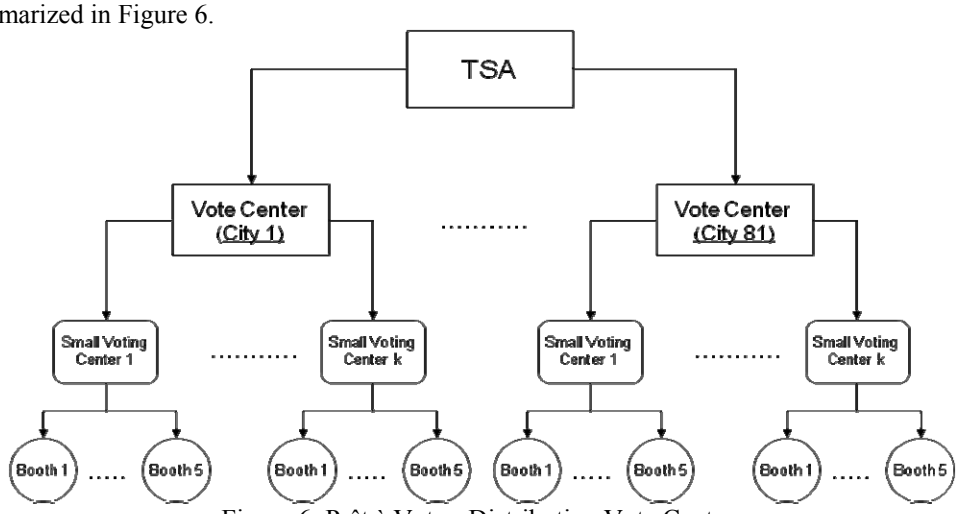


Figure 6: Prêt à Voter: Distribution Vote Centers

The voting and counting process are simply performed as follows. First of all, the vote forms are generated by Turkish Election Authority with help of tellers and registrars. These forms are distributed to each province and small voting centers. Now, the voting process is performed as follows: During the registration, a voter first comes to a small voting center and he/she verifies his/her own identity in order for vote. After the identity verification, the voter gets a random form in the center and goes into a random booth. He/she cast his/her vote in the booth and he also destroys some part of the form in the booth. After that, he/she comes back to the vote center and the casted form is digitized by the scanner and signed by a digital signature. The digital votes are sent through vote center in the province. In each vote center, we need a back-end server which collects the votes and backup them securely.

After the vote process done successfully, a sufficient number of tellers of the city combine their secret shares and do the counting process by the underlying threshold cryptosystem. The results are sent to Turkish Election Authority via a secure channel. The copies of the votes are also sent to

Turkish Election Authority in order to keep it for safety. The voters can also verify whether their votes are counted in the counting process through Turkish Election Authority's website.

Compared to the classical voting process, 25000 computers and scanners will be needed. If a computer with scanner costs about 1000 TL, then the overall additional costs for voting process would be around 25.000.0000 TL. For the counting process, about 81 servers are needed (one for each city). If each server costs about 10.000 TL then the additional cost for counting process will be 810.000 TL. Note that the adaptation of the new technology to the society and the overhead costs are excluded. Hence, total additional cost for providing vote verifiability is about 26.000.000 TL (1 Euro is 2.2 TL).

4. DISCUSSION AND CONCLUSION

With today's technologies, electronic voting is becoming popular in elections (also in Turkey) and is already used in several countries around the world. Unlike Western countries, there are several strong geographical, cultural, economical and political differences involved in Turkey. Particularly in Turkey, difficulty of mobility on the voting day and having no special voting mechanisms for citizens abroad are the two major problems with the current system. Therefore, from politics to election authorities many people are willing to make the system more flexible and more secure. Cryptography is the most important part of the system in order to guarantee its security. Without cryptography it is almost impossible to have a secure e-voting system. There have been many voting systems proposed in the literature, some of which are even practically used in several countries. We note that every country has its own culture and therefore, it is important to have a special designed voting system for Turkey. Still, it is good to have a case-study using well-known voting examples for referendum, local and parliament elections.

