# A Homomorphic Encryption Approach in a Voting System in a Distributed Architecture

Segundo Moisés Toapanta Toapanta
Computer Science Department
Universidad Politécnica Salesiana Ecuador
Guayas, Guayaquil, Ecuador
E-mail: stoapanta@ups.edu.ec

Luis José Chávez Chalén
Computer Science Department
Universidad Politécnica Salesiana Ecuador
Guayas, Guayaquil, Ecuador
E-mail: lchavezc@est.ups.edu.ec

Javier Gonzalo Ortiz Rojas
Computer Science Department
Universidad Politécnica Salesiana Ecuador
Guayas, Guayaquil, Ecuador
E-mail: jortiz@ups.edu.ec

Luis Enrique Mafla Gallegos
Computer Science Department
Universidad Politécnica Salesiana Ecuador
Guayas, Guayaquil, Ecuador
E-mail: enrique.mafla@epn.edu.ec

***Abstract*—It is considered that Electronic Votes is an alternative of safer systems, which provides greater confidence and transparency to the general public, but the problems exist in the organisms that manage this process. The main objective is to describe the Homomorphic encryption, understand why this algorithm is the basis for different schemes mentioned in the document. There are several implementations of homomorphic properties that generate the possibility to continue analyzing the different encryption schemes and application areas as visualized in electronic voting. We use the deductive methodology, logical analytics, and exploratory research to analyze the description of three schemes that have a Homomorphic base. It is a basis for properly selecting a homomorphic scheme that fits a specific need. It is concluded that the homomorphic schemes presented in this analysis have different uses of algorithms, but they do not leave behind the efficiency that all present, at the same time the reference is made to a distributed architecture that helps to have an additional point when dealing with the information obtained in electoral.**

***Keywords—Homomorphic, encryption, cryptogram, security database, security information***

## I. INTRODUCTION

The electoral process has always been a topic of controversy in several countries of the world, owing to inconsistencies and fraud at the time of defray and counting the votes. In addition, it should be noted that the electoral votes are unsustainable and spend many resources such as the large number of ballots [1], additional tools that are currently provided to perform the so-called rapid count, including police and military personnel, as they must protect the ballot box so that there are no inconsistencies. This is compounded by the fact that in many countries people deprived of their liberty, as the word implies, do not have the freedom to vote [2], since they do not want to spend resources on them. From this problem is born the electronic vote that is a mechanism that is being implemented little by little in different countries like Mexico, Switzerland, USA, Spain, etc.[2][3]. There are several proposals for a device to apply electronic voting, such as cell phones, tablets, electronic machines specially designed for voting [4]. Consequently, there is also a growth in electronic and computer insecurity. When having this growth of insecurity several algorithms and methods of encryption for the information of the votes are proposed. In this case, we particularly talk about Homomorphic encryption, which has a wide scalability since there are several schemes and processes where its algorithm is implemented [5]. The analysis of this cryptographic method occurs both on the part of the voter and when making a vote count, despite its efficiency has flaws that are trying to improve, modifying its structure, but maintaining its Homomorphic logical base [5][6].

Why use Homomorphic encryption for the security of electoral information having more options in the middle?

For through this type of algorithms you can optimize the vote count; the homomorphic encryption technique is used to perform calculations on encrypted data, therefore it is not necessary to decipher the data [6], this saves time by performing an unnecessary process.

The articles reviewed in this phase are:

Advance E-Voting System Using Paillier Homomorphic Encryption Algorithm [7], Secure Voting in the Cloud Using Homomorphic Encryption and Mobile Agents [8], Okamoto-Uchiyama Homomorphic Encryption Algorithm Implementation in E-Voting System [9], Homomorphic Encryption-State of the Art [10], Efficient Proof Of Validity Of Votes In Homomorphic E-Voting [11], E-Voting Requirements and Implementation [12], Electronic Voting - Scopes and Limitations [13], Desing of a Secured E-voting System [14].

