The Analysis of Current State and Future on the E-voting System

Her, Yong-Sork
Dept.Computer & Communication Enginnering,Taegu Univ

Sakurai, Kouichi
Dept. Computer Science & Communication Enginnering Kyushu Univ

出版情報：Proc.of the 2002 Symposium on Cryptography and Information Security. I, pp.537-542, 2002-01. Symposium on Cryptography and Information Security
バージョン：
権利関係：

The Analysis of Current State and Future on the E-voting System.

Yong-Sork HER[1] , Kouichi SAKURAI [2]

ysher2001@hotmail.com sakurai@csce.kyushu-u.ac.jp

Abstract

In recent years, a new vote methods have been developing and studying in many countries In this paper, The first, we explain the necessity and whole of structural elements in e-voting. The second, we analysis the developing or proposed e-voting. Finally, we anaysis the current state of e-voting and shows the future of the e-voting development.

Key word Voting, PKI, Authentication, Confidence, Digital signature

1. Introduction

In this thesis, we conduct research on the area of e-voting, one of the most critical areas of e-Politics. There are a number of voting methods currently being employed by various countries. But, the losses related to manpower, time, and money in carrying out voting are still far too great for most countries. Moreover, at the moment, the voters' political indifference poses a more significant threat: It translates directly to a decrease in votin-g ratio. Due to such reasons, the development of new voting method can be said to be an important project of national significance. The fact that div-erse forms of e-voting where convenience, efficiency, and accuracy are punctuated via the advancement in electronic and information and telecommunications technologies are currently being developed is a testament to such claim.

2. Structural elements in E-voting

2.1 Requirements for E-voting

The core of voting is only legal voter to voting and correct counting must be getting. In voting and counting process, the contents of voting and counting haven't to being modify and omit. The key of success e-voting is due to a correct voting and a exact counting. For it do so, it keeps as following.

- All voter be authenticated
- All legal voter can vote only one
- All voter cann't to make any action after voting
- Nothing haven't to affect the voting
- The e-voting system is provided the secret

.2.2 Registration

In traditional voting method, voter can enter the voting place after compared with a pollbook and identification card. The voter authentication can be considered a core technology, along with the encryption of voting result. Differences exist, however, in voter authentication methods according to which e-voting system is used. The method where a password is given to each voter from a voting place through an election management committee is used most frequently. But a diverse range of methods have been proposed, including a special electronic citizen identification and fingerprint recognition device. Differences also exist whether the voting place will be traditional voting places or the voter's home, office, or public buildings. Certainly the former would be considered more secure than the latter but the latter would coincide with the development path of e-voting. Only valid voters should be allowed to vote.

2.3 Voting and Encryption transmission

The crux of the voting system is in proper voting and accurate tallying. The introduction of new e-voting in place of the conventional voting method could find justification in its convenience and accuracy. On the issue of accuracy, the encryption technology is mandatory in order to prevent alteration or forgery of vote counting. But the tandem of security and hacking and that of encryption and decryption is an endless struggle. There are scholars who go as far as saying, 'Cryptography is not the problem. Many wonderful cryptographic voting protocols have been

[1] Dept.Computer & Communication Enginnering,TaeguUniv, 15 Nariri, Jinyang, Kyungsan, Kyungbuk. 712-714, Korea

[2] Dept. Computer Science & Communication Enginnering, Kyushu Univ, 6-10-1, Hakozaki, Fukuoka, 812-8581,Japan

proposed.'[21] But the encryption technology need to be developed on a sustained basis as long as hacking exists.

2.4 Computerized Vote-Tallying and Ballot Counting

The most important aspects in computerized vote-tallying are accuracy, integrity, and security. Accuracy, especially, is the most fundamental factor in computerized vote-tallying and is based on integrity and security. This aspect is one of the purposes of developing e-voting in the first place and could also minimize the loss in manpower and time associated with the conventional voting method.

3. Cryptography using the e-voting

3.1 The classification of the e-voting by technology

There are various kinds of the vote. A representative votes are pros and cons vote for deciding the opinions and a election vote for electing a representative.

In present, the developing e-voting is two types ; one is the type of using multi-party protocol, the other is the type of using anonymous channel[26].

The e-voting using the anonymous channel of mix type is the first by Chaum, Digicash corp. As the anonymous channel of mix type is used RSA , the e-voting used the public key scheme is seems the improved or extended vision of a Charm.

The compare of these is as Table 1 [19].

