ISSN: 1306-3111/1308-7223 Status : Original Study
NWSA-Technological Applied Sciences Received: February 2012
NWSA ID: 2013.8.3.2A0082 Accepted: July 2013
E-Journal of New World Sciences Academy

Edip Şenyürek
Turgut Özal University, esenyurek@turgutozal.edu.tr, Ankara-Turkey
İbrahim Yakut
Anadolu University, iyakut@anadolu.edu.tr, Eskisehir-Turkey

http://dx.doi.org/10.12739/NWSA.2013.8.3.2A0082

A BRIEF SURVEY ON ELECTRONIC VOTING

ABSTRACT

With the evolution of technology over many applications, electronic voting mechanisms have been also developed and realized into practice. In this study, we focus on electronic voting from legal, technical and social requirements to the security mechanism provided by cryptographic techniques. We also examine related applications and practices at a glance. After giving e-voting preliminaries, we discuss e-voting in context of Turkey’s perspective.

Keywords: Electronic Voting, Homomorphic Encryption, Paillier Cryptosystem, Mechanism, Decoding

ELEKTRONİK OYLAMA ÜZERİNE KISA BİR ARAŞTIRMA

ÖZET

Teknolojinin birçok uygulama üzerine gelişmesiyle, electronik oylama mekanizması da gelişmekte ve pratiğe dökülmektedir. Bu çalışmada, Elektronik oylamanın yasal, sosyal ve teknik açıdan gereksinimlerini kriptografik tekniklerle yapılan güvenli mekanizmalarla sağlanması üzerine odaklanılmıştır. Ayrıca pratikte uygulanan benzer çalışmalar da incelenmiştir. E-oylama hakkında genel bilgiler verildikten sonra, e-oylamanın Türkiye perspektifi tartışılmıştır.

Anahtar Kelimeler: Elektronik Oylama, Homomorfik Şifreleme, Paillier Kriptosistemi, Mekanizm, Şifre Çözme

1. INTRODUCTION (GİRİŞ)

With the evolution of technology electronic applications for online environment have become more essential components for the business and daily life. Like online education, management information systems, online shopping, remote tracking so many tasks can be done on a computer that is connected to a network. Even, electronic voting (e-voting) mechanisms are developed for voting through secure network rather than using conventional election setup. An electronic voting scheme is a set of protocols which allow voters to provide ballots while a group of authorities collect the votes and output the final tally [1].

The classical voting systems on ballot box bring some disadvantages with it. Such problems are the difficulty of the specification of the vote for which candidate, the possibilities of to put the vote to wrong ballot box, the problems of counting level, documentation and the expenditures of election [2]. If security metrics are satisfied, more scalable and reliable elections can be carried out by means of e-voting methods [1].

In this study, we examine e-voting schemes through requirements for appropriate elections, developed technologies and recent e-voting applications among different countries. We also present a common cryptographic mechanism used in many e-voting schemes, as well. Finally we discuss the feasibility of e-voting in the context of Turkey.

2. RESEARCH SIGNIFICANCE (ÇALIŞMANIN ÖNEMİ)

In this study, we focus on electronic voting from legal, technical and social requirements to the security mechanism provided by cryptographic techniques. We also examine related applications and practices at a glance. After giving e-voting preliminaries, we discuss e-voting in context of Turkey’s perspective.

3. REQUIREMENTS FOR E-VOTING (E-OYLAMA GEREKSİNİMLERİ)

In a typical election scheme, the main issues to be satisfied can be listed as privacy of voters, anonymity of votes, public verifiability of so anonymous votes, and robustness of voting mechanism. To develop an authoritative e-voting system, we should also respond the requirements ensuring such issues. In [3], the requirements are discussed in the context of e-voting. These requirements can be categorized as legal, technical and social requirements.

3.1. Legal Requirements (Yasal Gereksinimler)

The legal requirements should be fulfilled in order to obtain legally valid election results. They can be listed as

- **Privacy of vote:** Any vote shouldn’t be associated to voter of it.
- **Right of voting:** Only the registered voters can vote, not the others.
- **Uniqueness of vote:** A voter should vote once, i.e. not more than one vote.
- **Announcement of the results:** The results should be announced, publicly.