The objective of this study is to analyze, understand and give to understand the schemes that are derived I have implemented with this type of homomorphic encryption, when used for electronic voting. To this is added a review of why a distributed architecture would be indicated for this type of electoral process.

The result obtained from the study is to understand and

have the basis to be able to choose properly a homomorphic scheme that fits our need. It is concluded that the homomorphic schemes presented in this analysis have different uses of algorithms, but they do not leave behind the efficiency that all present, at the same time reference is made to why a distributed architecture helps to have an additional point when processing information obtained in electoral processes.

It is concluded that the Homomorphic schemes presented in this analysis have different uses of algorithms, but they do not leave behind the efficiency that all present, at the same time reference is made to why a distributed architecture helps to have an additional point when processing the information obtained in electoral processes

## II. Materials and Methods

One of the main advantages of the homomorphic encryption is that you do not need to decrypt your data to be carrying out a vote count automatically, therefore also the results that will be shown will be encrypted [5][6]. There is also the possibility of decrypting these data, this would be achieved through public [7] or private keys depending on the scheme used. For this reason, this encryption has been implemented in different schemes such as in the cloud or hosted in servers distributed nationwide in a specific región [8]. In this study, some schemes or derivations of Homomorphic encryption are recognized, having this algorithm as a base.

## III. Materials

### *A. Homomorphic Cipher Scheme Using ECC with ElGamal.*

ECC with the ElGamal is based on the algebraic structure of elliptical curves on fields [6][7]. The elliptic curve cryptosystem is a public key encryption technique. It works on points in an elliptical curve. The security of elliptic curve cryptography depends on the size of the key used. It works on points in an elliptical curve. The security of elliptic curve cryptography depends on the size of the key. Use a smaller key size compared to other public key cryptosystem algorithms with better security [6].

Fig. 1 gives us an overview of how this ElGama scheme works. First, the input text will be coded to points on an elliptic curve and then encrypted with the ECC-ElGamal encryption scheme. Then the results are sent to the end user, for this the encryption is decoded again to have an output in plain text [4][6].

### *B. Okamoto-Uchiyama Algorithm.*

These algorithms use asymmetric keys to perform their encryption, use a public key to encrypt a message or text and with the private key they can decrypt that message. As mentioned above, one of the main characteristics of Homomorphic properties allow to perform encrypted operations, such as addition, subtraction, multiplication [5][9]. This property will remain in the algorithm, the difference with other algorithms will be that Okamoto- Uchiyama, generates public keys by means of prime numbers of large digits.

### *C. Paillier Cryptogram.*

This type of cryptography is based on a probabilistic encryption with a Homomorphic base. This encryption makes use of two public keys that can be X, Y [7][10]. The applications that use this cryptography are used both in electronic votes and electronic money applications, likewise it must be remembered that these applications have a base of homomorphic properties [10].

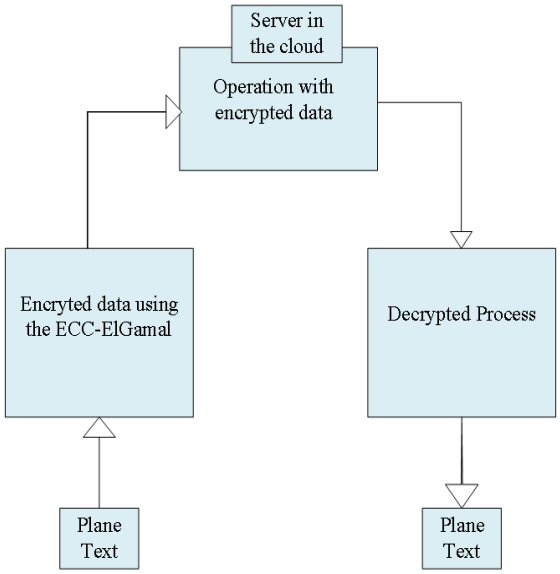


Fig. 1. Proposed Model for ECC-ElGamal.

