Improving Anonimity in e-Voting system with ElGamal Homomorphic Cryptosystem

Shraddha Padhar[a,1,*], Payal Parmar[a,1,*], Shafika Patel[a,3,*], Niyatee Bhatt[a,4,*], Rutvij H. Jhaveri[b,1,*]

[a] *Shri S'ad Vidya Mandal Institute of Technology, Gujarat technological University, Bharuch.*
[b] *Assistant Professor, Shri S'ad Vidya Mandal Institute of Technology, Gujarat technological University, Bharuch.*

Abstract

The increasing use of public environments for storing data has raised the issue of confidentiality of processed data. Homomorphic encryption is solves this issue by allowing computations on the encrypted data to provide high degree of confidentiality for private information. Homomorphic encryption can be applied in any system by using either symmetric algorithms or asymmetric algorithms. In this paper, we propose an e-voting system to maintain secrecy about users' information by using ElGamal homomorphic cryptosystem; the system, does never decrypt the original votes and the voter's identity during the whole computation and hence, anonymity becomes the key advantageous feature of the system. ElGamal has the IND-CPA (Indistinguishability under chosen-plaintext attack) level security which contains highest degree of security. The paper represents the design of an e-voting system having the properties of homomorphic encryption with smaller key size.

Keywords: e-voting, Cryptography , ElGamal, Security , Homomorphic Encryption

1. Introduction

Data can be easily exposed by directly computing on the plaintext. Homomorphic encryption allows the mathematical operations on the ciphertext rather than on the original data which can never be decrypted for getting the result.

*Corresponding author
URL: s10padhar@yahoo.com (Shraddha Padhar)
[1]B.E., Shri S'ad Vidya Mandal Institute of Technology, Bharuch.
[2]B.E., Shri S'ad Vidya Mandal Institute of Technology, Bharuch.
[3]B.E., Shri S'ad Vidya Mandal Institute of Technology, Bharuch.
[4]B.E., Shri S'ad Vidya Mandal Institute of Technology, Bharuch.
[5]Assistant profesor, Shri S'ad Vidya Mandal Institute of Technology, Bharuch.

Hence, it is the most useful scheme in terms of security. The main aim behind the proposed approach is to apply the homomorphic encryption in the existing e-voting system for improving anonymity as well as to reduce the chances of breaking the original voting result before the announcement. Homomorphic encryption has two properties; multiplicative and additive homomorphic encryption. There are many factors which prove that the multiplicative homomorphic encryption is more efficient than additive homomorphic encryption. These factors are elaborated in [1]. Although the multiplicative homomorphic encryption has the higher performance than the additive, it is yet not applicable. So now we are going to preserve the multiplicative property of homomorphic encryption in our proposed system. Multiplicative property may be preserved by using RSA and ElGamal encryption algorithms [2]. ElGamal is semantically secure over the box where as in RSA, it is semantically secure only if there is a random padding [3]. Because of this reason we have chosen ElGamal encryption algorithm for preserving multiplicative property.

Due to the wide spread use of internet, e-voting is often presented as the ultimate manifestation of the democratic process, especially when applied to the conduct of general elections. The e-voting system should have the benefits like Mobility, Increased participation, Increased efficiency and accuracy, Transparency and many more [4, 5]. There are some requirements and principles of e-voting system for election which includes: Confidentiality, Anonymity and Integrity [6, 7]. Mix network and Homomorphic tallying are two main methods which have been applied to design e-voting schemes. E-voting system has some general entities like User (by whom the vote is given), Certificate Authority (User can get certificate from it), Administrative (it is for checking the eligibility of the user), Counter server (it counts the users' vote and gives the final result)[8].

The contribution of this paper is to build e-voting system having the characteristics and advantages of homomorphic encryption. In our system, the votes are never be decrypted even if the whole system is completed its counting of votes. And the algorithm we have used to implement multiplicative homomorphic encryption has the high degree of security and requires very large amount of time to decrypt it with only the knowledge of algorithm only so that even if any attacker will attack on the system, he will get result after a very long time. It has no meaning because before it the system will declare results itself. Thus the counting is done on the encrypted votes only. It preserves the characteristic of homomorphic encryption.

