New Blind Digital Signature Based On Modified Elgamal Signature in Electronic Voting

Amir Aliabadian, Ali Delavari Ghara

Abstract- The electronic election is an electoral system that allows voters to submit their vote with the highest safety and protection coefficient. Such electronic form of election can reduce holding costs and increase the public participation as well. The wide variety of Protocols in the fields of Electronic voting has been introduced, that each of these projects paid attention to how to have the safe and secure elections. Of course each of these projects had problems. With regard to the security and wide range of usage and high efficiency, the requirement for a blind digital signature mechanism seems to be necessary for the future information society. Then there should be embedded a way to eliminate the negative factors of progress. Chvam presented many projects in the field of blind signatures that each of them were provided in order to increase the security. Nowadays the use of the public key encryption systems is highly regarded. This paper presented a new generalized blind signature scheme based on modified Elgamal signature. The new design has an important property that ensures if a message is signed multiple times, the corresponding signatures are different (this property is one of the properties of Elgamal signature). This property in addition to the property of not to be identified of the blind signature is seen in our plan. In this new signature for reaching to our goal we used of number theory and Mathematical integrity techniques. With the blind signature scheme proposed in this paper, one with the use of quality of common Elgamal signature can produces the blind signature. New design in comparison with RSA blind signature scheme has less computational complexity **and is faster as well. Our plan which is presented in comparing to the previous blind signatures which** *were based on the modified Elgamal signature has less computational complexity.*

Key words- blind signature, Elgamal signature, Number theory, RSA blind signature

I. INTRODUCTION

The electronic election is an electoral system that allows voters to submit their vote electronically with the highest safety and protection coefficient. Supporters of the electronic election point out that such an electronic election can reduce the holding costs and at the same time increase public participation. Of course, this system has some critics that they believe without the use of paper, counting of the obtained votes will be a difficult process and moreover manipulation and fraud in counting of the obtained votes can distort the actual results. In the new process of electronic elections, the usage of the telephone and personal computer networks and the Internet are introduced as useful tools in the field of e-election. The Electronic voting can expedite the counting process, and furthermore it can increase the participation of disabled people and people with disability in motion. With Regard to the safety and high efficiency and wide range of usage, the requirement of a digital blind signature mechanism in the future information society seems to be necessary. Then there should be embedded a way to eliminate the negative factors of progress. The blind signature is one of the digital signature schemes that should provide some important characteristics such as the avoidance ability of fabricate and the avoidance of communicating, which means only the signatory must be able to produce a valid signature. Avoidance of communication is a multifold security property that the blind Signature must meet and that means any one except the signature applicant (person who requested the signature) fails to establish a credible link between the signature protocol and the verified signature. A blind signature scheme is used in electronic voting (5), a digital payment systems without identity (6,7), database security (2) and many other applications. Due to the high safety and efficiency and wide usage, the requirement for a blind digital signature mechanism seems to be necessary for the future information society. The First blind signature scheme was introduced in 1982 by David Chvam (1). This plan was based on the RSA digital signature. We at the rest of the paper, in the second part, briefly will refer to the RSA digital signature scheme and Chvam blind signature and in the third section the Elgamal signature is presented. In the fourth section we indicate to the modified Elgamal signature and a new blind signature scheme based on it. In the fifth section of a brief articles about the comparing of computational complexity compared of the new blind signature with the RSA blind signatures and as well as the previous similar blind signatures (which are modified based on based on Elgamal signature) is presented. In the sixth section we offered some recommendations on presenting more research in the future.

II. THE SECURE AND PROTECTED ELECTRONIC ELECTION PROTOCOLS:

Secure elections must meet at least the following characteristics:

Protocol (1)

1. Only registered voters can vote.
2. No one can vote more than once
3. No one can determine the vote of another person
4. all can be assured of counting their votes
5. No one can take out a copy from the vote if another one
6. No one can secretly change the vote of another person.

Manuscript published on 30 August 2012.
***** Correspondence Author (s)

Amir Aliabadian, Faculty member of Electronic and Computer Engineering Department of Shomal University, Amol, Iran.
Ali Delavari Ghara, Department of Electronic and Computer Engineering Department of Shomal University, Amol, Iran..

7. All of the followed rules and regulations by an organization track the central CTF of voting.

Two following sections describe the feature six more.

1. All voters encrypt their vote with public key of the CTF and post out to CTF via email.
2. CTF organization, at first decodes votes and classifies them and finally publishes the results.

In this protocol, there are many problems, such as: the CTF can not tell if the vote has been sent from the registered voters or whether the registered voters gave more than one vote or not.