Table 1 . The compare by each methods of e-voting

Classfication	Multi-Parry Protocol	Anonymous Channel
Proposer	Cohen	Charm
Methods	Publickey residue cryptosystem + ZIP	Blind signature + Anonymous channel
Safety	Excellent	Good
Efficiency	Bad	Excellent
Apply vote	Pros and cons	Multi-vote
A voting scale	Small scale	Large scale
Consider items	Efficiency	The realize Problem of anonymous

3.2 The developing and proposed E-voting

To enhance the readability of this paper, we will explain the developing and proposed E-voting.

3.2.1 Sensus

The Sensus [14] is expanded on the work of 'FOO92', This uses blind signatures to ensure that only registered voters can vote and that each registered voter only votes once, while at the same time maintaining voter's privacy. Sensus allows voters to verify independently that their votes were counted correctly, and anonymously challenge the results should their votes be miscounted.

Registrar

The register implementation requires that each voter be sent a voter identification number (which need not be secret) and a secret token T prior to the registration process. Eligible voters generate public/private key pairs and register to vote by sending the register their voter identification number, T, and public key. The register verifies that the applicants have submitted the correct tokens and adds their identification numbers and public keys to the registered voter list. The registered voter list also contains a validation field for each voter which is set to 0 before each election and changed to 1 by the validator after a voter's ballot is validated.

Validator

The Validator uses the registered voter list to obtain each voter's public key and check the signature on their ballots. The validator changes the contents of the validation field from 0 to 1 after validating a ballot. With this method no record is kept of the order in which ballots are validated.

Tallior

The tallior computes a 16-byte digest of each encrypted ballot received and uses it to index the encrypted ballots and receipts. A hash table could be added for greater efficiency in looking up encrypted ballots. This modifications is probably necessary to accommodate large-scale elections.

3.2.2 OMAFO99 Scheme

In this scheme[13],Voter's privacy is guaranteed by using blind signature and mix-net, and robustness is provided through the threshold encryption scheme. This system is figured as Fig1following.

(1) Voter Authentication
    Voting + Encryption +Blind signature
(2) Voting
    Voting +Encryption +Signature
(3) Opening
    Threshold Decryption

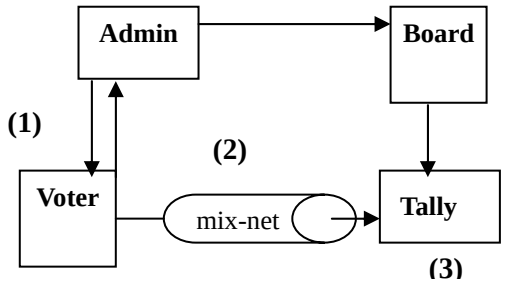

Fig 1. The overview of OMAFO99 scheme

4. The Proposal of E-voting using the PKI and Korea-PIN

4.1 PKI

4.1.1 . PKI components

Usually, the PKI makes used of digital signature (or Electronic signature)in the network. PKI is based on the use of public key cryptography. Public key cryptography play an important
This is provides the assurances users need before they can confidently transmit sensitive information over the Internet and other network.
The components of PKI is the following. [18]
- PAA : Policy Approving Authority
- CA : Certificate Authority
- ORA: Organizational Registration Authority
- Clients
- Directory Server

There are certificate and CRL (Certificate Revocation List) in the management of PKI. The message form of PKI which IETF PKIX(Public Key Infrastructure X.509) defined , is as Table 2 following :

Table 2 . The message form of PKI

Header	Body	Protection (Optional)	ExtraCerts (Optional)

4.1.2 The role of PKI in the E-voting

Public key cryptography plays an important role in providing security services such as confidentiality, authentication, digital signatures, and integrity. Especially,
It is the voter certification. One person (certificat-e)- One voting, that is prevented the multi -voting. And the only legitimate person can voting. The role of PKI in the e-voting via Internet was figured as Fig 2 the following.

4.2 The Korea-PIN

A Korean have the Korea-PIN(Personal Identification Number) from the registration of a birth. This Korea-PIN is consist of the 13-figures as Table 3.Generally, A Korean has been used the Korea-PIN in order to be verify oneself. Most of the paper is filled up a form.

Identity-based system

An identity-based cryptographic system (ID-based system)[1] is an asymmetric system where in an entity's public identification information (unique name) plays the role of its public key, and is used as input by a trusted authority T (along with T's Private Key) to computer the entity's Correspond-ing private key.