Henceforward this paper is organized in five sections. In section 2, some existing e- voting systems are briefly described which are related to the proposed approach. In section 3, flow of proposed e-voting system is shown with proper design view. In this section the limitations of existing system and the advantages of the proposed system over those existing systems are also discussed. In section 4, experimental results are given. At last in section 5, the paper is concluded which gives the summarized presentation of the whole paper.

2. Related Works

In this section, some related work of the e-voting system is briefly discussed. For the election monitoring process and receiving complaints from entities involved [9], adds an election commissioner (EC) in the scheme, in addition to the other entities. Protecting data transferred between e-voting components through insecure channel is performed by using cryptographic techniques. Asymmetric cryptographic systems can achieve high security strength but at high computational cost. Conventional solution is to employ asymmetric cryptography to perform key agreement and encrypt the data using the symmetric key afterwards. Research in [10] offered a hardware-based 277-bit ECC in the key exchange ECKE-2 protocol and AES-256 bit for data encryption. It is believed that by using this protocol-on-chip (PoC) and implementing symmetric algorithm, the process will be faster. In this cryptography process, every entity like certificate authority (CA), administrator (A) and counter (C) generates the key pair separately and announces the public key. No Collusion between all those entities is assumed here.

The e-voting scheme described in [11], there are two counters in order to increase security of the data for encryption/decryption of users' message; each counter has different key pair. Notations for this system are:

(i) **Counter1:** Private Key (Cpr1), Public key (Cpr2)
(ii) **Counter2:** Private key (Cpr2), Public key (Cpb2)
(iii) **Text:**vote/message (m)

In this system, first of all the user receives the certificate from CA. Then the user confirms the certificate to the administrator. The administrator checks users' eligibility and certificate validity. If those two factors in step (c) have been confirmed to be valid, the candidate list is sent to the user, in addition to its offline version; otherwise the user has to ask a new certificate to CA and the process is reset. The user encrypts the vote with both Cpb1 and Cpb2 separately to get (Ecpb1 (m), Ecpb2 (m)). Once receiving the vote, the administrative checks its validity by decrypting the message. In addition, the user list is kept to avoid votes from the same user. After all those processes, two counters exchange the decrypted vote. After that both counters send the acknowledgement to the administrator. And then administrator sends final acknowledgement to the user [11]. In following section we have described our proposed system. We have taken the existing system described in [11] as a benchmark system and have modified that system by applying homomorphic encryption.

3. Proposed Approch

The systems described in above section are improved by applying the homomorphic encryption. For this ElGamal cryptosystem is used because it has the highest security level of IND-CPA [12]. In addition, ElGamal is an efficient algorithm which cannot be easily decrypted as compared to other algorithms. It