Protocol (2)

1. Each voter will sign his/her vote with the private key.
2. Then each voter will encrypt their signed vote by public key of the CTF and post for it via email.
3. The CTF will reopen all of the votes, examine and classification the signatures, and then results will be published by this organization.

This protocol will guarantee specification one ,two and six that only registered voters can vote and no one can vote multiple times. Also no one can change any votes of others.

The problem is that the CTF organization knows voters voted to whom, and voters should trust entirely to the CTF. Next protocol will solve this problem.

Protocol (3)

1. Each voter prepares set of ten messages. Each set includes a right vote for any possible outcome, and each message also includes a random twenty- digital number.
2. Every voter specifically and individually blind signature of his/her votes and email it to the CTF.
3. CTF organization to ensure that voters did not render their blind signature vote previously in the election, will review the list of registered voters. The CTF randomly select nine to ten votes and wants from the voter to reveal those votes, after reopening by the voter, the CTF checks that whether these nine set are similar or not? In the case of similarity, the Central Election CTF, specifically sign the tenth vote without reopening and return it via email to the voters and stores his/her name in the list.
4. The Voters reopen the copy of tenth signed set by the CTF and this collection will remain by the possible signed vote key by the CTF. The CTF can determine which vote is belonged to which voter.
5. The voter will choose any possible vote and encrypted it with the second public key of CTF and e-mail it to the CTF organization.
6. The CTF reopened and examine the signatures, search its list of the similarity in twenty-digital number and stores twenty-digital number in the database. The CTF will publish the results of the election with the votes and its twenty digital-digit number. The Blind digital signatures ensure that votes are unique. No one can make a fake vote or change the vote of others because the private keys of the CTF are hidden, and moreover the determination of voting to whom is impossible. In the presence of various CTF organizations, the CTF organization cannot determine that to whom people voted. Each voter can verify that her/his vote is properly tabulated or not.

However, if CTF organization be able to determine where the votes are come from, it can associate them with the voters and this matter is considered as a weakness. If the CTF was not able to do this, still it can generate and offer a lot of valid votes.

If Alice realizes that the CTF organization has changed her vote, she can not prove this violation, and the next protocol in addition of the above six features also has two following properties:

7. A voter can change his/her mind within a given time, which is including of wiping out the old vote and giving the new vote.
8. If the voter realizes that his/her vote was not counted, he/she can solve the problem without hurting to the hidden property of votes.

Protocol (4)

1. the CTF organization will publish a list of all qualified voters
2. Before the deadline, each voter will tell to the CTF organization that whether she/he has the intention to vote or not
3. After the deadline, the CTF will release the list of all qualified voters who votes.
4. Each voter will get a twenty-digit numbers randomly or by using of digital blind signatures
5. Each voter will produce the RSA keys, (d,e,n) with the cipher encryption function E and decipher D function. If his/her vote if V, two I,E(I:V) message without identity will be posted to CTF organization.
6. CTF will verify the receiving of the vote by the release of E (I,V) message.
7. Every voter will email to CTF the I,d message
8. CTF will decipher the votes; CTF can do it as soon as receiving d for each vote. Then CTF can calculate D(E(I:V)→I,V. When the election ended, CTF will publish the results, and for each different vote, the List of all the different E(I:V) that were included in that vote will be published too.
9. If one voter see that his/her vote has not been counted, with sending an E-Mail of E(I:V) and (I,d) to CTF, will object to the negligence.
10. If a voter wants to change his/her vote from V to V', he/she must email the E(I:V') and (I,d) to the CTF.

Stages one to three related to protocol (4) are the preliminary rules for a real voting. These rules will reduce the producing and adding of the fake votes by CTF.

If two voters select the similar ***I*** in the fourth stage, then the CTF will recognize it in stage 5. The CTF will produce a new twenty- digital number and choose one vote, and publish the ***I′ ,E (I:V).***

A person who gets that vote will recognize it and with repeat fifth stage, vote with the new ***I′***.

In the sixth stage, each voter can check that her/his vote is counted accurately or not. If it was not counted, he/she could object to this matter in the ninth stage and prove his/her claim. One limiting problem is that the CTF organization can form fake votes for those who have responded in the second stage, but did not vote. A more serious problem is that if the CTF neglect in counting votes, Alice can accuse them that the CTF has neglected the counting of votes deliberately, whereas the CTF organization can claim that she has never even voted!

