IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 Volume 2, Issue 8 (August 2012), PP 06-11
www.iosrjen.org

A Novel secure protocol, IES, for Mobile Voting

Somayeh Izadi[1] Saeed Zahedi[2], Reza Ebrahimi Atani[3]
[1] *Department of Information Technology The University of Guilan, Rasht, Iran*
[2]*Department of Information Technology The University of Guilan, Rasht, Iran*
[3]*Department of Computer Engineering The University of Guilan, Rasht, Iran*

Abstract : - *Mobile voting is a kind of Electronic voting, or maybe is new generation that use of cell phone that is user interface for sending. As for construction of cell phone and its limitation, so we need to define a different and new security protocol that can observe max requirement of voting. We offer a new protocol with different structure from whatever said now. In this protocol, we use from blind signature in cell phone and Mix networks in Intelligence. Defining, implementation and employed trick make it possible the requirement such as Privacy, Receipt-freeness, Fairness, Verification, and Universal verification, Anonymity, Comfortable, Performance, Incoercibility, Accuracy and Robustness.*

Keywords: - *Electronic voting, Mobile voting, from blind signature, Mix networks, Privacy, Receipt-freeness*

I. INTRODUCTION

Electronic voting is one of democracy basis that should lead the citizenry to reliability, and calm. The necessity of making facility while regarding security in e-voting, had causes that governments move to e-voting from ballot paper and traditional voting. The important point is that most of the people with their notion can not rely on internet and computer. Although election in developed countries has failed, and has been suspicion, but according to three important points, time, cost, and comfort, so voting in situation that is in their authority, is most important for society. Therefore we define the cell phone for interface voting. Electronic voting is based primarily on three approaches:

- ✓ Mix Networks
- ✓ Blind Signature
- ✓ Homomorphic Encryption

II. RELATED WORKS

Introduced protocol is base on two approaches, blind signature and mix net. Actually we design a hybrid protocol. In [3] the FOO have been introduced base on blind signature and zero knowledge proofs. Radvin in [10] introduces another protocol in same method. In [5], [11], [14], [15], are another protocols that are base on blind signature. In [1], [2], [6], [9], we are introduced protocol who are base on anonymous Channel, homomorphic encryption and mix nets. One of recent work is [8] that present an e-voting system which is base on blind signature. Of course, there had been some attacks on blind signatures (e-payment or e-voting) and all of them have been successful.

III. ELECTRONIC VOTING SCHEME

Generally, e-voting scheme consists of three main stages: initialization stage, voting stage, and counting stage. The stage can consist of more phases.

A: Initialization stage At this stage, authorities set up the system. They announce the elections, formulate the question and possibilities for an answer, create a list of eligible voters, and so on. They generate their public and secret keys, and publish the public values.

B: Voting stage. Voters are casting their votes. The voter communicates with authorities through the channels he can use, forming a ballot containing his vote. Finally he sends his ballot to its destination.

C: Counting stage. Authorities use their public and secret information to open the ballots and count the votes. They publish the result of elections.

IV. SECURITY REQUIREMENTS FOR MOBILE VOTING PROTOCOL

In different protocols, according to kind of elections and applications, we need different stages and different requirements. In order to be usable in practice, electronic voting scheme has to satisfy some requirements.

1) ***Verifiability.*** A voter should be able to verify whether his vote was correctly recorded and accounted in the final vote tally. We distinguish between individual and universal verifiability. In the latter case not only the voter but anyone can verify that all valid votes were included and the tally process was accurate.
2) ***Dispute-freeness.*** A voting scheme must provide a mechanism to resolve all disputes at any stage.