3.2. Technical Requirements (Teknik Gereksinimler)

Following technical requirements should be provided to set up robust e-voting system:

- **Accuracy of results**: The votes should be counted correctly. Any vote cannot be changed, deleted or copied.
- **Vote must unproven**: A voter shouldn't proof how he/she voted.
- **System verifiability**: Voting and tallying should be proven that is correct.
- **Receipt-freeness**: a voter does not obtain any receipt-like information which can be used to prove the given vote.
- **Personal verification**: A voter should be ensured that his/her vote is counted.
- **System efficiency**: Registration, voting and tally should be done in efficient time.
- **Open source software**: Source code could be inspected while keys and encryption system should be secret.
- **Backup and physical security**: E-voting system must have a backup system and reliability mechanism for technical faulty.
- **Safekeeping the votes**: All the votes should be saved in a safe place after voting on hard copy and digital as well.
- **Fairness**: No partial results are revealed before tallying.
- **Recountability of the votes**: Votes, which are saved on digital and/or hard copy, could be counted again.

3.3. Social Requirements (Sosyal Gereksinimler)

- **Coercion-resistance**: Nobody should put pressure on and direct the voter for intention of voters. There is no way to sell/buy votes.
- **Right of abstention**: If a voter wouldn't like to vote, he/she must not vote.
- **Right of cancellation of voting**: Voter should cancel her/his vote before sending the vote.
- **Right of blank voting**: Voter should be able to vote blank
- **Easy to use**: For voting no need to have special ability. Everbody can vote.
- **Transparency of election**: Privacy of votes and voters should be preserved and all the other components of the e-voting system should be transparent.

4. E-VOTING APPLICATIONS (E-OYLAMA UYGULAMALARI)

Kapıdere et al. [4], mentioned that the e-voting can be categorized into two with respect to placement:

- Polling place e-voting
- Remote e-voting

While the former one is more similar to conventional election methods, the remote e-voting is more complex to prove in security and reliability. According to [4 and 5], e-voting methods can be performed over five different mechanisms:

- Punch card that has holes on it.
- Paper-based ballot forms
- Special electronic device as a ballot collector.
- Voting over telephone.
- Internet-based voting.

Initial three mechanisms can be exploited for polling place e-voting and in such mechanisms the main modification is a particular device usage instead of ballot box. Well-known example for paper-based ballot form is Prêt à Voter which uses special forms that are turned into encrypted receipts to provide security and auditability [6]. Along all mechanisms, there are needs for robust infrastructures to realize e-voting processes and many e-voting schemes are proposed in this context [1 and 6].

E-voting has become realized since the first use in USA and Europa in early 1990s and several e-voting systems were tried and/or put into practice by many countries, worldwide [8]. In 2000, Australian parliamentary election was done by e-voting. In 1996, about 30% of Brazilian voters were able to cast their vote with Direct Recording Electronic Voting System. In Estonia, the e-voting system started in 2001 with the use of smart cards and electronic signatures. India is using Electronic Voting Machine (EVM) since 1998. In 2003, all state elections were done by EVMs. E-voting is not a first priority of the government in Austria. A first test of remote e-voting was done at Student Union election at Vienna University of Economics and Business Administration, in May 2003. In Ontario, a state of Canada, first in November 2003, e-voting system was done in 5 days. The voting was via internet or via telephone.

According to [8], in 2010 e-voting was done by voting machines in Australia, Brazil, Canada, France, India, Japan, Kazakhstan, Peru, Russia, United States of America, United Arab Emirates and Venezuela. Additionally, e-voting via internet was done in Austria, Canada, Estonia, France, Japan and Switzerland. Countries such as Argentina, Azerbaijan, Belarus, Bulgaria, Chile, Czech Republic, Finland, Greece, Italy, Latvia, Lithuania, Mexico, Nepal, Nigeria, Norway, Peru, Poland, Portugal, Romania, Slovakia, Slovenia, South Africa, Spain, South Korea and Sweden are planning or trial to e-voting system. However, in Germany, Ireland, The Netherlands and United Kingdom the e-voting systems were terminated.