III. RSA DIGITAL SIGNATURE

Consider a standard RSA system in which the ***(e, n)*** is the public key and ***d*** as a private key and mode be considered as ***n***, and from multiplying of two large prime numbers, ***p, q*** are formed, then we have:

$$ed \equiv 1 mod \varphi(n), \varphi(n) = (p-1)(q-1)$$

Suppose we want to sign the message ***m*** with an RSA digital signature, and ***m*** is an integer between zero and ***n*** (since$m \in Z_n$) the signing has one stage, and is as follows:

- *to sign*

The Signatory to form a sign uses from the private key **d** as following:

$S = m^d \ mod \ n$

- *to Verify*

At this stage, everyone with possessing the public key, can verify the corresponding message **m** to the sign, every time received the pair **(m, s)** and as following he/she will recognize the validity of signature:

$$S^e = m \ mod \ n$$

Because:

$$S^e = (m^d)^e = m^{ed} = m \ \ mod \ n$$

The RSA digital signature scheme in more detail is defined in reference (8).

IV. THE BLIND SIGNATURE BASED ON RSA (CHVAM BLIND SIGNATURE PROTOCOL)

In this signature two important roles are collaborating, one of them is a signature applicant and the other one is signatory, The blind signature stages are is as follows:

- *To Blind The Message*

Applicant first multiple his/her message in a blindness factor and in this way she/he blind his/her message:

$$r \in Z_n^*$$

$$\overline{m} \equiv m.r^e \ mod \ n$$

Then he delivers the blinded message ***m*** to the signatory.

- *to sign*

The signatory Like what was shown at the RSA digital signature will sign by using of I his/her private key as below:

$$\overline{S} \equiv \overline{m}^d \ mod \ n$$

Then send S which is the blinded message to the applicant

- *reopening of the blindness*

The Signature applicant after receiving **s** will acquire a valid signature from it as follows:

$$S \equiv \overline{S} \times \frac{1}{r} mod \ n \equiv (mr^e)^d \times \frac{1}{r} mod \ n \equiv m^d \ mod \ n$$

Then he/she deliver the pair (m, s) to verifier.

- *to Verify*

The verifier acts prior to the previous method, means that he/she examine that the following equality is true or not :

$$S^e \equiv m \ mod \ n$$

More details about this signature is defined in reference(1).

V. ELGAMAL DIGITAL SIGNATURE

Elgamal signature was first presented in 1985 and this signing plan like the encryption systems, is considered as a non-deterministic. It means that unique message can have multiple signatures, and its algorithm is as follows:

At first the prime number *p* is chosen so that its discrete algorithm can not be easily calculated. Then the member of $\alpha \in Z_p^*$ is chosen so that it be the prime root then we have $\beta \equiv \alpha^a \ mod \ p$, where (α, β, p) keys are public and a is as private key.

- *to sign*

To sign a message *x*, first the $k \in Z_{p-1}^*$ is randomly selected and the signing action of message *x* is done randomly by *k* parameters, in this way $Sig(x, k) = (\gamma, \delta)$ that here the δ, γ includes:

$$\delta \equiv (x - a\gamma)k^{-1} \ mod \ p-1$$

$$\gamma \equiv \alpha^k \ mod \ p$$

Then the (a, k) are private keys of signature and the pair (γ, δ) are also signature of the message *x*.

- *the verify algorithm*

To verify the signature, the verifier acts as the following: if the equality of $\beta^\gamma \alpha^\delta \equiv \alpha^x \ mod \ p$ is true, then the verifier the verified the validity of the signatures for message *x*, and otherwise the signature is not valid. For more information See reference (3).

VI. CHANGING IN A ELGAMAL DIGITAL SIGNATURE

We will change the Elgamal signature as follows:

- *to sign*

To sign a message *x*, first $k \in Z_{p-1}^*$ is randomly selected and $Sig_k(x, k) = (\gamma, \delta)$ where δ, γ is defined as follows:

$$\delta \equiv \big(x - (a+k)\big)\gamma \ mod \ p1$$
$$\gamma \equiv \alpha^k \ mod \ p$$

Then (a, k) are private keys of signatory and the pair (δ, γ) are the signature of message x.

- *verify algorithms*

If following equality is true, the verifier will validate the authentication of the signature for the desired message:

$$\alpha^{\gamma x} \equiv \alpha^\delta (\beta\gamma)^\gamma \ mod \ p$$

Because:

$$\alpha^{\gamma x} \equiv \alpha^\delta (\alpha^a \alpha^k)^\gamma \equiv \alpha^{\delta + \gamma(a+k)} \ mod \ p$$

$$\Rightarrow \gamma x = \delta + \gamma(a+k) \ mod \ p-1$$

At the result:

$$\delta \equiv \big(x - (a+k)\big)\gamma \ mod \ p-1$$

VII. NEW BLIND SIGNATURE SCHEME

- *to blind the message*

Suppose if the signature applicant of message *x* blind the message with the random selection of $h \in z_p$:

$$\overline{x} \equiv x + h \bmod p - 1$$

And send the $\overline{x}$ for the signatory.

