Ensuring the Blind Signature for the Electoral System in a Distributed Environment

Segundo Moisés Toapanta Toapanta¹, a, Darío Fernando Huilcapi Subia¹, b, Milton Andrés Cepeda Aveiga¹, c, Luis Enrique Mafla Gallegos², d

¹Computer Science Department, Universidad Politécnica Salesiana Ecuador, Robles 107 Chambers, Guayaquil, Guayas, 042590630, Ecuador
²Faculty of Systems Engineering, Escuela Politécnica Nacional, Ladrón de Guevara E11-253, Quito, Pichincha, 022976300, Ecuador
a stoapanta@ups.edu.ec, b dhuilcapi@ups.edu.ec, c mepedaa@est.ups.edu.ec, d enrique.mafla@epn.edu.ec

Keywords: blind signature, security, distributed, electronic voting, privacy, confidentiality, integrity

Abstract: This paper analysed several alternatives of blind digital signatures, an electronic electoral system in a distributed architecture environment, in view of the persistence of blind signature problems in electoral processes. The objective is to recognize and propose an alternative of a blind signature scheme to improve privacy, confidentiality for the voter, and to reduce any type of vulnerability with respect to the information of the same. The deductive method was used to summarize the information of the scientific articles studied. It resulted in a blind signature prototype based on algorithms to mitigate the vulnerabilities of voter information. It was concluded that, in order to guarantee privacy and confidentiality, several blind signature schemes must be implemented together to obtain the benefits of each of them and thus reduce the risks to which the voter's information is exposed in this process.

1. Introduction

At present, the subject of electronic voting is discussed a lot, both in its positive and negative aspects. Some prefer not to implement this system and keep with the traditional electoral voting system, based on electoral schools, ballots, long queues and many expenses of resources and money.

Nowadays, there are several countries that have implemented electronic voting with legal validity at national level, such as Belgium, Estonia, Brazil, the Philippines, Venezuela and India; in the case of the United States and other countries, they have done it only at a partial level, not in all its states. Some others have considered the possibility of implementing the system and are in the process of studying it in the end to decide if they are given to change, among which is Ecuador. However, countries such as Germany, Finland, Holland, Ireland and the United Kingdom having studied and
implemented them, they decided to legally prohibit it for reasons of lack of security, privacy, transparency, among others.

It must be borne in mind that a system, however profitable or secure, will not always be unbreakable in one hundred percent. The electronic vote must have at least the same security and privacy that the traditional voting presents, therefore, it must be a fairly robust system in order to maintain these requirements or in the best of cases have a notable improvement with respect to the traditional one. If reliability is obtained in electronic voting, it will be easily implemented anywhere without fear of cyber fraud or the theft of voter information.

But, is it really necessary to implement this type of system? Thanks to new technologies and daily technological advances that help society, it can be deduced that the change is necessary for reasons of updating and even improvements. Since, economically speaking, countries would not spend millions of dollars on materials such as paper, pens, tapes, markers and many more, neither in payments to the personnel that is in the different electoral schools and another type of expenses that are made in the process of the electoral suffrage.

It should be noted that the investment needed to implement electronic voting is not cheap either. It is estimated that the approximate cost per person is 7 dollars in a traditional electoral vote and approximately 14 dollars per person in the case of electronic voting, thus, the cost doubles. However, in the long term, we will benefit from the investment of machines and different equipment or systems, since this will last for years, something that in the traditional vote is spent every time a new election is made.

This paper discusses different models created or proposed for blind digital signature protocols and describes their processes, in order to ensure privacy and confidentiality in electronic voting. A big deficiency that exists is the little knowledge of cryptographic algorithms, or in its case inefficient algorithms.

The objective is to determine which algorithm should be used for the optimization of an electronic signature scheme in a voting system in a distributed architecture.

Why should an electronic signature scheme be optimized in a voting system in a distributed architecture? It is to improve the integrity of the electronic signature scheme information in a voting system.

The deductive method and the exploratory investigation are used in order to analyze the information of the articles found in the reference.

Our research results in a scheme that ensures the blind signature process, so that the voter's information remains integrated and private with others.

It is concluded that, to implement a voting system with blind digital signature in distributed architecture, it is necessary to encrypt the information in order to certify the integrity of it and guarantee the electoral processes. It is stated that a single blind signature scheme will not be useful for all the applications in which it works, because each scheme has advantages and disadvantages.

2. Materials and Methods

The main function of the digital blind signature protocol, confidentiality and privacy to the voter, is to make sure that the content of the message cannot be seen by entity, since there is no protocol like the one of the blind signature, can be obtained, information that can be delicate as in the case of electronic votes, in which the voter must know for whom his vote was, thus removing the right to privacy.

The deductive method and the exploratory investigation were used to analyze the information of the articles of the reference.

Within this study of several methods and models of blind digital signature, the most efficient and effective methods were obtained to be able to be implemented within the electronic vote in Ecuador.

