International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Secure Sum Computation using Threshold Encryption for Semi-Ideal Model

Rashid Sheikh, Durgesh Kumar Mishra

Abstract: ***The need of preserving privacy of data arises when multiple parties work together on some common task. In this scenario each of the parties has to provide its sensitive data for a common function evaluation. But, the parties may be worried about the misuse of the data. Here comes the subject of Secure Multiparty Computation (SMC). The area where multiple cooperating parties jointly evaluate a common function of their data while preserving the privacy and getting the correct result is SMC. Here, we devise a new model and algorithm to compute sum of private data of mutually distrustful cooperating parties. We coin the term Semi-Ideal Model as it is hybrid of Ideal model and real model. The computation is secure on insecure network as well.***

Keywords: Secure multiparty computation, secure sum, semi-honest model, trusted third party.

I. INTRODUCTION

When multiple parties jointly work on some data, privacy becomes a concern for each of the parties as they may not be interested to reveal their data to other parties. The parties can be multiple government departments jointly working on a plan, many banks working on some project to find defaulters' pattern, and corporate that are working on some joint project. The area of information security where multiple cooperating parties evaluate a function of secret data without revealing the secret data to each other is called SMC. Many SMC protocols are available in the literature [1]. Primarily there are two goals of SMC; privacy of data and correctness of the result. SMC literature describes two models vz. Ideal and Real Model. There exists a Trusted Third Party (TTP) in first one which assists cooperating distrustful parties evaluate a function of secret data. The TTP must keep the data of each party secret and only declare the result of SMC to other parties. If the TTP work maliciously and disclose private data to some other party, the whole scheme fails. But in actual practice this model is used to provide government services to citizens and the government department or some government approved organization works as TTP. In other model no TTP exists and the parties themselves follow certain algorithm to evaluate the function of secret data. The participating parties are modelled as honest, semi honest, or malicious parties.

Manuscript published on January 30, 2020.
* Correspondence Author
Rashid Sheikh*, Computer Science and Engineering Department, Mewar University, Chittorgarh, India, prof.rashidsheikh@gmail.com
Durgesh Kumar Mishra, Computer Science and Engineering Department, Sri Aurobindo Institute of Technology, Indore, India, drdurgeshmishra@gmail.com

An honest party follows the rules in the algorithms and doesn't try to learn the sensitive data. The semi honest party follows the rules but also tries to learn secrets data of others. The malicious party may violate the rules of the protocol and attacks on the privacy. It is also called the corrupt party.
While designing a protocol for SMC the behaviour of the party must be taken in to account. The protocols differ in complexity and cost in respect of behaviour of participating parties.
SMC allows evaluation of different mathematical functions. For example sum, product, average, union, intersection, etc. In calculating the sum securely individual data is added and the result is obtained correctly without revealing the secret data to other parties. One of such algorithms was devised by Clifton et al. [2] in which the joint parties are supposed to form a ring structure. One of the parties works as an initiator. It selects a random number and adds to its secret data. The partial sum is sent to the adjacent party. The receiving party simply adds its private data to the received value and sends the new sum to adjacent party. This process is continued until the initiator party gets the sum of all the secret data plus the random number. Since the random number is known to the initiator party only, it subtracts the previously chosen random number to get the desired sum. The sum is distributed to all the cooperating parties. Clifton's scheme is shown in fig-1. The scheme is suitable for secure network as the data is sent in unencrypted form. The parties must be semi honest parties to get the correct result.
Our earlier work on the secure sum computation is presented in [3-5] where we dropped the use of random number and used segmentation technique. The individual data is broken into segments and the computation of the sum is done on these segments achieving the privacy and correctness goal of the SMC. We also presumed the semi honest behaviour of parties and the secure network. Here we propose an algorithm to evaluate sum securely and is also suitable for insecure networks. We use threshold encryption scheme [16] where a value is broken into pieces. The value can be reconstructed out of these pieces by taking the sum of certain minimum number of pieces (not necessarily all pieces).
Remaining paper is organised as follows: related work done is described in section 2. Section 3 provides informal description and formal description with algorithm. In section 4 results are given in a tabular form. Section 5 provides conclusion with some future possibilities of extension of our work.

