Comparative Analysis of Elliptic Curve Cryptography Based Algorithms to Implement Privacy Preserving Clustering through Secure Multiparty Computation

Ankit Chouhan
MTech Student
Dept. of Computer Engineering
NIT, Surat
(91)(9510391926)
chouhan.ankit03@gmail.com

Sankita Patel
Assistant Professor
Dept. of Computer Engineering
NIT, Surat
(91)(2612201588)
sankitapatel@gmail.com

Dr. D. C. Jinwala
Professor
Dept. of Computer Engineering
NIT, Surat
(91)(2612201593)
dcjinwala@gmail.com

ABSTRACT

In this paper, we focus on Elliptic Curve Cryptography based approach for Secure Multiparty Computation (SMC). Widespread proliferation of data and the growth of communication technologies have enabled collaborative computations among parties in distributed scenario. Preserving Privacy of data owned by parties is crucial in such scenarios. Classical approach to SMC is to perform computation using Trusted Third Party (TTP). However, in practical scenario, TTP are hard to achieve and it is imperative to eliminate TTP in SMC. In addition, existing solutions proposed for SMC use classical homomorphic encryption schemes such as RSA and Paillier. Due to the higher cost incurred by such cryptosystems, the resultant SMC protocols are not scalable.

We propose Elliptic Curve Cryptography (ECC) based approach for SMC that is scalable in terms of computational and communication cost and avoids TTP. In literature, there do exist various ECC based homomorphic schemes and it is imperative to investigate and analyze these schemes in order to select the one suitable for a given application. In this paper, we empirically analyze various ECC based homomorphic encryption schemes based on performance metrics such as computational and communication cost. We recommend an efficient algorithm amongst several selected, that offers security with lesser overheads and can be applied in any application demanding privacy. The same can be incorporated in the Privacy Preserving clustering which aims to protect the underlying attribute values of objects subjected to clustering analysis. In doing so, the privacy of individuals would be protected.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information System**]: Security and Protection

General Terms

Security

Keywords

Privacy, Homomorphism, secure multi-party computation, Clustering.

1. INTRODUCTION

The Privacy Preserving Data Mining (PPDM) is an area that aims to achieve data mining, while hiding the sensitive data from disclosure or interference [1]. It is required as nowadays organizations are collecting huge amounts of data and privacy issues arise when we use data mining tools on those data.

To achieve PPDM, Randomization based and Cryptography based approaches are used. The Cryptography based approaches provide a higher level of privacy but poor scalability[2]. Secure Multiparty Computation (SMC)[3] is a Cryptography-based approach which can be achieved with the help of Oblivious Transfer, Homomorphic and Secret Sharing based schemes. Oblivious transfer based schemes are not scalable due to their high computational and communicational overhead. Secret sharing schemes either use a dedicated server or Trusted Third Party (TTP) to achieve high level of privacy and accuracy but at high computational and communication overhead[4, 5].

Here, our focus is only on distributed clustering application. As a starting point we empirically evaluate the various ECC based Cryptosystem in order to incorporate that in the Privacy Preserving clustering because the secure multiple party addition is the basic building block which is required in the privacy preserving clustering. We used ECC for partitioned datasets as the advantages of key length of ECC over any other cryptographic techniques, gives us a low computational and communication complexity. The Cryptography based approach provides a higher level of privacy and it can be achieved by the Secure Multiparty Computation (SMC) through Elliptic curve cryptosystem.

In our proposed Approach, we have used different ECC Homomorphic Algorithm as encryption technique. We have used ECC preferably because of avoidance of multiple encryption, decryption and secure multiparty addition that eliminates the assumption about the Trusted Third Party (TTP).

2. PROPOSED APPROACH

In our proposed approach, we have taken three parties A, B, C. with their private messages m1, m2, m3. We used a base point that is generator which first converts the message into coordinates form M_1, M_2, M_3. Encryption/Decryption is performed by Party A. The decrypted total value is sent to B then to C and A.

As shown in Figure 1, M_1 is encrypted by one of the algorithm of ECC which converts the message M_1 to $E(M_1)$ which is sent to party B. Party B adds message M_2 with $E(M_1)$ and is sent to C. The cumulative Encrypted with addition of message from C is sent to A. The decryption is then performed on A where we decrypted our encrypted message and we get the total message as M. We performed rmap(M) by which we get the message m. This message from A is given to B and subsequently to C and then back to A.

After carrying out this algorithm, we calculated time and the cost to achieve SMC. We have proposed changes in the decryption part in the traditional algorithm of EC-NS[7], EC-P[8], EC-OU[8]. In our approach we have reduced the cost of B's and C's encryption. This proposed decryption was successfully run fulfilling the required SMC.

*The part of this paper is accepted and to be published in Journal of Information Security, Scientific Research, 2013.

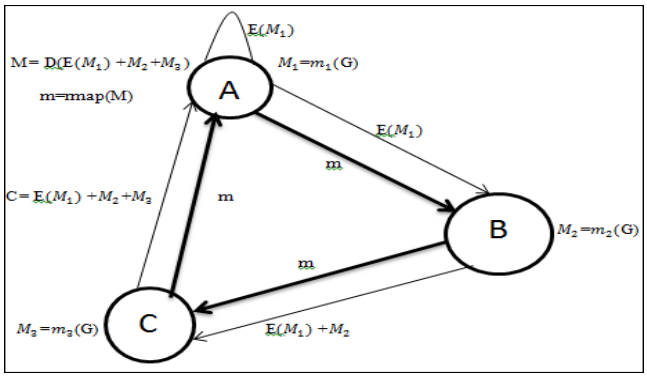

Figure 1. Proposed Approach

3. PERFORMANCE RESULT & ANALYSIS

We show our experimental results based on the time and cost on three Elliptic Curve Parameter, 112 bit or 160 bit or 256 bit [6].