In this paper, we analyze referendum using Prêt à Voter scheme. The referendum requires only two "YES" and "NO" choices in the voting form. The use of Prêt à Voter is a simple example for electronic voting in which the user has ability of verifying his own vote during the counting process. However, the use Prêt à Voter will become impractical as the number of choices increase because a big letter papers for voting forms are required to fill whole candidates and so the process of scanning the papers correctly and voting would be more difficult. Besides, in that case, the very fast and sensitive scanners are required, so the cost of voting would be increase rapidly.

BIBLIOGRAPHY

[ACDMTV05] Akritidis, Periklis , Yiannis Chatzikian and Manos Dramitinos and Evangelos Michalopoulos and Dimitrios Tsigos and Nikolaos Ventouras (2005), "The VoteSecure TM Secure Internet Voting System", *Lecture Notes in Computer Science*, Vol. 3477, pp. 420-423.

[Aus09] ÖH-Wahl (2009), E-voting for the 2009 elections of representatives of the Association of Austrian students of post-secondary level education, http://www.oeh-wahl.gv.at/Content.Node/33092_3.php, [Accessed 23.03.2011].

[CC06] Deniz Cetinkaya, Orhan Cetinkaya, E-Seçim Uygulamaları için Gereksinimler ve Tasarım İlkeleri. "Türkiye'de İnternet" Konferansı Bildirileri 21 - 23 December 2006 (in Turkish).

[EES] Estonia E-Voting System, http://www.vvk.ee/public/dok/Yldkirjeldus-eng.pdf, [Accessed 28.03.2011].

[JCJ02] Juels Ari, Dario Catalano and Markus Jakobsson (2005), "Coercion-resistant electronic elections", *WPES '05*, pp. 61-70.

[Sch04] Bruce Schneier (2004), What's Wrong With Electronic Voting Machines?, http://www.schneier.com/essay-068.html, [Accessed 23.03.2011].

[MA06] Melda Akin, Elektronik Oy Verme Sistemlerinde Güvenlik : Deneyimler ve Öneriler. Ekonometri ve İstatistik Sayı:3 2006- 12-11 (in Turkish).

[Net06] About EDRI-gram (2006), European e-voting machines cracked by Dutch group, http://www.edri.org/edrigram/number4.19/e-voting, [Accessed 23.03.2011].

[NVS] E-Vote 2011- Pilot Project, Norway. http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658, March 28, 2011.

[CD07] Orhan Cetinkaya, Ali Doganaksoy: A Practical Verifiable e-Voting Protocol for Large Scale Elections over a Network. ARES 2007: 432-442.

[CC07] Orhan Cetinkaya, Deniz Cetinkaya: Towards Secure E-Elections in Turkey: Requirements and Principles. ARES 2007: 903-907.

[DC83] David Chaum, Blind signatures for untraceable payments, Advances in Cryptology - Crypto '82, Springer-Verlag (1983), 199-203.

[EV], Electronic Voting, http://www.e-voting.cc/, [Accessed 28.03.2011].

[RAD78] R. Rivest, L. Adleman, and M. Dertouzos, “On data banks and privacy homomorphisms” in Foundations of Secure Computation,pp. 169–177, Academic Press, 1978.

[RS06] P. Y. A. Ryan and Steve A. Schneider (2006), “Prêt à Voter with Re-encryption Mixes”, *ESORICS*: 313-326.

[RP09] P.Y.A. Ryan and and Thea Peacock (2009), “Putting the human back in voting protocols”, *In Fourteenth International Workshop on Security Protocols,* LNCS: 5087, pp. 13–19.

[YSK] Turkish Supreme Committee of Elections, http://www.ysk.gov.tr, [Accessed 28.03.2011].