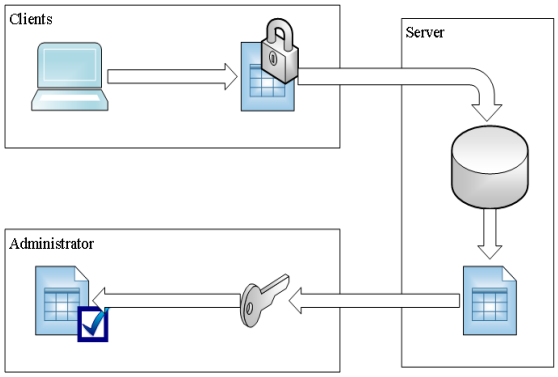


Fig. 2. Design of an electronic voting system.

Fig. 2 shows a basic scheme at the time of making the vote, the customer makes his vote and this Fig. is automatically encrypted to be sent to a server that was responsible for making the vote count, then the indication that the Encrypted file, the sea of one vote or the total vote counts can be viewed by an administrator with the proper key.

### *D. Homomorphic Property.*

This property has been mentioned in all the previous schemes since each scheme has its function [5][8][10] and according to its work has come to modify the structure of the Homomorphic Encryption, but keeping it the base that would be can perform their algebraic operations while the text is encrypted [11]. We have two types of encryption:

*1) Partial homomorphic encrytion*

This cipher is the best known and is considered a homomorphism, where five variables are used:

- P which is an infinite set of possible plain text.
- C designates a finite set of encrypted texts.
- K a finite set of possible keys.
- E state that for each $k \in K$, there is an encryption rule $e_k \in E$
- D state that for each $d_k \in D$ there is an encryption tule [5] [10].

Example:

$$e_k : P \to C \text{ y } d_k : C \to P$$

This example gives us to understand that for each $e_k$ containing $P$ plain texts, there will be an encryption $C$ and at the same time $d_k$ expresses that for each ciphered text $C$ open the key to decipher.

*2) Full Homomorphic encrytion*

This complete encryption is known as RING, has the same variables as a partial encryption, but change their rules when encrypting and decrypt these would be:

- K it is th space of the key.
- For each $k \in K$, there is an encryption rule $e_k \in E$ and a corresponding decryption rule $d_k \in D$ [5] [8] [10].

*E. Distributed Architecture*

A distributed system in an electronic voting system will be essential, since with this the voter will send the information not only to a database to process the results. These distributed architectures are a requirement because they save the fact of interacting directly with the democratic process [12], comparing with the ballot system that you have to be aware of the polls and more resources. And according to the configuration that is used the systems will not only help to distribute a vote, they will help keeping voting credentials, passwords, etc.

The distributed systems that are to be applied for an electronic electoral process must provide:

- Secure channels that provide privacy and maintain the so-called secret vote
- Anonymous channels that goes hand in hand with maintaining the identity of a voter and his election in the electoral process [12].

## IV. METHODS.

This analysis is carried out by means of a logical analytical method when reviewing algorithms and schemes where Homomorphic encryption is used, which is currently used to perform a count of electronic votes at scale, since it does not need to be reviewing user by user [11]. As a first point we have to mention the algorithms Okumato-Uchiyama, Pailler, ElGamal. [6][7][9][10], which are applicable for the electronic voting modality, besides its application is not limited to only this process, since they can be used for security in electronic money [10]. The result of a vote is a total sum of all the voters having as a response a winning candidate, the one with higher SI or acceptance [8]. Any Homomorphic scheme that is applied must allow:

- Hiding: that says an administrator should not know what value is YES or NO or the election of the voter.
- Homomorphic Counter: Refers that any user adding a new YES or NO successfully uploads to where they will be hosted either in the cloud or in teams distributed regionally.
- Verification: this allows the voter to verify that their vote has been counted for the final sum [11][12].
- Multiple candidates: it refers to the ballots whit multiple options and that can be assigned a certain number of votes per user [8][14].

## V. RESULTS

The result of the research and analysis is that there is not only a Homomorphic scheme applicable to electronic approval. These different schemes with respect to the homomorphic algorithm, are responsible for making the electronic voting systems safe and functional, maintaining the integrity of the stored data.