Table 1. Results for 3 party communication when private value and prime value are random

Algo Name	secp112r1		secp160r1		secp156r1	
	Time (ms)	Cost (Byte)	Time (ms)	Cost (Byte)	Time (ms)	Cost (Byte)
EC-OU	316	1116640	335	1759344	399	2719744
EC-EG	254	1740624	286	2766464	322	4865544
EC-NS	303	4224968	349	4906592	402	7487984
EC-P	247	2437072	285	3741640	351	7123320

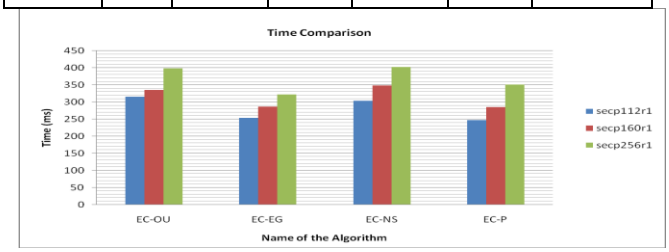

Figure 2. Time Comparison

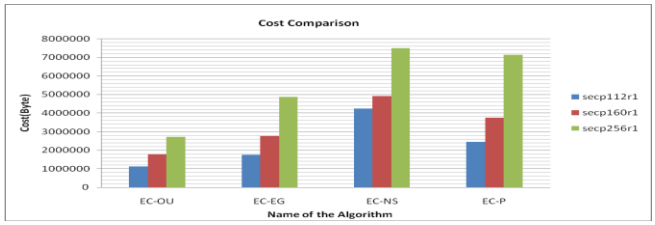

Figure 3. Cost Comparison

To get the fair results, we then took random parameters which are 341 bits long for all the algorithms other than EC parameter: We analyzed the results as shown in Table 2 During analysis we found that EC-OU and EC-EG takes lesser time where as EC-OU takes lesser space which is more than half of the other three Algorithms.

Table 2: Results for 3 party communication when private value and prime value as 341 bit long

Algo Name	secp112r1		secp160r1		secp156r1	
	Time (ms)	Cost (Byte)	Time (ms)	Cost (Byte)	Time (ms)	Cost (Byte)
EC-OU	316	1116640	335	1441264	399	2719744
EC-EG	309	4849840	321	5181296	357	6474552
EC-NS	336	5538552	382	6198584	407	8124376
EC-P	326	5515056	356	6504448	383	8760352

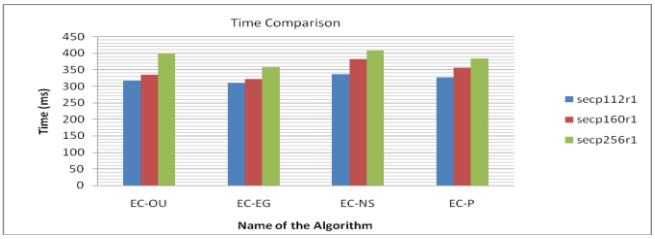

Figure 4. Time Comparison

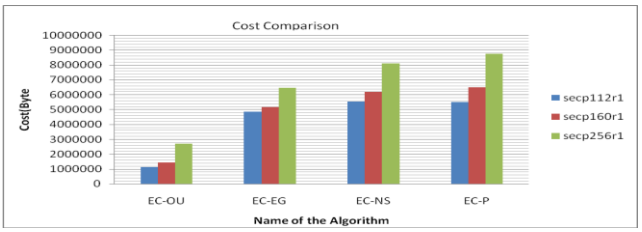

Figure 5. Cost Comparison

4. CONCLUSION AND FUTURE WORK

We presented an efficient approach for achieving secure multiparty computation with ECC additive homomorphic algorithm. We have carried out the experiment with four different algorithms. Our results clearly demonstrate that ECC based Okamota gives the best result with respect to time, cost and reduce the number of encryptions and decryptions for achieving secure multiparty communication.

Currently our algorithm supports secure multiparty computation. As a future work, we intend to extend our proposed approach for privacy preserving clustering. In addition, we intend to show the results from a realistic distributed emulation

5. REFERENCES

[1] Patel Sankita, Sweta Garasia, and Devesh Jinwala. 2012. An Efficient Approach for Privacy Preserving Distributed K-Means Clustering Based on Shamir's Secret Sharing Scheme. Trust Management VI, pp.129-141.

[2] Wang, Liu, Yue. 2007 Privacy preserving data mining re-search: current status and key issues. In: 7th International Conference on Computational Science 2007, pp. 762–772.

[3] O.Goldreich. 2004. The Foundations of Cryptography, vol. 2. Cambridge Univ. Press, Cam-bridge.

[4] Upmanyu, M., Namboodiri, A.M., Srinathan, K., Jawahar. 2010. Efficient Privacy Preserving K-Means Clustering. In: PAISI, pp.154-166.

[5] Doganay, Pedersen, Saygin, Savas. 2008. Distributed privacy pre-serving k-means clustering with additive secret sharing. In: 2008 international workshop on Privacy and anonymity in information society, pp. 3-11. Nantes, France.

[6] Elliptic Curve Domain Parameters. http://www.certicom.com/index.php/.

[7] T. ElGamal. 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. CRYPTO, IT-31(4):469–472.

[8] P. Paillier. 2000. Trapdooring Discrete Logarithms on Elliptic Curves over Rings. ASIACRYPT, pages 573–584.

[9] Steffen Peter, Dirk Westhoff. 2010. A Survey on the Encryption of Converge cast Traffic with In-Network Processing, IEEE Transactions on Dependable and secure computing, vol. 7, no.1.