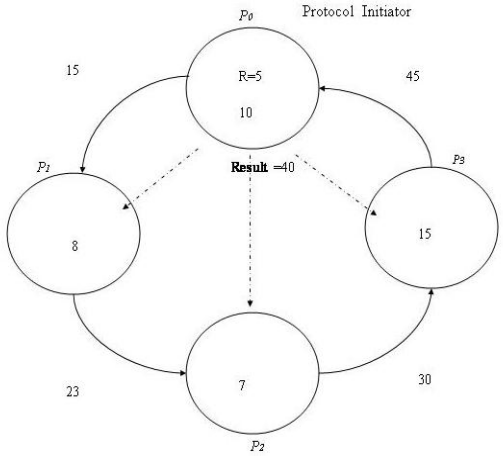

Fig.1. Secure sum algorithm [2].

II. RELATED WORK

The subject of SMC dates back to 1982 when Yao provided a solution to an interesting problem where two millionaires are interested in determining who is richer without showing individual wealth to each other. The problem is known as millionaires' problem. The solution to this problem used cryptographic methods. After Yao's two-party problem many other researchers like Goldreich [7] extended the problem to multiparty version using circuit evaluation technique. Based on these findings many researchers used the techniques to solve real life privacy-preserving problems like privacy-preserving private information retrieval [8, 9], privacy-preserving data mining [10, 11], privacy-preserving geometric computation [12], privacy-preserving scientific computation [13], and statistical analysis [14].

Computing sum securely forms an important component of distributed data mining where geographically distributed sites need to perform computation on their private data but no site wish to disclose the same. Clifton's algorithm is an important milestone for secure sum computation but suffered from few limitations. It is suitable for secure network lines, and for semi honest adversaries. Such adversaries around a victim party in the ring can conspire to learn the secret of middle party just by sharing what they send and what they receive. By taking difference of these shared values they can learn middle party's data. We in our work [4] removed this drawback by using segmentation approach. Another protocol [3] provided by us uses position change strategy in the ring to eliminate the probability of conspiracy by neighbours. In distributes k-secure sum protocol [5] we distribute the segments among parties before computation. This reshuffling eliminates possibility of being aware of the party's data segment. All these protocols are designed for a secure network where the data can flow unencrypted without any leakage. But the principle of security always assumes the network to be insecure. This fact raises the need of designing protocols for insecure network. In this paper we devise a secure sum algorithm suitable for insecure networks using threshold encryption [16] and Paillier's cryptosystem [15] for homomorphic property. In [16] Shamir proposed a scheme called (k, n) threshold scheme which allows reconstruction of a data D using k pieces out of total n pieces of D. That means it needs at least k pieces for reconstruction of the data.

Paillier's secure additive cryptosystem allows performing addition over encrypted data to get the result. Two data d_1 and d_2 satisfy following:

$E_{PU}(d_1+d_2) := E_{PU}(d_1) + E_{PU}(d_2)$

$E_{PU}(k.d) := k \times E_{PU}(d)$

Where PU denotes public key and E ( ) is the encryption function and k is a constant.

III.PROPOSED ALGORITHM

The Trusted Third Party (TTP) is in the centre of the structure which helps the cooperating parties evaluate the sum of their secret values. The objective is to get the sum correctly without disclosing the secret data to each other. The TTP is also not fully trusted by parties. Therefore the parties will not directly supply their data to TTP instead they seek help only. The responsibility of the TTP is to generate public-private key pair PU and PR. It also generate n shares of the private key using (k, n) threshold scheme where $k<n$. The scheme allows reconstruction of the private key using at least k shares.

A. Informal Description

The cooperating parties are kept in a logical ring. TTP's position is assumed to be in the centre of the ring as in Fig.2. The TTP will distribute the public key and the share of the private key to each of k parties, (PU, S_i) where S_i is the share of the private key for the party P_i. Now, one of the parties will work as the protocol initiator similar to the secure sum algorithm as in Clifton et al. [2]. The initiator party encrypts the data with it using public key received from the TTP. It send the encrypted value to the adjacent party. Receiving party adds this value with its encrypted data. The process is repeated by all the parties until the initiator party receives sum of encrypted data. As, the key pair is generated using homomorphic cryptosystem like Paillier [15], the sum is equivalent to the ciphertext of the sum of all the data. If it is decrypted by the private key, the result of the sum which is desired in this case.