5. CRYPTOGRAPHIC MECHANISMS FOR E-VOTING (E-OYLAMA İÇİN KRİPTOGRAFİK MEKANİZMALAR)

The problem of “e-voting” takes attention cryptography researchers and there are several many cryptographic mechanisms to perform e-voting tasks [1, 7 and 9]. In this context, homomorphic encryption schemes is a versatile mechanism which allows perform mathematical operations on ciphertexts [9]. In this study, among the many proposed homomorphic cryptosystems, Paillier cryptosystem is examined since it is preferred by many e-voting methods [1 and 7].

The Paillier Homomorphic Cryptosystem (PHC) is a modular, public key encryption scheme, created by Pascal Paillier in 1999. PHC is based on probabilistic public key infrastructures and it has several interesting properties [4]. The important property of PHC is the addition of plaintexts through multiplication of ciphertext. Such property constitutes potential baseline to a form of e-voting. PHC is additive homomorphic cryptosystem. That means, as shown in Eq.(1), with the given public key, the encryption of two different messages m1 and m2 will be the same result of the encryption of the $\mathbf{m_1 + m_2}$

$$\boldsymbol{\varepsilon}(\mathbf{m_1 + m_2}) \equiv \boldsymbol{\varepsilon}(\mathbf{m_1}) \cdot \boldsymbol{\varepsilon}(\mathbf{m_2}) \quad (1)$$

PHC consists of three processes such as key generation, encryption, and decryption which can be summarized as the following text.

5.1. Key Generation (Anahtar Oluşturma)

Firstly two large prime numbers denoted by $\mathbf{p}$ and $\mathbf{q}$ should be chosen randomly and independent from each other provided that

$$\mathbf{gcd\,(pq,(p-1)(q-1))=1,} \tag{2}$$

where gcd stands for greatest common divisor. The multiplication of these prime numbers will be $\mathbf{n=pq}$ and $\boldsymbol{\lambda}$ can be computed as $\boldsymbol{\lambda}=\mathbf{lcm(p-1,q-1)}$ where $\boldsymbol{\lambda}$ and lcm are Carmichel's function and least common multiplier, respectively.

The next step, integer numbers α and β is selected from Zn, to determine generator

$$\mathbf{g=(\alpha n+1)\beta^n mod\,n^2,} \tag{3}$$

where $\mathbf{Z_n}$ and $\mathbf{Z^*_{n^2}}$ are set of integers n and set of integers coprime to $\mathbf{n^2}$, respectively.

Then the public key, for encryption, generates as $\mathbf{(n,g)}$ and the private key, for decryption, generates as $\mathbf{(\lambda,\mu)}$. $\boldsymbol{\mu}$ can be computed as

$$\mathbf{\mu=\left(L(g^{\lambda}\,mod\,n^2)\right)^{-1}mod\,n,} \tag{4}$$

where L is defined as $\mathbf{L(u)=\frac{u-1}{n}}$. (5)

5.2. Encryption (Şifreleme)

The message is m where $\mathbf{m\in Z_n}$ and selected random r where $\mathbf{r\in Z^*_n}$ where $\mathbf{Z^*_n}$ is set of integers coprime to n. Then the ciphertext can be computed as

$$\mathbf{c=g^m r^n\,mod\,n^2} \tag{6}$$

5.3. Decryption (Şifre Çözme)

The ciphertext is c where $\mathbf{c\in Z^*_{n^2}}$ and to decrypt the ciphertext use the equation:

$$\mathbf{m=L\left(c^{\lambda}\,mod\,n^2\right)\mu\,mod\,n.} \tag{7}$$

5.4. Homomorphic Properties (Homomorfik Özellikler)

The PHC has additive homomorphism property; however, multiplication operation can be derived from such addition property. Homomorphic addition of two given values $\mathbf{m_1}$ and $\mathbf{m_2}$ where $\mathbf{m_1,m_2\in Z_n}$ via PHC can be shown algebraically as the following; Let $\mathbf{r_1}$ and $\mathbf{r_2}$are randomly selected numbers where $\mathbf{r_1,r_2\in Z^*_n}$. According to Eq.(3) the ciphertexts are computed as