2.1. Methods and Schemes of Blind Signature.

The following schemes are presented.

1) Based on Elliptic Curve Cryptography: It has small parameters, reduced public key certificates, use of less bandwidth and reduced hardware processor requirements, as described previously [14].

2) Based on RSA (Trackable) by Chaum: This was the first blind signature method created, consisting of five stages, which are: initialization, blinding, signature, reversal of blinding and verification.

3) Based on RSA (Not trackable) by Hwang: It is the improved version of the Chaum scheme, since it does meet the requirement of being non-traceable, to give more privacy and security to the protocol.

4) Based on ElGamal (Not Tracked) by Lee Et Al: Like the one based on RSA, it consists of the same five phases, which are: initialization, blinding, signature, reversal of blinding and verification, but with different subprocesses.

5) Based on Identity by Hess: This allows to avoid the trust problems that exist in public key infrastructures which are based on certificates (PKI), as described in Reference [8].

6) New blind signature based on Identity: PKG is responsible for generating private for users and knowing master keys. Some cryptographic operations can be carried out, two of which are deciphering or signing, mentioned in detail in Reference [10].

7) Based on ECDLP discrete logarithm of elliptic curve: This scheme consists of four phases, such as key generation, blinding, signature, unmasking and verification [13].

8) Anonymity: The voting location is where the electronic voting devices are installed, and it is divided into the registration step and the voting step. The eligible voter registers with the administration administrator and then takes a vote at the polling place. This method suggests that the system receives a paper receipt from the voting device [2].

9) Proxy-based: It has the delegable property of the proxy signature and the non-binding signature of the blind signature. In a blind proxy signature, the original signer delegates to a responsible signer their right of signature. The responsible party generates a blind signature for a message sent by the voting user, as described above [12].

10) Blind signature Undeniable: It consists of four stages which are preparation, registration, voting and counting. In the first stage, the voting authorization center composes unique integer pseudonyms for each applicant. The authorization center and voting users generate their own private and public keys. At the registration stage, voters generate their own pseudonym and make their ballot. In the next stage, an undeniable protocol of response to the challenge is used between the voting authorization center and the voters to ensure equal voting. And in the last stage the voting authorization center counts the ballots for each applicant. If you reject a voter's ballot, the voter must
initiate the protocol of disavowal anonymously to recognize whether the ballot is authorized or not [5].

11) Blind signature of efficient user: There are two participants, a signatory and a group of users, in which user requests signatures to the signatory, and the signatory issues blind signatures to the users. This blind signature scheme consists of four phases: application initialization, signature and extraction [3].

12) Based on certificates: A blind signature model based on a certificate, which involves three entities, the certifier, the signatory and the voting user, mentioned in Reference [11].

2.2. Structure and Requirements of a Blind Signature.

The requirements that an ideal blind signature must have are these presented.

1) Correction: Someone who owns the public key of the signer can correct the signature of a message already signed.

2) Blinding: The content of the vote should not be seen by the signer.

3) Impossibility of forcing: The signature is the sole proof of the signatory, and there is no other entity that can carry out forged signatures.

4) Non-tracing: The signatory cannot associate the signature pair of the vote, even if the signature is revealed to the public.

There are many blind signature schemes that meet the first three requirements, however, to be considered effective, must meet the requirement of non-traceability to keep secret the vote of the voter, as well as the anonymity of it.

The basic structure of a blind signature consists of three algorithms and two entities which are the signatory and the voting user in case of electronic votes. The structure is detailed.

1) Configuration: Algorithm that takes a security parameter and formulates a pair of public keys "y" and private keys "x" for the blind signature model.

2) Generation of blind signatures: Protocol that is applied by the voter and the signer. The voter first blinds the V vote and gets a new V* version of V and then sends it to the signer, who uses his private key to sign V* and gets S* and sends it to the recipient, who then disables it to get S, which is a blind signature in V.

3) Verification: Algorithm that given a vote V and its presumed blind signature, any person who knows the public key of the signer can verify the validity of S. If this is legitimate, the algorithm throws "1", otherwise the result is "0 ".

2.3. Algorithm of the Electronic Voting Process with Blind Signature.

First it is necessary to know the acronyms of the algorithm, to have a better perception and understanding of it, which are specified.

V = Voter
AC = Authentication Center
LC = Collection Center
CC = Counting Center
VS = Voter Signature
SAC = Signature of the authentication center
BM = Blinding Method
VM = Voter Message  
RM = Random Message  
MAC = Message from the authentication center  
RT = Recovery Technique.

**First Stage:**
1) AC is responsible for sending the information to the voter.  
2) The voter V selects the option.  
3) V sends the message VM in which the blind signature technique is used BM.  
4) The voter V signs the message to send it to the AC.  
5) AC receives the message and for this he verifies the following points: - V should be eligible  
- V should not have done the process before - The signature VS of the message VM is valid  
6) AC signs the message with the signature SAC.  
7) AC generates a random message RM for the voter V  
8) AC sends the RM and the MAC to the voter V.