For getting the private key all parties need to get the sum of the shares of the private key. The sum of these shares can be computed using k-secure sum protocol as in Sheikh et al. [4]. The initiator gets the sum of all the shares. By applying the properties of threshold scheme like Shamir's secret sharing [16] the sum is same as the private key PR. Now, the initiator will decrypt the public key encrypted sum of data by the private key. The result will be the sum of the secret data. The result is then distributed to all the parties.

Thus, in all there will be two rounds, one for the computing the sum of public key ciphertext and another for computing the sum of private key shares to recover the key.

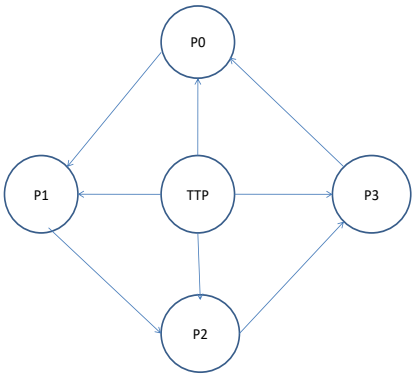

Fig. 2. Secure sum computation using threshold encryption in Semi Ideal Model

B. Formal Description

Formally, assume the parties P_0 to P_{k-1} having individual data d0 through d_{k-1}. The objective is to compute $\sum_{i=0}^{k-1} d_i$ such that any of the parties must not know the secret of any other party. The TTP generates a key pair (PU, PR) using homomorphic public key cryptosystem. It also generates n > k shares of the private key PR using Shamir's sharing of secret key [16]. Let us call a share as S_i. The algorithm comprising of two rounds, ciphertext summation round and the private key recovery round is shown as Algorithm 1 below.

Algorithm 1

TTP Actions:

Step1: TTP generates public key pair (PU, PR)

Step2: TTP generates n shares of private key PR with (k, n) threshold scheme such that k < n.

Step3: TTP distributes (PU, S_i) to each party P_i, where S_i is the share of PR for P_i.

Party Actions:

Round 1: For getting sum of public key ciphertext

Step1: One party say P_0 is selected as the protocol initiator. It computes ciphertext of its data d_0 as $E_{PU}(d_0)$ using public key, sends this vajue to adjacent party within the ring.

Step2: Each party P_i receives partial sum $\sum_{j=0}^{i-1} E_{PU}(d_j)$ of ciphertext from previous party P_{i-1} and adds ciphertext of its data $E_{PU}(d_i)$ and sends the new partial sum of ciphertext $\sum_{j=0}^{i} E_{PU}(d_j)$ to the next party P_{i+1} in the ring.

Step3: At the end the initiator party receives sum of ciphertext of all data $\sum_{i=0}^{k-1} E_{PU}(d_i)$

Round 2: For getting sum of private key shares to recover private key

Step1: One party say P_0 is selected as the protocol initiator. It sends its key share S_0 to next party P_1 in the ring.

Step2: Each party P_i receives partial sum $\sum_{j=0}^{i-1} S_j$ of Private key shares from previous party P_{i-1} and adds its share S_i, sends the partial sum of shares $\sum_{j=0}^{i} S_j$ to the adjacent party P_{i+1} in the structure.

Step3: At the end the initiator party receives sum of all shares $\sum_{i=0}^{k-1} S_i$

As per the threshold encryption scheme $\sum_{i=0}^{k-1} S_i = PR$

Round 3: Getting sum of data using property of homomorphic encryption

The sum of ciphertext received in the round 1 is equal to the ciphertext of the sum of data. When we decrypt the sum using the recovered private key we must get the sum of secret values with the joint parties. This is the secure sum.

$DPR(\sum_{i=0}^{k-1} E_{PU}(d_i)) = \sum_{i=0}^{k-1} d_i$

IV. RESULTS

Our work is theoretical research (not an experimental work) where we propose privacy preserving algorithms which are improved as compared to previously available algorithms. These improvements are depicted in the table I.

Table- I: Improvements if our proposed work

S. No.	Criteria	Previous Research	Our Proposed Algorithm
1.	Use of Random Number	Cliften et al. [2] used random numbers	Random number not used
2.	Type of network	Previous work [2-5] assume secure network	Applicable to insecure networks
3.	Role of TTP	In [17] the data is supplied to TTP	No data is supplied to TTP
4.	Type of SMC Model	Earlier literature describes only real and ideal model	Proposes a novel semi ideal model

The proposed model has many benefits while computing the sum of secret data of all the cooperating parties. The protocol is suitable for insecure networks as the data flow in encrypted form. The role of the TTP is also limited as it supplies only keys pair and the share of the private key. It does not deal with the secret data of the cooperating parties.