SSL

For Internet-based elections another simple securi-ty measure is to use a secure web server for collec-ting the votes. In that case, the communication b-etween the voter's client and the web server is pro-tected by a protocol such as SSL(Secure Socket L-ayer). Once the communication between client and server is protected by SSL, the information neces-sary for casting a vote (possibly including softwar-e such as a Java applet) may be do downloaded se-curely to the client, and the vote and authenticatio-n information may be uploaded securely to the se-curely to the server. The use of SSL thus prevents the votes from being read or altered when travelin-g over the Internet[4].

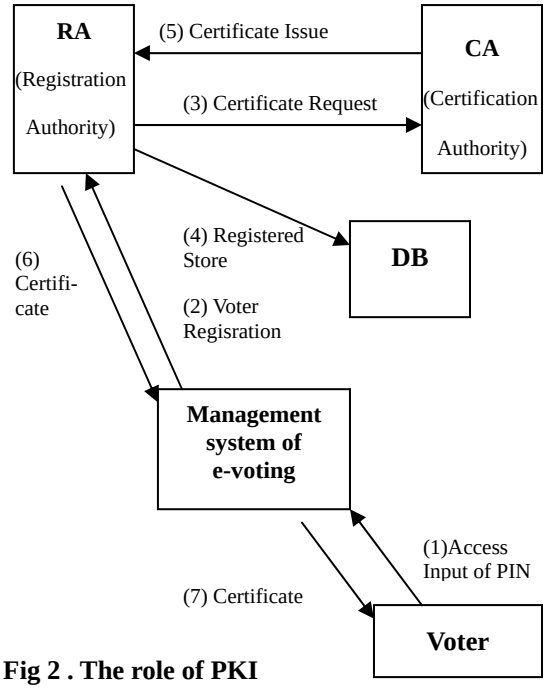

Fig 2 . The role of PKI

Table 3 . The construction of Korea-PIN

x	x	x	x	x	x	-	x	x	x	x	x	x	x
Year		Month		Date			M or F						
One's birth								Identification Number					

* If a man is Male, it is 1, or (Female) 2

4.3 A Proposal of E-voting using Korean-PIN

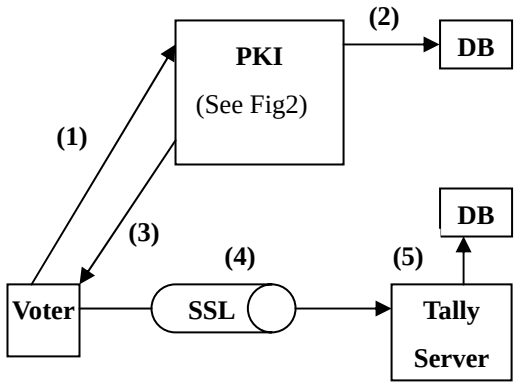

Fig 3 . The overview

4.3.1 Registration step (1)(2)(3)

- Access the PKI for registration
-The PKI send the Voter's public key for the encryption
- Generate ID and send the encrypted data (voter's ID and Korea-PIN)
- After decrypt and identify a voter's data, Certificate lssue (including K-PIN and Registered information together Tally server's public key)

4.3.2 Voting step (4)

- If voter is voting , be send the encrypted contents and K-PIN of vote via SSL
- After decrypt using Tally server's private key, automatic counting and store the DB

4.3.3 Counting step (5)

- Compare the number of counting and DB, announce the result of voting
- DB is utilized the inspection of voting

5. Current State of E-voting

The e-voting is currently being employed in some countries, including the Netherlands, Belgium, and Brazil and the trend is expected to proliferate. This e-voting method takes a form of visiting a voting place in person and voting through a computer or terminal installed at the location after which the voting result is sent to a tallying place for computerized tallying. Estonia became the first country that allowed online voting and plans to implement it for elections, beginning in 2003.[26]

5.1 America

The very first Internet voting in the United States took place in real-life situation during the Democratic Presidential Primary in Arizona from March 7 to 11 in 2000. After the U. S. Court recognized the legal validity of Internet voting, it was conducted in two ways. Voters could either access the web site of Election.com that oversaw the process during the specified 5-day period for voting or go to a voting place on March 11, the official voting date, by using the computer there. The voting proved to be a success. The total number of voters reached 85,750, a 622% increase from 12,800 recorded for 1996. The Internet voting was used by 39,942 people, assuming 46.5% of the total voters and no technical problems were reported[6][7].