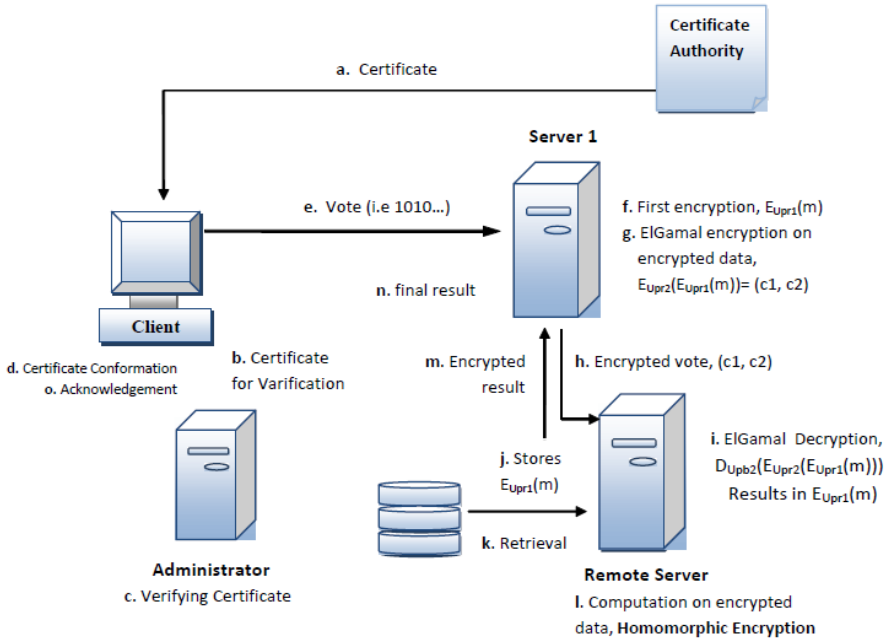

Figure 1: Our proposed e-voting system

allows lower system cost because it needs very low memory for implementation. So it is suitable for most of the devices used in e- voting system [13]. It is a somewhat simple algorithm compared with the ECC which would be very complex with many calculations. Hence use of ElGamal could save the processing time [14]. The main advantage of the ElGamal is that it gives the different cipher text for the same plain text each time it is encrypted [15].

In this section, the working of the proposed system is shown in the diagram. Here, the system is divided in two phases. In the first phase of system, there can be number of clients can vote and their votes are encrypted by symmetric encryption and then the result of the symmetric algorithm encryption will be further encrypted by the ELGamal encryption. Hence, double encryption is done from which only one encrypted message is decrypted but it gives the encrypted data. And the processing is done on these encrypted data only. So, the original data cannot be disclosed anyhow. In second phase, the encrypted message by ElGamal encryption algorithm is then decrypted by server and the decrypted data is stored in the counter and counter will give the sum of the encrypted data. Then result is given to the server at client side. Figure 1 shows the model of our system.

(i) **m :** original message
(ii) **User :** Private keys (U_{pr1}, U_{pr2}), public key (U_{pb2})

(iii) $\mathbf{E_{Upr1}}$, $\mathbf{E_{Upr2}}$: encryption by using private key of user.
(iv) $\mathbf{D_{Upb2}}$ **:** decryption of ElGamal using public key of user.

The steps in which the system works are given below.

(a) User receives the certificate from the certificate authority.
(b) User confirms the certificate to the administrator.
(c) Administrator checks users' eligibility and certificate validity.
(d) Certificate authority gives the confirmation message to the user if the certificate is valid.
(e) User or voter votes for the candidates. This vote will be generated in the binary form. 1 for the candidates who has been voted and 0 for the candidate who is not voted. And generates m. i.e. there are 4 candidates and the votes are given to the candidate number 1 and 3 then,

Candidate 1: voted (1)
Candidate 2: not voted (0)
Candidate 3: voted (1)
Candidate 4: not voted (0)

Hence the message will be: 1010 (m1)
(f) Then this m will be encrypted by the server1 with users' private key and generate EUpr1 (m). Suppose there is key l1 for the user 1 then the vote given by 1st user will be transferred as,

$$m1' = l1 + m1 \tag{1}$$

$$\boldsymbol{l} = (l_1, l_2, \ldots, l_n) \tag{2}$$

(g) After this first encryption, the encrypted message will also be encrypted further by the ElGamal encryption algorithm. And suppose it will generate two cipher texts say c1 and c2 from one plaintext.

$$E_{Upr2}(E_{Upr1}(m)) = (c1, c2) \tag{3}$$

$$c1 = g^k mod p \tag{4}$$

$$c2 = m'K mod p \tag{5}$$

Here, g is the generator and p is the prime number and

$$K = Y^k mod p, Y = g^x mod p. \tag{6}$$

(h) These c1 and c2 will be then transferred to the remote server.
(i) These c1 and c2 will be decrypted by the remote server by using ElGamal decryption algorithm. Here it will get the encrypted message because the decryption of that encrypted c1 and c2 is the result of the first encryption,

$$(E_{Upr1}(m)) \tag{7}$$

Firstly, following will be calculated.

$$c1^x mod p = k \tag{8}$$

$$m' = K^{-1} c2 mod p \tag{9}$$

where k^{-1} is evaluated by using Extended Euclidian.