$$\mathbf{c_1=g^{m_1}{r_1}^n\,mod\,n^2} \tag{8}$$

$$\mathbf{c_2=g^{m_2}{r_2}^n\,mod\,n^2} \tag{9}$$

$$\mathbf{c_1*c_2\,mod\,n^2=g^{m_1}{r_1}^n*g^{m_2}{r_2}^n\,mod\,n^2} \tag{10}$$

Then the Eq.(10) becomes,

$$\mathbf{g^{m_1+m_2}(r_1*r_2)^n\,mod\,n^2} \tag{11}$$

When the Eq.(11) is decrypted using Eq.(7), the result will be

$$\mathbf{m_1+m_2\,mod\,n} \tag{12}$$

Homomorphic multiplication of two given values and selected random numbers as in Eq.(10). Taking the exponent $\mathbf{m_2}$ of $\mathbf{c_1}$ then,

$$\mathbf{{c_1}^{m_2}mod\,n^2=(g^{m_1}{r_1}^n)^{m_2}mod\,n^2} \tag{13}$$

$$\mathbf{g^{m_1m_2}{r_1}^{nm_2}\,mod\,n^2} \tag{14}$$

When the Eq.(10) is decrypted using Eq.(7), the result will be

$$\mathbf{m_1*m_2\,mod\,n.} \tag{15}$$

5.5. Voting and Tallying (Oylama ve Sayım)

In this part, we show how PHC can be used for e-voting on numerical example. Assume that there are 6 voters having at most one-vote right as in Turkey parliamentary elections and 3 candidate parties, namely A, B, and C. Since the number of voters is less than 10, we can assign a decimal digit for each party and let assign most significant digit to A as $\mathbf{10^2}$, intermediate digit to B and least significant digit to C as $\mathbf{10^1}$. Then, plain vote values can be just equal to each parties assigned digit value. Then, maximum plain vote value is 100 and possibly maximum total plain vote value ($\boldsymbol{T_{max}}$) is 600.

Then, with the specification of the inputs above the election authority (EA) can set up keys:

- Since modulus (n) should be greater than $\boldsymbol{T_{max}}$ then n>600. Select p and q having the similar length where $\mathbf{q > \sqrt{600} = 24,5}$. Selection of $\mathbf{p = 23}$ and $\mathbf{q = 29}$ that provides Eq.(2). Then $\mathbf{n = pq = 23 \cdot 29 = 667}$ and $\mathbf{n^2 = 444889}$
- $\boldsymbol{\lambda}$ can be computed by finding lcm of values (p-1) and (q-1) then $\boldsymbol{\lambda} = \mathbf{308}$.
- $\mathbf{g}$ can be evaluated using Eq.(3), first let α=2 and β=3. $\mathbf{g = (2 \cdot 667 + 1)3^{667} mod\, 444889^2 = 372165}$
- According to Eq.(4), $\boldsymbol{\mu}$ is modular inverse of $\mathbf{L(372165^{308} mod\, n^2)}$ under $\mathbf{mod\, n}$. Then, $\boldsymbol{\mu} = \mathbf{170}$.

All public and private keys are computed respectively as $\mathbf{(n, g) = (667, 372165)}$ and $(\boldsymbol{\lambda}, \boldsymbol{\mu}) = \mathbf{(308, 170)}$

In the second step, voters can contribute their votes into e-voting process. Voting procedure is as follows:

For each $\mathbf{voter_i}$

- Select your party and compute plain vote ($\boldsymbol{m_i}$).
- Select random r where $\mathbf{r \in Z_n^*}$.
- Compute encrypted vote $\mathbf{c_i = g^{m_i} r_i^{\,n}\ mod\ n^2}$.
- Send $\mathbf{c_i}$ to the ballot server.