3) ***Accuracy.*** A voting scheme must be error-free. Votes of invalid voters should not be counted in the final tally.
4) ***Fairness.*** No one should be able to compute a partial tally as the election progresses.
5) ***Robustness.*** A scheme has to be robust against active or passive attacks and faults as well.
6) ***Receipt-freeness.*** A voter should not be able to provide a receipt with which he may be able to prove his vote to any other entity.
7) ***Practicality***. A voting scheme should not have assumptions and requirements that may be difficult to implement for a real application.
8) ***Eligibility***. Only valid voters who meet certain pre-determined criteria are eligible to vote.
9) ***Privacy.*** In a secret ballot, a vote must not identify a voter and any traceability between the voter and his vote must be removed.
10) ***Individual verifiability.*** Each eligible voter can verify that his vote was really counted.
11) ***Universal verifiability.*** Any participant or passive observer can check that the election is fair: the published final tally is really the sum of the votes.
12) ***Incoercibility***. Say that the scheme is incoercible if the voter cannot convince any observer how he has voted. This requirement prevents vote-buying and coercion.
13) ***Democracy.*** No voter can vote more than once.
14) ***On-line property.*** A voter can join or leave the voting session at any time without losing the possibility to vote once.
15) ***Walk-away property.*** After a voter has cast his vote he can leave the voting session ("walk-away") with the assurance that his vote is counted.
16) ***Availability***. A voter eventually succeeds in casting a vote.
17) ***Anonymity.*** No one can't access to any vote.
18) ***Performance***. E-voting systems should can faced with any problem in high volume and can continue their activities and ultimately count the obtained valid votes, and then to inform the results with end of performance.
19) ***Comfortable.*** Any one even the handicapped and illiterate can vote.

V. BLIND SIGNATURE

A blind signature allows somebody for instance an authority to sign an encrypted message without decrypting it. Once the message signed and resent to the sender, he has a signed version of his vote by the authority and a guarantee that his vote has not been seen. We use in the rest of the document these notations. Formally, the blind signature scheme with message space M is a 5-tuple (η; χ; σ;δ; Γ) , where

a) η is a polynomial-time probabilistic algorithm, that constructs the signer's public key (pk) and its corresponding secret key (sk);
b) χ is a polynomial-time blinding algorithm, that on input a message $m \in M$, a public key pk and a random string r, constructs a blind message m';
c) σ is a polynomial-time signing algorithm, that on input a blind message m' and the secret key sk constructs a blind signature s' on m';
d) δ is a polynomial-time retrieving algorithm, that on input a blind signature s' and the random string r extracts a signature s on m;
e) Γ is a polynomial-time signature-verifying algorithm that on input a message signature pair $(m; s)$ and the public key pk outputs either yes or no.

Blind signature is often used to get a token from the authority: The voter gets a signature from the authority of his ballot and then he is able to cast his ballot. It is used to achieve eligibility.

VI. INTRODUCING OF PROTOCOL IES

Protocol will define in 6 stages that describe here:

1) Registration

In this stage qualified persons refer to certain places such as governor- general, and give their national card, receive two keys that one of them is public and another one is private from access authority.

Meanwhile, voter will take a list of candidates that in this list the person have been identified by face, and name and ID number which contain two digits. Another point is that some numbers will be given to voter by dispatches for sending message. These ID's are connected to servers of mix nets and the transmitted messages to those servers. With this method, votes and usual messages will separate together.

2) Initialization stage

In this stage an eligible voter will receive a file which is voting program. The voter must copy this soft ware on his cell phone. This program needs private key to install. Voting program will be applicable only once and it

will lose the ability to run after first time. On the other hand the private key is One-Time-Pad (OTP) and it will cancel after installing program. Thus the voter will access to voting environment only once. This subject will help us to obtain two requirements: democracy and fairness. Figure 1 show the registration and initialization stage.