(j) Remote server will store this encrypted data (m') one by one in the database. This process will be continued until the voting process is completed.

(k) Then at the time of completion of the process, remote server will retrieve those encrypted data from the database for performing computation.

(l) Remote server will perform the computation on the encrypted data which are stored in the database

(m) Send this encrypted result data to the server1.

(n) At last the final result will be computed at the user side only by deception with the private key of the user. This key is only known to the server1 which is only at the user side.

$$\sum_{n=1}^{k} m'_n - l_n \tag{10}$$

(o) Finally the result is sent to the admin and admin will announce the final result.

According to the trustworthy entities scheme [16], the users' anonymity is also kept. The original vote will never be decrypted in the whole system so that no one attacker can get the original data. Hence In our system, all the entities like confidentiality, integrity, efficiency, accuracy, privacy, authentication as well as verifiability can be maintained.

4. Theoretical Analysis

The proposed system is the ElGamal based e- voting system which has the improvement that the voting scheme is secured by the homomorphic encryption. Here, instead of additive property the multiplicative property of the homomorphic encryption is preserved for making system more efficient because with the same factors needed standard exponentiation for tallying in additive homomorphic encryption is larger than it is in multiplicative homomorphic encryption [17].

The inspiration for making proposed e-voting scheme with the great degree of security is obtained by the system described in [11]. In this previous system based on the ECC encryption scheme, the original message is decrypted by counter and then votes can be counted. Hence, there is no privacy preservation can be maintained for vote. In addition, voter identity is also given to administrator with original vote so that any hacker can easily find which vote is done by which user. These are some limitations which can be overcome in the proposed system. The proposed system works only with the encrypted data so even if any attacker wants to read the votes or the result of the election before the announcement is done by the system itself, he will get the encrypted data only which is in the same form if the original data which make the attacker confused that whether it is original data or not. Even If he get the idea about the non originality of the vote, he will get the original result after a very long

time which is totally meaningless because before he can disclose the data, system will announce the result by itself. Hence neither active nor passive attack may create hurdle in the system. Following are some terms and features which are maintained in the proposed system analyze the security and measure the performance.

- **Authentication:** Only the authenticated users are allowed to vote. Any other voter will not be allowed. For example, only those users who are registered will be allowed.
- **Integrity:**If the sequence and the content of the votes are changed, it produces the wrong result. This problem is solved in the proposed system. In the proposed system, the fake votes will never be counted hence sum of only valid ballots will be counted.
- **Confidentiality:** The attacker cannot get any information about votes. The random number of each vote can only be known by the legal sender and private key of the receiver can be known by itself, so the proposed scheme can assure that there is not any piece of contents will be eavesdropped.
- **Privacy preservation :** All the ballots are secretly stored, not leaked to the voters. As well as each votes are encrypted twice before it is transferred to the remote server for the counting this preserves the high level of privacy of the votes.
- **Transparency:**No one can get the intermediate votes result in the proposed system. This is because in our system the original votes are never decrypted even if the whole system completes the counting as well.
- **Non- repudiation:**in the proposed system, if any voter has voted already then it cannot vote for second time. It means system verifies that voters' participation count should be only one. Duplication is strictly prevented.

5. Experimental Results:

In this paper, the main focus is on the comparative evaluation of ElGamal based homomorphic encryption for e- voting scheme to the existing e-voting scheme based on ECC cryptosystem described in [11]. The proposed system can maintain integrity, confidentiality and anonymity. The main advantage of the ElGamal is that it is based on the difficulty of computing discrete logarithm. For any attacker, it is too difficult to know the private key of the sender because to recover the sender's private key, it would have to compute,

$$L = dlogK_{g,q}(YA) \tag{11}$$

For this the K must be recovered which requires to determine the random number k, and this requires the computation of the discrete logarithm