**Second Stage:**
1) AC sends the list of random messages RM to the LC and the CC.  
2) The voter V signs with the technique RT.  
3) The voter V verify that the signature SAC is necessarily from AC, if the result is negative, the voter V indicates that the signature is not valid.  
4) The voter V encrypts the VM with the public key of the CC and sends it along with a random message RM to the CC.

**Third Stage:**
1) V looks for his random message in the ads, if this fails, it notifies that his vote is not counted.  
2) V checks if the message that is in the ad is its, if it fails, it can claim that the vote is not on the list.  
3) LC is responsible for sending all the encrypted votes to the CC  
4) CC decrypts all the votes with his private key, publishes all the random messages and decrypts the votes in the announcements, and waits for the response of the voter.  
5) V checks if your vote was correctly decrypted, if it fails it tries again.  
6) When all the voters notify that their votes have been correctly decrypted, CC calculates the result and finally publishes it.

Table 1. Comparison of two voting systems.

<table>
<thead>
<tr>
<th></th>
<th>Remote Access</th>
<th>Anonimity</th>
<th>Votes Verification</th>
<th>Results Manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Vote</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>E-voting with Blind Signature</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 1 shows the comparative example of two voting systems; where it can be evidenced that in traditional voting systems through ballots there can be greater manipulation by the people involved and in electronic voting systems there is greater control.

This is a general scheme of blind digital signature presented to give privacy and reliability to the electronic voting system.

Figure 1 describes the general scheme of the digital blind signature; where it can be evidenced the entry of the original information that is processed by an encryption of the Hash algorithm with its respective digital certificate and their respective processes to guarantee the blind digital signature.
3. Results

This research resulted in the scheme that ensures the blind signature, obtaining privacy and reliability on the voter data.

It resulted that the RSA algorithm must be used for the optimization of an electronic signature scheme in view that after the analysis. It is determined that it is the fastest and most efficient compared to the others, when adding the encryption with a certified private key, we generate the security of the digital signature at the time of taking the features protects the integrity of the data. The algorithms seen are responsible for the privacy of the voter data as well as the content of the stored votes, the comparison between the different algorithms helps us to understand how each of them works and the weaknesses and strengths they have. The presented scheme accommodates tests and applications, thus being able to present improvements to this model and achieve better privacy for the electronic voting process, totally eliminating the vulnerability of voter confidentiality. If the blind signature process is successful, we will have achieved the objective of privacy and confidentiality, including encryption algorithms in the presented scheme, which helps to strengthen the security of information, proposing that the voter's information does not run any risk.

Figure 2 shows the description of the voting process to be signed from the voter to the signer and vice versa.

Explanation of the generated diagram is described.

The voter carries out the process of suffrage.

The voter requests the signer's public key.

In response, the signer sends his public key to the voter.

The voter masks and encrypts the vote through the RSA algorithm using the signer's public key.

The voter sends the encrypted message to the signer to proceed with the blind signature.

The signer signs the vote with his private key without knowing the information of the vote.

The signer returns the vote already signed to the voter.

The voter, through the reverse RSA algorithm and unmasking process, obtains the signed vote.
4. Discussion

According to the results of this investigation of our scheme, the protocol of the blind signature together with complemented algorithms manage to assure the process of the same in the electronic votes, and thus maintain the integrity of the data.

Our model proposes the union of several blind signature insurance schemes, in order to implement a prototype that meets the privacy requirements in the electoral votes, so that, in this way, the traditional is changed to something more secure and faster.

In our opinion, the algorithms used have better characteristics and capacity to reduce information security risks.

Every system has some percentage of failure, therefore, this model presented is exposed to changes and improvements to solve any failure.

5. Future Work and Conclusion

To define a prototype for the experiment and thus verify the assurance of confidentiality and privacy of the blind signature, this paper adopts cryptographic algorithms and security protocols to reduce risks in the electronic voting process.

It was concluded that, to implement a voting system with electronic signature in distributed architecture, it is advisable to encrypt the information to ensure the integrity of the system and guarantee the electoral processes. Although a single blind signature scheme will not be useful for all the applications in which it works, each of the exposed ones are efficient for some scope and inefficient for another. It is necessary to know that any system or scheme, especially in sensitive situations such as electronic voting, can be breakable, such as the manipulation of information or lack of privacy, which means that it is not safe in its entirety. Despite this, the algorithms studied in this article are highly efficient and safe, which can be used, together with cryptographic algorithms to

Figure 2 Description of the voting
keep the voter's information private.

Acknowledgment

The authors thanks to Universidad Politécnica Salesiana del Ecuador, to the research group of the Guayaquil Headquarters “Computing, Security and Information Technology for a Globalized World” (CSITGW) created according to resolution 142-06-2017-07-19 and Secretaría de Educación Superior Ciencia, Tecnología e Innovación (Senescyt).

References