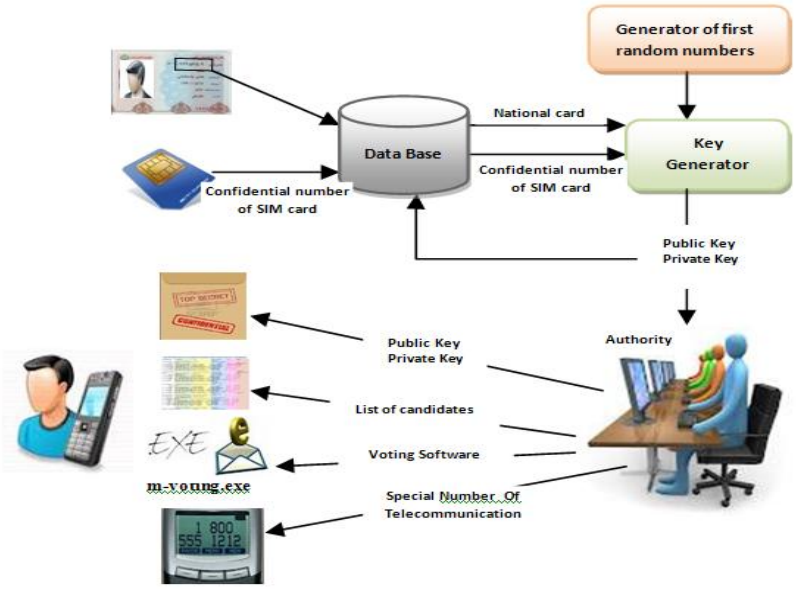

Figure1: Registration and Initialization Stage

3) Voting stage

The interface between user and authority will be "message". We need two managers. The first one will issue the certification of entering in voting. The second one is the person who is responsible of investigating of errors. It is possibility of installation of program by expert user .This managing will lead to meet the comfortably requirement.

The voter thinks that for sending his vote has inserted the number of his candidate, then enter public key, then push " send" key, but it's deception. The protocol has designed another way. Public key has been produced by random prime number, and number of unique national (from her/his national card). The public key has consisted of 3 parts, as it has been shown in figure 2. One part is popular key that is the main part, then separating, and the third part is seductive.

Figure 2: Public Key Structure in this model

The main part will separate (5 alphabet are as separator, that are not repetition in another part of public key) from seductive part.

At first, the voter types the number of his candidate, then will begin to type her/his public key. So, when he encounters one of the 5 alphabets, the software as soon as typing of that alphabet, (according software programming commands) will encrypt the content of what has been typed so far.

Therefore the contents of vote, the main public key and confidential number of SIM card (that already had been read by the software) will be encrypt together. In the interval that voter is engaging to entering seductive part, software has necessary time for encryption.

4) encryption

In blind signature, authentication of voter will be done by key pairs, who the authority give her/him.

Then the voting program will change the encrypted context with typed context in "outbox".

Whatever will remain in "send item" after final sending is obscurant context that can not show the content of issued vote. This changing is for meeting the receipt-freeness requirement.

When user push "send" key, the cipher text will sent. But in the period of individual verification, the same obscurant context will help to authority. Because of authority can decrypt the same obscurant context and prove the voter that her/his vote has been counted or no. Of course, through transmission of confidential number of SIM card, it's possible to universal verifiability. However, we can get help from "delivery" (which is second stages of blind signature for confirmation of blind signature) for survey of universal verifiability.

Point: We assume that the passage of cell phone to dispatches in this protocol is secure. Although if in period of sending the vote, attacker can access to the sending vote, protocol will be robust. Because he must spend much time or braking it.

Because any thing the attacker has obtained is the unclear and should spend a lot of time to break it. Attacker can not access to all keys of all voters, which has been created according to identity card (national card) and with time limitation of voting, it is impossible to exploitation of that.

5) Mix net

After sending vote to dispatches by voter with special number (voter received it at time registration), the message content will encrypt in mix nets again. This encryption obtain anonymity requirement. There is no difference between kinds of different mix nets. Because of the dispatches platform is powerful. It is better use of mix nets with variety length of passage which is more resistant. Figure 3 shows what happen in voting stage.