$$k = dlog_{g,q}(C1) \tag{12}$$

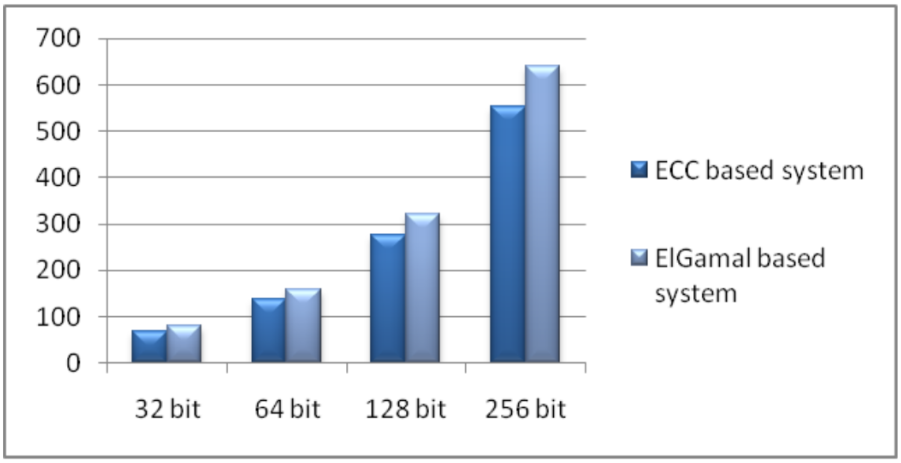

Figure 2: Comparison chart of encryption time

It is not a time consuming process which perhaps gives the result but after very long time when system itself announce the result.

The experiment is carried out in ASP.NET 2010. The Experiments are conducted on two different machines. Both the machines have similar configuration of Intel Core i3 processor, 4GB of RAM and 2.40 GHz of processing power. Proposed system contains many numbers of complex mathematical operations for performing encryption which makes system slower but provides high degree of security. Hence, it can be said that the system enhances the security level at the cost of time. In figure 4, there is a graph of time (msec) vs. key size used for encryption for both the system (ECC- based e-voting system and ElGamal based e-voting) is shown. The graph shown above shows that the previous e-voting system his faster than the proposed system but security level is improved. The voting system wants the higher security at the primary requirement. In figure 3, there is the graph of time (msec) Vs. Key size required for decryption is shown. As shown in above figure, the time required for decrypting our proposed system is higher than the existing system. It means that our system cannot be easily decrypted. This is because there are many complex operations are made in the system for the encryption. Hence, for disclosing the original data much time is required to decrypt the data. In addition ElGamal is used for applying the homomorphic encryption which has the highest security level and till now it is not decrypted by anyone. So decryption of ElGamal takes more time and before any attacker can know the original result by the decryption system itself provides the result.

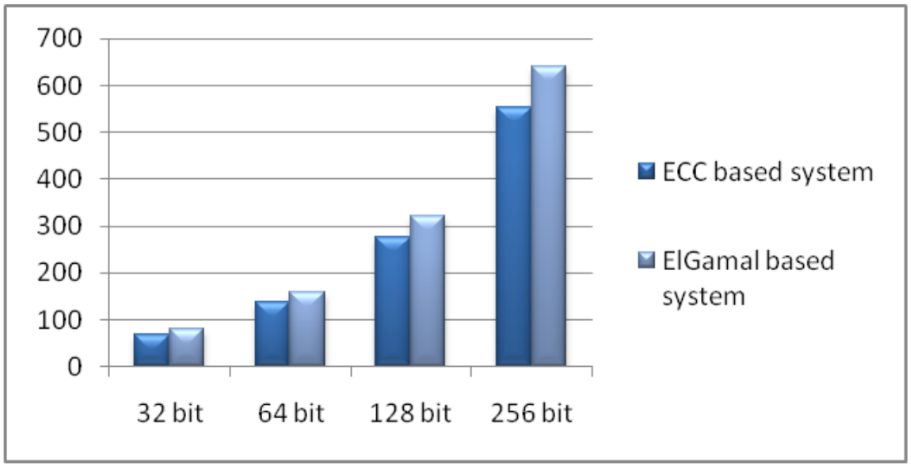

Figure 3: Comparison chart of decryption time

6. Conclusion

Encryption of the data transferred between two parties in the public environment is a critical part in keeping data security, especially for a confidentiality and integrity. But for having high level of security level, it is not good solution to use the algorithm demanding high computational cost. In our system we have used ElGamal encryption algorithm having higher security level with lower computational cost. Having the properties of homomorphic encryption in the e-voting system where the original votes and even the original counted result is not decrypted during whole system is itself a new approach for preserving high level of security. In this paper, we have described our proposed system theoretically which can be helpful to those researchers who want to make e- voting system more and more secure. Our paper may also help to the researchers who are wishing to carry out the research in the direction of the homomorphic encryption.