Also let each voters gives vote as in Table 1 where 1s stand for preference of $\mathbf{voter_i}$ to the corresponding party. Note that $\mathbf{voter_5}$ provides blank votes. We also calculate ciphertexts for our example and display them in Table 1 with randomly determined $\mathbf{r_i}$. The last column shows the interesting property of PHC. Although there are the same plain votes (e.g for parties B and C), no encrypted votes are identical. This is the self-blinding property of PHC which hides the same plaintext. By the way, nobody can distinguish the same votes from looking encrypted votes

Table 1. Voter's Preferences on Candidates
(Tablo 1. Seçmenlerin Aday Tercihi)

	Party A ($\mathbf{10^2}$)	Party B ($\mathbf{10^1}$)	Party C ($\mathbf{10^0}$)	Plain Vote ($\boldsymbol{m_i}$)	$\boldsymbol{r_i}$	Cipher Vote ($\boldsymbol{c_i}$)
voter1			1	1	11	382987
voter2		1		10	16	399542
voter3	1			100	3	239434
voter4		1		10	7	378617
voter5				0	4	188194
voter6		1		10	123	406370
Total	1	3	1	**131**		

The last step of election is tallying and it is performed via the additive homomorphism property of PHC given in Eq.(10). Encrypted version of resultant tally ($\mathbf{T_{final}}$) of the given votes can be obtained multiplication of cis given in Table 1 as

$$\boldsymbol{\varepsilon}(\mathbf{T_{final}}) = \mathbf{382987 \cdot 399542 \cdot 239434 \cdot 378617 \cdot 188194 \cdot 406370 = 156068 \bmod 444889}$$

After EA decrypts $\boldsymbol{\varepsilon}(\mathbf{T_{final}})$ with private keys $(\boldsymbol{\lambda}, \boldsymbol{\mu})$ then $\mathbf{T_{final}}$=131. Digit-10 (being 3) is greater than the other digits, then EA announces that Party B wins the elections.

We give comprehensible and brief example to demonstrate how to set up election by means of PHC. However, there are large scale e-voting schemes based on cryptographic mechanisms [1, 6]. For example, Baudron et al. [1], presented PHC-based multi-candidate election system that can tolerate any number of participants and candidates. In their system the voting will be casted 1, 0 or null. On their voting scheme, each authority has their own public key. Figure 1 shows the hierarchical levels and organization of the authorities [1]. Consider a voter, from second local level of third regional level, would like to vote for $\boldsymbol{m^{th}}$ candidate, needs public keys those pk for national level, $\mathbf{pk_3}$for regional level and $\mathbf{pk_{3,2}}$ for local level. Each user compute three distinct encrypted votes and proof values for each level with corresponding public keys [1]. At the end of voting process, all the authorities tally the votes own and verified the result.

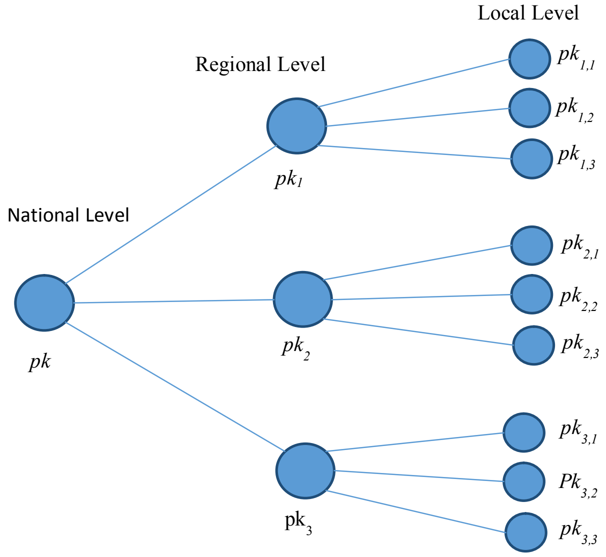

Figure 1. Organization hierarchy of the authorities [1]
(Şekil 1. Otoritelerin organizasyon hiyerarşisi [1])

6. CONCLUSIONS (SONUÇ)

In this section, we give SWOT-based analysis on e-voting for our country Turkey case. First of all, strengths of the e-voting system:

- There are many e-government solutions and e-applications are provided by governmental agencies. By the way, Turkey have a great deal of experience about information technologies.
- The Internet is widely exploited by public and there is substantial communication infrastructure such as fiber-optic networks etc.
- Population of Turkey includes the majority of young and dynamic citizens who can be easily adapted to novel e-voting schemes

- There are sophisticated and well-educated people graduated from universities who can easily carry out the assignments given in e-voting realization process.