Fig. 3 tells us that Homomorphic schemes are efficiently coupled to a distributed architecture because they give a bonus to keep the data intact, and at the same time have a good performance in saving the data in the cloud that can be private and public to the time. The latter is used for public knowledge and obtain voting credentials. It is not necessary to download all the encrypted votes to perform Homomorphic operations referring to the addition, subtraction, multiplication, division, this can be done directly in the cloud and you only get the result that will also be encrypted.

## VI. DISCUSSION

With what has been mentioned in the results obtained from this research, the importance of encryption for electronic votes and the different algorithms that can be taken is appreciated. The robustness of the algorithm will depend a lot on the scheme that is applied and for which technological means will be implemented. By applying an encryption based on homomorphism to a distributed architecture we are expanding the data processing to have shorter response times. There is still a great variety of schemes with homomorphic properties that are not mentioned in the study, because applying the property of calculating an encrypted text is considered homomorphism. This analysis will provide an understanding to know what algorithms and encryption to use. It will help boost reading and search methods to apply security to electronic voting.

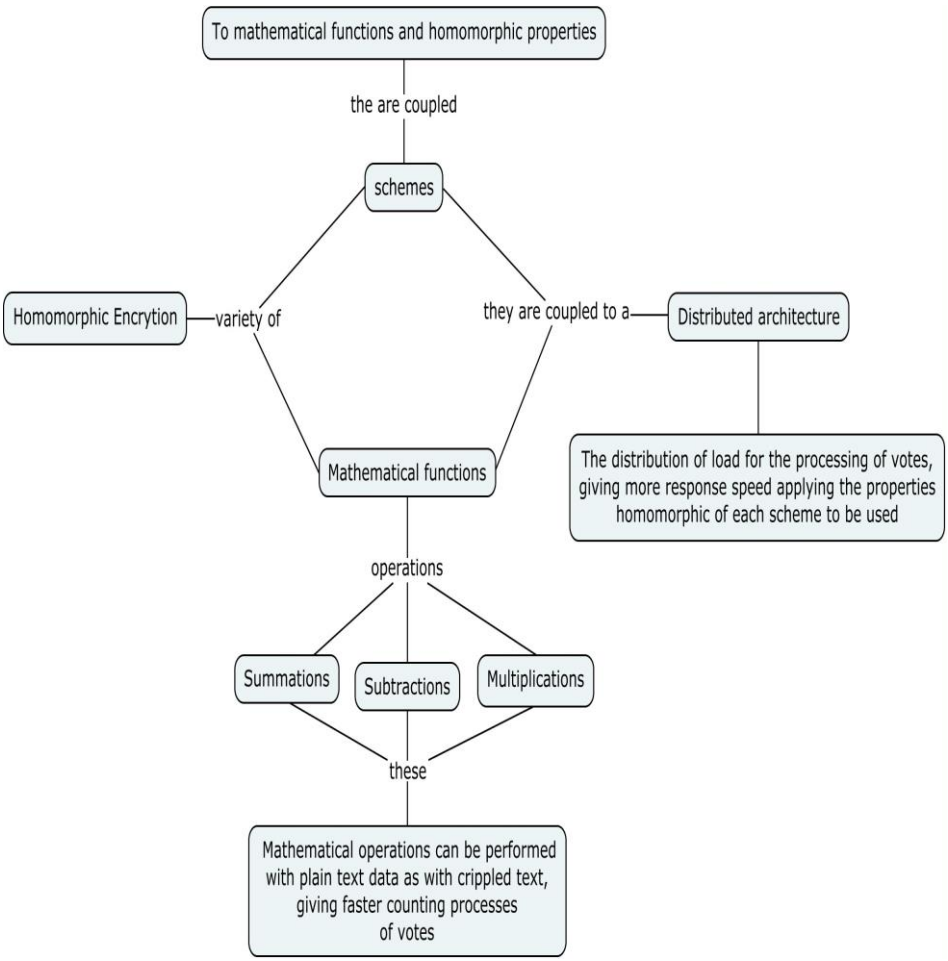


Fig. 3. Analysis of homomorphism

## VII. Future Works and Conclusions

We define the processes and resources in an electoral organization to choose, experiment and implement a Homomorphic encryption to verify the assurance of the integrity of the data.