Palm Beach County of Florida implemented a card-type voting based on a ballot in the shape of butterfly for the past U. S. Presidential Election. To cater to the elderly who typically suffered from weakened vision, the ballot was made in two pages to accommodate larger fonts. But such implementation resulted in a large number of votes that could not be deciphered one way or another with certainty at ballot counting, causing a great deal of controversy. To prevent this from recurring, a new legislation is in the making for introducing new voting procedures and methods.[3] In addition, Caltech and MIT are developing a new machine for voting.[6]

5.2 Europe

The CyberVote project[9] officially started on 1 September 2000 and will end on 1 March 2003.

This system will be tested in 2003 during trial election that will be held in Germany, France and Sweden. These trials will involve more that 3000 voters and will allow full assessment of the system before any potential product launch.

This project aims to an improvement of the democratic process by increasing voter participation and there by increasing the number of votes.

5.3 Japan

The General Affairs Office of Japan announced on the 23rd of the past month, "A proposal for

revising the election law for public offices will be submitted to the Diet in order to allow electronic voting and ballot counting." The Japanese Government plans to conduct an electronic election as early as the election for the provincial governorship of Hiroshima in November of 2001 and is working on revising the related laws and regulations. Japan plans to implement e-voting in the Hiroshima governorship election as a trial and plans to widen its scope ultimately to the general election after correcting for the problems that could perspire. [27]

5.4 Korea

In Korea, several companies have plans for forging an alliance with foreign companies and PIBKorea has started an election agency business through the Internet by collaborating with evotesystem.com. The Korean-style e-vote system will be linked with the IMT-2000 Project and is being pushed forward with research on wireless Internet voting system and individual authentication.

6. Future of the E-voting

In the future, an e-voting system that will have moved beyond the conventional voting method by focusing on convenience, accuracy, and security will be used. Things to consider in implementing such system will be proposed from four different perspectives in this thesis.

- Voting Place
- Education on Election administrator(officer) and Voters' Voting Methods
- Preparation for Threats to Voting Equipment
- Compatibility among Voting Equipment

6.1 Voting Place

One of the things that needs to be considered first in implementing an e-voting system is where the voting would take place: whether it should be done at a specified voting place or at a location convenient for the voter such as home, office, and various public locations. For the former case, the voter needs to confirm his registration by directly visiting the voting place for voting and the latter would require online registration. Although the latter case poses a number of technical issues that need to be hurdled, it would become the choice of voting method in the future. As for the methods in online registration, a number unique to a given voter, fingerprint recognition, and electronic citizen identification, among other things, are being used.

6.2 Education on Election administrator (officer) and Voters' Voting Methods

Voters who are familiar with the voting method that has been used for a long time may be reluctant to use a new voting method. At the same time, voters who are not familiar with the new voting equipment may encounter problems during the voting process. This may be true especially for the elderly. Avi Rubin[1] cited coercibility, vote selling, vote solicitation, and online registration as the problems with e-voting. administrator(officer) or people whose interest coincide with the candidates may impose themselves on voters, ask favors, or disburse money for votes. Therefore, educating the voters on the new voting method in advance and promoting and educating the importance of proper exercise of voting right are vitally needed. Moreover, systems employed in e-voting system inevitably need to be managed by the election management committee. One cannot rule out a possibility where the administrator alters or forges voting results with ulterior motive. In order to carry out e-voting, rigorous management of the system administrator would have to be implemented as well.

6.3 Preparation for Threats to Voting Equipment

All e-voting systems are always exposed to risk. This kind of risk may be of more serious nature than that of the conventional voting method. An intentional error by a system administrator, attack from outside, system malfunction, and even unexpected system problems could occur. No amount of preparation before the e-voting implementation could prevent mechanical problems that could occur any point in time. A secure e-voting system would result only when all possible problems are reviewed and appropriate measures instituted. In addition, this issue is also related to the issue of system security, including encryption

6.4 Compatibility among Voting Equipment

e-voting equipment currently under development typically rely on a single kind of device but in the future, more than one device (personal computers, personal digital devices, mobile phones, web phones, etc.) will be used in e-voting. In order words, voters will be able to vote by choosing the device most convenient for her. In turning such conception into reality, the issue of compatibility among various devices, including operating systems that drive devices, browsers, and input devices, will have to be considered.[10] Because

the voting method in each country differs in voting equipment, voting paper, ballot counting process and such, standardizing the system across the board could face difficulty. But a gradual standardization effort on details in hardware and software would have to proceed at this point for eventual resolution of compatibility in the future.