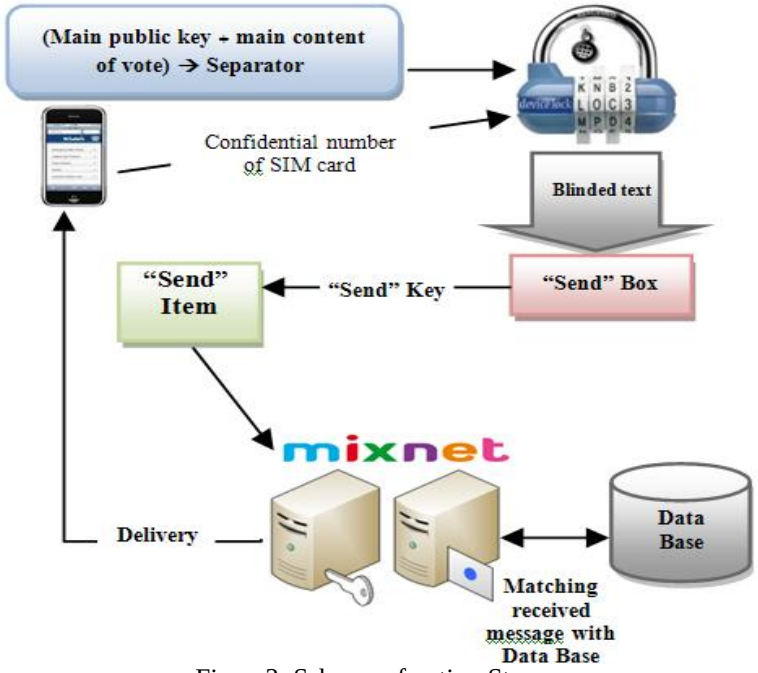

Figure3: Schema of voting Stage

6) Counting and publish result

Authorities use their public and secret information to open the ballots and count the votes. They publish the result of elections. Posted result of mix nets will decrypt by public key servers and private key servers and also match with database information, and then the counting will present the winning candidate. It must be noted that system and protocol must be so secure that candidates can relay on results and accept them .It is necessary to explain and define of design for candidates .

VII. ANALYZES OF PROTOCOL IES:

For analyzing of protocol, meeting all of the requirements and investigate them.

a) Privacy

One of the most important employments of blind signature in voting is consider privacy. In any subject that privacy is important, using of blind signature recommended. Since structure of blind signature will destroys connection between the signer and message.

b) Receipt-freeness

Changed context and encrypted vote with public key which remain in "send" box, causes that voter can not shows the content of her/his vote.

c) Democracy and eligibility

At first, by investigating of national card and identity documents of applicant by authority, only eligible person can take the public key and private key. Also since, the software is installed only once and will uninstall after once sending message, so any one can't send more than one vote. Therefore we have eligibility and democracy in this protocol. Voter only can use one time SIM card and send vote. If she/he want to use another

time, second vote do not counted. In the first vote, the information of SIM card will be sent with vote to intelligence network and will be adjusted with bank data bases, so if there is repeated, new vote will be omitted.

d) Individual verification

Everyone after sending vote, with two ways can find that is her/his vote be counted or not. First by receiving the report of deliver from authority, and the second can refer to authority and show content of "send box", since the authority has accessible to public key, private key and confidential number of SIM card, can easily persuade the voter's request.

e) Universal verification

The organization of voting can announce the amount of participation of people with match the SIM card's number and received messages. and also say to people and universal organization the situation of counting and receiving correct or wrong votes. This will be done by helping of mix nets.

f) Anonymity and Robustness

Using of mix nets that main properties with quality is anonymity and robustness, is an important role in voting structure.

g) Accuracy and Performance

By investigating of receiving messages and the messages that are as delivery report has been sent form intelligence, can calculate the accuracy, and performance of voting system. .On the other hands, holding elections using the minimum time and cost, can help the voting system and government to meet performance.

h) Comfortable and Mobility

Cell phone is a set in addition to accessing of most of people, make it easy sending vote from any place, it is easy for voters to use of it. Voters don't need to stand in long lines to vote and are capable of issuing any point. It's so comfortable for voters and obtained mobility requirements.

i) Incoercibility

No party can enforce the voter and wants compulsory to vote the candidate that is opposite of her/his opinion. No voter can sell his vote. It is because content of "send" box can not show the content of virtual vote.

j) Fairness

After declaration of authority on close the election, system start to decrypt the votes and count them. Before this time, all votes are in mix nets servers.

k) Dispute-freeness

As soon as the voter sends her/his vote, can't denial the vote, because public key was available exclusively and also confidential number of SIM card shows that she/he sends the message. It's far-fetched that in one time public key, private key and SIM card have been stolen.