Weakness of Turkey can be listed in the context of e-voting application:

- There are some people being uneducated and unconsciencous about informatics. E-voting system should be user-friendly especially for such people.
- Despite strong communication network, some authorized staff can access contents of data flew in network. These issues should be handled.

Following opportunities promised if e-voting system is realized:

- Work load for election would become less for the government and election authorities and agencies compared to conventional voting system. By the way the tallying would be more faster
- The initial establishment costs will be higher but the routine expenditure would be much more less for each election setup.

Threats of the e-voting system:

- Elections are too critical events and many malicious attacks can be expected. Virus-oriented software and attacks intended to manipulate voting results to the information technologies of the system.
- Crucial faults and interruptions can be occurred through electrical power systems and communication networks. The election centres should be equipped with devices such as generators, UPSs and initially communication networks may be planned for alternative communication pathways should be defined for e-voting such as if fiber-optic communication is down then immediately return to 3G or public phone network etc.

Considered above mentioned strengths, Turkey has sufficient potential however weaknesses and threats should be considered extensively and well-suited solutions should be realized. By upgrading to e-voting systems, the country reduces election costs and workloads. Moreover, if all requirements given in Section II is provided and the security metrics are justified, then more dependable and reliable election results will be achieved.

NOT (NOTICE)

Bu çalışma, 20-21 Mayıs 2013 tarihleri arasında Elazığ Fırat Üniversitesinde yapılan 1.Uluslararası Adli Bilişim ve Güvenlik Sempozyumunda sözlü sunum olarak sunulan çalışmanın hakemlik sürecinden geçirilmiş ve yeniden yapılandırılmış halidir.

REFERENCES (KAYNAKÇA)

1. Baudron, O., Fouque, P.A., Pointcheval, D., Poupard, G., and Stern, J., (2001). Practical Multi-Candidate Election System. Rhole Island, USA. In Proceedings of the 20th ACM Symposium on Principles of Distributed Computing.
2. Bilgin, M., (2013). Biyometrik Tabanlı E-Seçim Sistemi. Antalya, TR. In Proceedings of Akademik Bilişim 2013.
3. Çetinkaya, D. and Çetinkaya, O., (2006). E-Seçim Uygulamaları Için Gereksinimler ve Tasarım Ilkeleri. Ankara, TR. In Proceedings of the Eleventh Conference on Internet.
4. Kapıdere, M., Doğan, N., and Çinpolat, A., (2007). Türkiye Için Yeni Bir Electronik Seçim. Kütahya, TR. In Proceedings of Akademik Bilişim 2007.

5. Telciler, C., (2007). Elektronik Seçim Sistemi. Kütahya, TR. In Proceedings of Akademik Bilişim 2007.
6. Ryan, P.Y.A, Bismark, D., Heather, J., Schneider, S., and Xia, Z., (2009). The Prêt à Voter Verifiable Election System. IEEE Transactions on Information Forensics and Security. Volume: 4 (4), pp: 662–673.
7. Damgård, I., Jurik, M., and Nielsen, J.B., (2010). A Generalization of Paillier's Public-Key System with Applications to Electronic Voting. International Journal of Information Security. Volume: 9(6), pp: 371-385.
8. http://aceproject.org/ace-en/focus/e-voting/countries, Countries with e-voting projects, ACM Projects, (Access Date: 07.04.2013).
9. Paillier, P., (1999). Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Prague, Czech Republic. In Proceedings of EUROCRYPT '99 Proceedings of the 17th international conference on Theory and application of cryptographic techniques.