7. Conclusion

A various countries around the world have been trying to many study and effort in order to the new voting methods. Especially, the United States sees the need for e-voting from its experience in the presidential election in 2000 and is currently pushing for its development.

This is caused by the indifference toward the traditional voting methods and the decline of a voting rate. This e-voting will be realized in the near future due to the rapid growth of communication network and advances in cryptographic techniques. Together the develop or the techniques, a number of countries are revising election laws to cater to the e-voting system. The e-voting is propers and needs of the times.

In order for it to take root, it would require a concerted effort and trial and error. Even the very best system and equipment were used for voting, it would be in vain unless voters exercise their voting right in proper manner.

Reference

[1] A.J.Menezes, P.C.van Oorschot, S.A. Vanstone " Handbook of Applied Cryptograhpy" CRC, 1997

[2] Avi Rubin. Security Considerations for remote electronic voting over the Internet, 2000 http://avirubin.com/e-voting.security.pdf

[3] B.Schneier "Applied Cryptography" Wiley,2nd, 1996

[4] B.Schoenmakers "Fully Auditable Electronic Secret-Ballot Elections" Internet Techhology, http://www.win.tue.nl

[5] B. Schoemakers " Fully Auditable Electronic Secret-BalletElections" vol .8 , num1, Jul. 2000 **http://www.win.tue.nl/**

[6] California Institute of Technology and Massachusetts Institute of Technology. Voting technology project. http://www.vote.caltech.edu

[7] Califormia Internet Voting Task Force, Final Report. http://www.ss.ca.gov/executive/ivote

[8] Derek Dictson , Dan Ray " The modern Democratic Revolution : An Objective Survey of Internet-Based Elections" White paper, 1, 2000, http://www.securepoll.com/

[9] European Commission " An innovative Cyber Voting System for Internet Terminals and Mobile Phones " IST-1999-20338 http://www.eucybervote.org/main.html

[10] Internet Policy Institute. Internet Voting. http://www.internetpolicy.org

[11] Irwin Mann, CFP '93.- Open Voting Systems, New York University, Mar, 1993

[12] K.J. KIM, " Design and Implementation of Internet Voting System to the Worldwide Level" 28.Aug. 2001

[13]Kwangjo Kim, Jinho Kim, Byoungcheon Lee, and Gookwhan Ahn "Experimental Design of Worldwide Internet Voting System using PKI" SSGRR2001, L'Aquila, Italy, Aug. 6-10, 2001 http://caislab.icu.ac.kr/pub/paper_international/body.html

[14] L.F.CRANOR, R.K.Cytron "Sensus : A Security-Conscious Electronic Polling System for the Internet" http://theory.lcs.mit.edu/~cis/voting

[15] .Mark A. Herschberg, Secure Electronic Voting Using the World Wide Web, Master's Thesis. MIT, Jun, 1997

[16] Michael Shamos. CFP '93- Electromic voting-evaluating the threat. http://www.cpsr.org/

[17]..National Commission on Federal Election Reform. http://www.reformelections.org

[18] National Computerization Agency " A study on the Functional Standard of Certificate Authority Software for Electronic Document in Government"

[19] National Security Research Instiute "Modern Cryptology" Kyungmoon, 2000

[20] Ronald L. Rivest, David Jefferson, Shuki Bruck, A Modular Voting Architecture ("Frogs") , August 18, 2001

[21]Ronald L. Rivest, Electronic Voting, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambrige, MA 02139

[22]Ronald L. Rivest,, Security in Voting Technology, MIT, May 24.2001

[23]Roy G. Saltman. Accuracy, integrity, and security in computerized vote-tallying. Technical report, Computer Science and Technology, National Bereau of Standards, Gaithersburg, MD20899, August 1988. NBS Special Publication 500-158. http://www.itl,nist,gov

[24] Roy G. Saltman CFP'93 - Assuring Accuracy, Integrity and Security in National Elections, The Role of the U.S. Congress, National Institute of Standards and Technology. Dec 2, 1993

[25] Senator Dary. L.Jones, Newsletter, Vol 1 . Issue2

[26] http://www.emarketer.com/estanews

[27] http://www.evotesystem.com, Weekly-Public Vol7, 9. Feb.2001

[28] http;//www.pibkorea.co.kr

[29] http://www.senate.gov/~gov_affairs/gov