- *to sign*

the signatory After receiving the $\overline{x}$,signs it as before, namely he/she selects a random *k* which calculated the $k \in Z_{p-1}{}^{*}$.

$$\overline{\delta} \equiv \left(\overline{x} - (a + k)\right)\gamma \bmod p - 1$$
$$\gamma \equiv \alpha^{k} \bmod p$$

Then the signatory delivers the pair $(\overline{\delta}, \gamma)$ as a blind signature of message $\overline{x}$ to the signature applicant.

- *to open the blindness of the message*

In this stage, the signature applicant, derives the validate signature as follows for the message X of the blind signature that he/she has received from the signatory.

$$\delta \equiv \overline{\delta}\left(\overline{x} - (a + k)\right)\gamma \bmod p - 1$$
$$\gamma \equiv \alpha^{k} \bmod p$$

Demonstrates:

$$\delta \equiv \overline{\delta} - \gamma h \equiv \gamma\left(\overline{x} - (a + k)\right) - \gamma h$$
$$\equiv \gamma(x + h) - \gamma(a + k) - \gamma h \equiv \gamma\left(x - (a + k)\right) \bmod p - 1$$

- *verify algorithms*

verify algorithms as before is like the review of the following equality:

$$\alpha^{\gamma x} \equiv \alpha^{\delta}(\beta\gamma)^{\gamma} \bmod p$$

VIII. A BRIEF ANALYSIS OF THE COMPUTATIONAL COMPLEXITY

The new blind RSA signature scheme process in comparison with RSA blind signature scheme has less computational complexity and is faster than it because in the new design one act is required for blinding message but in a blind RSA signature scheme the act first must be squared and then multiplication act should be done. The same situation is also for reopening the signature blindness. If one considers the blind signatures be based on the modified DSS in reference (4). The blind Algorithm and reopening of blindness in this project will involve in the multiplication action and the exp function and the inverse operator, which this process in comparison to the adding and multiple process which is used in our plan, is more complex and thus our signature scheme is far faster.

IX. MORE RESEARCH IN FUTURE

Due to the safety and high efficiency, the need for a suitable blind signature mechanism seems to be something important in the information society thus a definite need is for providing a way to eliminate negative factors of progress. Still there are too many topics in the field of blind signature that can be considered as background for further works including in this scope, which are including the presenting of new designs based on other systems or integrated systems or new projects with better operations, better security, or a mixture of these two scopes.

REFERENCES

[1] D.Chaum,A FGiat and M.naor, “ untraceable electronic cash “ advanced in cryptology,ceypt0 88,s. Goldwasser (E.d),spring-velage 1982.

[2] D.Chaum,and T.p. Pederson, “ wallet database with observers”, advanced in cryptology-CRYP to 92,(1993) pp 89-105

[3] T.Elgemal “a public-key cryptosystem and signature scheme based on discrete logarithm” IEEE transactions on information theory ,vol IT-31 ,No.4, pp.469-472,1985

[4] J.L. Camenisch,J.M. Piveteao,M.A stadler, “Blind signatures based in the discrete logarithm problem” advanced in Cryptology eurocrypt,94,Perugia,Italy,pp 428-432,1994

[5] A.Fujioka,T.Okamoto,and K,Ohta, “A practical secrete voting scheme for large scale election”, advanced in cryptology AUSCRYPT Y2,(1992) pp 244-251

[6] I,Fan, and C.L.Lei “ low-computation practically blind signature for electronic cash” ,IEICE Transactions on Fundamentals,Vol,E81-A

[7] T.Oktamoto and K.Otha “universal electronic cash”, advanced in Cryptology-CRYPT0’YI,(1992) pp 324-337

[8] William Stalling,” cryptography and network security: principles and peactice”,second edition, prentice Hall,1999

Amir Aliabadian was born in Babol, Iran, in 1982.He received his B.Sc.degree in Electrical Engineering from the Mazandaran University and his M.Sc.degree in telecommunication system in Emam Hossein University, Iran, in 2004 and 2007, respectively. Now, He is Faculty member of Electronic and Computer Engineering Department of Shomal University, Amol, Iran. Research interesting: Encryption, Communication, Image Processing.

Ali Delavari Ghara was born in Babol, Iran, in 1989.He received his B.Sc.degree in Electrical Engineering from the Shomal University, Iran, in 2008 and 2012.Research interesting: Electrical Power, Communication, Image Processing.