7. References

References

[1] Peng, Kun, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee, "Multiplicative homomorphic e-voting," in *Progress in Cryptology-INDOCRYPT* 2004, pp. 61-72. Springer Berlin Heidelberg, 2005.

[2] Taher elgamal, member, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," in *IEEE transactions on information theory* vol. it-31, no. 4, july 1985.

[3] Smid, Miles E., and Dennis K. Branstad, "Response to comments on the NIST proposed Digital Signature Standard," in *Advances in Cryptology—Crypto'92. Springer Berlin Heidelberg* 1993

[4] Anane, Rachid, Richard Freeland, and Georgios Theodoropoulos, "E-voting requirements and implementation," in *E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services* pp. 382-392. IEEE, 2007.

[5] Delaune S., Kremer S and Ryan M., "Verifying Properties of Electronic-Voting Protocols," `ftp://ftp.cs.bham.ac.uk`

[6] B. I. Simidchieva, M. S. Marzilli, L. A. Clarke, and L. J. Osterweil, "Specifying and verifying requirements for election processes," in *Proc. The International Conference on Digital Government Research, Digital Government Society of North America* 2008.

[7] M. Volkamer and M. McGaley, "Requirements and Evaluation Procedures for eVoting," in *Proc. The second international conference on Availability, reliability and security, IEEE* 2007, pp. 895-902.

[8] Joaquim, Rui, André Zúquete, and Paulo Ferreira, "REVS–a robust electronic voting system," in *IADIS International Journal of WWW/Internet 1, no. 2* (2003): 47-63.

[9] X. Yi, P. Cerone, and Y. Zhang, "Secure Electronic Voting for Mobile Communications," in *Proc. Vehicular Technology Conference*vol. 2, 2006.

[10] R. Duraisamy, Z. Salcic, M. A. Strangio, and M. Morales- Sandoval, "Supporting symmetric 128-bit AES in networked embedded systems: an elliptic curve key establishment protocolon- chip," in *EURASIP Journal on Embedded Systems* 2007. 4738.

[11] Tohari Ahmad, Jiankun Hu, Song Han, "An E-cient Mobile Voting System Security Scheme based on Elliptic Curve Cryptography," in *Third International Conference on Network and System Security*2012.

[12] Fouque, Pierre-Alain, and David Pointcheval, "Threshold cryptosystems secure against chosen-ciphertext attacks," in *Advances in Cryptology—ASIACRYPT 2001, pp. 351-368. Springer Berlin Heidelberg* 2001.

[13] Elbarbary, Enas, Ghada Abdelhady, Hussam Elbehiery, and Abdelhahim Zekry, "Secured and Transparent Computerized Voting System accessible everywhere," in *Journal of American Science 10* no. 1 (2014).

[14] Gjosteen, Kristian, "A new security proof for Damgård's ElGamal," in *Topics in Cryptology–CT-RSA*pp. 150-158. Springer Berlin Heidelberg, 2006.

[15] Press, Jim, "Secure transfer of identity and privilege attributes in an open systems environment," in *Computers and Security 10*no. 2 (1991): 117-127.

[16] G. Schryen, "Security aspects of Internet voting," in *Proc. the 37th Annual Hawaii International Conference on System Sciences* 2004.

[17] Peng, Kun, Riza Aditya, Colin Boyd, Ed Dawson, and Byoungcheon Lee, "Multiplicative homomorphic e-voting," in *Progress in Cryptology-INDOCRYPT 2004, pp. 61-72* Springer Berlin Heidelberg, 2005.