l) Practicality

Certainly assembling some mix nets servers and design the software it does not seem a hard work and unlike the cast of traditional and electronic election, is so cheap and affordable. It can cause to increase the reception from election.

m) On-line property

A voter has allowed to install software voting program once and send her/his vote. If the voter enter to the program and type the vote, but don't press "send" key and exit from the software, the content of vote will remain in "out" box. So voter does not lose her/his franchise.

n) Walk-away property

When voter issues his vote, by receiving the delivery can be sure that his votes has sent to center of counting. According to assumption which the passage between Telecommunications mast and cell phone is security, so the message in "send" box shows that the vote had been counted.

VIII. CONCLUSION

Protocol and designed scheme which introduced in this text can be used in type's elections such as single choice (presidential elections) or multiple choice (parliamentary or council elections). It causes decreasing of expenses and welcome increase.

Defining new application needs progress in construction of cell phone. Whatever we have said needs cell phone that needs Operating system and it's processor can processes minimum processes of encryptions. Another form of this protocol can be used by biometric finger print which is needed more study. The input o fingerprint can be sorted pair as public key. While registration stages the identity must be clear and complete information data base. Applying the biometric can be used in future.

REFERENCES

[1] Byoungcheon Lee, Colin Boyd, Ed Dawson, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo. "*Providing receiptfreeness in mixnet-based voting protocols*". In Jong In Lim and Dong Hoon Lee, editors, ICISC, volume 2971 of Lecture Notes in Computer Science, pages 245–258. 2003.

[2] David Chaum, Peter Y.A. Ryan, and Steve A. Schneider. "*A practical, voter-verifiable election scheme*". Volume 3679 of Lecture Notes in Computer Science, pages 118–139, 2005.

[3] David. Chum, "*blind signatures for untraceable payments*", *CRYPTO*, 199 -203, 1982.

[4] Frank Koenders, "*Ad hoc voting*", Master's thesis, Department of Mathematics and Computer Science, Eindhoven, 2009.

[5] Krishna Sampigethaya, "*A Survey on Mix Networks and Their Secure Applications",* IEEE, Vol. 94,No. 12, 2006.

[6] Kwangjo Kim , Jinho Kim , Byoungcheon Lee , Gookwhan Ahn. "*Experimental design of worldwide internet voting system using PKI*". 2001.

[7] Laure Fouard, Mathilde Duclos, and Pascal Lafourcade, "*Survey on Electronic Voting Schemes*", supported by the ANR project AVOTÉ, 2007.

[8] Marius Ion, Ionuţ Posea, " *An Electronic Voting System Based On Blind Signature Protocol*", CSMR, VOL. 1, NO. 1,2011.

[9] Matthew Wrighty, Micah Adlery, Brian N. Leviney, Clay Shields, "*An Analysis of the Degradation of Anonymous Protocols*", supported by grant DT-CX-K001 from the U.S. Department of Justice, O_ce of Justice Programs, 2000.

[10] Michael J. Radwin, "*An Untraceable, Universally Verifiable Voting Scheme",* December 1995.

[11] Miyako Ohkubo, Fumiaki Miura, Masayuki Abe, Atsushi Fujioka, and Tatsuaki Okamoto. "*An improvement on a practical secret voting scheme*". In Masahiro Mambo and Yuliang Zheng, editors, ISW, volume 1729 of Lecture Notes in Computer Science, pages 225–234, 1999.

[12] Rong-Jaye Chen, "*Blind Signatures and Their ApplicationsI*", *CRYPTO*, 2010.

[13] Stefan Weber. "*A coercion-resistant cryptographic voting protocol - evaluation and prototype implementation*". Master's thesis, Darmstadt University of Technology, 2006.

[14] Wen-Sheng Juang and Chin-Laung Lei. "*A secure and practical electronic voting scheme for real world environment*", TIEICE: IEICE Transactions on Communications Electronics Information and Systems, 1997.

[15] Wen-Sheng Juang, Chin-Laung Lei, and Pei-Ling Yu. "*A verifiable multi-authorities secret elections allowing abstaining from voting*". International Computer Symposium, 1998.