Electronic votes are being implemented in many countries worldwide. This is due to the saving of already mentioned resources and the ease, scalability and reuse of computer resources; This last mentioned point is achieved once a digital device has been established such as cell phones, computers, etc. and a homomorphic scheme for their safety these two components can serve us in several electoral processes. The different homomorphic schemes would be easily coupled to any type of architecture, but the suggested one is a distributed architecture due to the better redundancy and the work load distribution. The results about the distributed architecture in a cloud give us a vision of the possible redundant and agile implementations that these architectures offer to share the information load that when uniting it with a homomorphic scheme, vote counts can be made with the encrypted data.

## 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

[1] X. Yang, X. Yi, S. Nepal, A. Kelarev, F. Han, "A secure verifiable ranked choice online voting system based on homomorphic encryption", *IEEE Access*, vol. 6, pp. 20506–20519, 2018.

[2] M. Lubis, M. Kartiwi, S. Zulhuda, "Election fraud and privacy related issues: Addressing electoral integrity", *2016 International Conference Informatics and Computing*. ICIC 2016, Icic, pp. 227–232, 2017.

[3] D. Y. M. Del Blanco, L. P. Alonso, J. A. H. Alonso, "Review of Cryptographic Schemes applied to Remote Electronic Voting systems: Remaining challenges and the upcoming post-quantum paradigm", *Open Math*, vol. 16, pp. 95–112, 2018.

[4] D. Gentles, S. Sankaranarayanan, "Biometric secured mobile voting", *Asian Himalayas Int. Conf*. Internet, 2011.

[5] K. Makkaoui, El, A. Beni-Hssane, A. Ezzati, "Can hybrid Homomorphic Encryption schemes be practical?" *Int. Conf. Multimed. Comput. Syst.-Proceedings*. pp. 294–298, 2017.

[6] M. M. Potey, C. A. Dhote, D. H. Sharma, K. J. S. College, "Efficient Homomorphic Encryption using ECC-ElGamal Scheme for Cloud Data", pp. 39–43, 2016.

[7] S. M. Anggriane, S. M. Nasution, F. Azmi, "Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm", no. Icic, pp. 0–4, 2016.

[8] M. A. Will, B. Nicholson, M. Tiehuis, R. K. L. Ko, "Secure voting in the cloud using homomorphic encryption and mobile agents", *International Conference on Cloud Computing Research and Innovation (ICCCRI)*, pp. 173–184, 2016.

[9] R. Suwandi, S. M. Nasution, F. Azmi, "Okamoto-Uchiyama Homomorphic Encryption Algorithm Implementation in E-Voting System", no. Icic, 2016.

[10] M. Mohan, M K, Kavitha Devi, V. Jeevan Prakash, "Homomorphic encryption-state of the art", pp. 1-6, 2017.

[11] K. Peng, F. Bao, "Efficient proof of validity of votes in homomorphic e-voting", *2010 Fourth International Conference on Network and System Security*. NSS 2010, pp. 17–23, 2010.

[12] R. Anane, R. Freeland, and G. Theodoropoulos. "E-Voting Requirements and Implementation," *2007 9th IEEE International Conference on e-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, e-Commerce, and e-Services(CEC-EEE)*, pp. 382–389, 2007.

[13] K. M. Alam, S. Tamura, "Electronic voting - Scopes and limitations", *2012 International Conference on Informatics, Electronics & Vision (ICIEV 2012)*, pp. 525–529, 2012.

[14] H. Hussien, H. Aboelnaga () Design of a secured e-voting system. *2013 International Conference on Computer Applications Technology (ICCAT)*, 2013.