V. CONCLUSION

We devise an algorithm for computation which allows multiple honest but curious parties compute sum of their secret data without revealing it to each other. We have used a TTP which generates public-private key pair using additive homomorphic cryptosystem of Pallier and also generate shares of the private key using Shamir's secret sharing threshold scheme. We call it Semi-Ideal model because while distributing public key, and the shares of the private key the model works as ideal model. But while computing the sum, the model works as real model as no TTP is involved in computation. As the data flow in encrypted form the proposed model can also be used in insecure networks. The private key PR can be reconstructed only when all the cooperating parties provide their share.

REFERENCES

1. http://en.wikipedia.org/wiki/Secure_multi-party_computation
2. C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining," J. SIGKDD Explorations, Newsletter, vol.4, no.2, ACM Press, pp. 28-34, Dec. 2002.
3. 3. R. Sheikh, B. Kumar and D. K. Mishra, "Changing Neighbors k-Secure Sum Protocol for Secure Multi-party Computation," in the International Journal of Computer Science and Information Security, USA, Vol.7 No.1, Jan. 2010.
4. R. Sheikh, B. Kumar and D. K. Mishra, "Privacy-Preserving k- Secure Sum Protocol," in the International Journal of Computer Science and Information Security, USA, Vol. 6 No.2, pp. 184-188, Nov. 2009.
5. R. Sheikh, B. Kumar and D. K. Mishra, "A Distributed k-Secure Sum Protocol for Secure Multi-party Computation," submitted to a journal, 2009.
6. A. C. Yao, "protocol for secure computations," in proceedings of the 23rd annual IEEE symposium on foundation of computer science, pp. 160-164, Nov.1982.
7. O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in STOC '87: Proceedings of the nineteenth annual ACM conference on Theory of computing, New York, NY, USA: ACM, pp. 218-229, 1987.
8. 8. B.Chor and N. Gilbao, "Computationally Private Information Retrieval (Extended Abstract)," In proceedings of 29th annual ACM Symposium on Theory of Computing, El Paso, TX USA, May 1997.
9. 9. B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private Information Retrieval ," In proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science, Milwaukee WI, pp. 41-50, Oct. 1995.
10. 10. Y. Lindell and B. Pinkas, "Privacy preserving data mining," in advances in cryptography-Crypto2000, lecture notes in computer science, Vol. 1880, 2000.
11. 11. R. Agrawal and R. Srikant, "Privacy-Preserving Data Mining," In proceedings of the 2000 ACM SIGMOD on management of data, Dallas, TX USA, pp. 439-450, May 15-18 2000.
12. 12. M. J. Atallah and W. Du. "Secure Multiparty Computational Geometry," In proceedings of Seventh International Workshop on Algorithms and Data Structures(WADS2001). Providence, Rhode Island, USA, pp. 165-179, Aug. 8-10, 2001.
13. 13. W. Du and M.J. Atallah. "Privacy-Preserving Cooperative Scientific Computations," In 14th IEEE Computer Security Foundations Workshop, Nova Scotia, Canada, pp. 273-282, Jun. 11-13, 2001.
14. 14. W. Du and M. J. Atallah, "Privacy-Preserving Statistical Analysis," In proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, USA, pp. 102-110, Dec. 10-14 2001.
15. 15. Paillier, P., "Public-key cryptosystems based on composite degree residuosity classes," EUROCRYPT'99 , Prague, Czech Republic, pp.223–238, May2- 6, 1999.
16. 16. Shamir, A, How to share a secret,Communications of ACM. v22 i11. 612-613, 1979.
17. 17. D. K. Mishra, N. Koria, N.Kapoor and R.Baheti, "A Secure Multiparty Computation Protocol for Malicious Computation Prevention for Preserving Privacyduring Data Mining," International Journal of Computer Science and Information Security, Vol. 3, No. 1, pages 79-85, Jul. 2009.

AUTHORS PROFILE

Rashid Sheikh, has received B.E. degree in Electronics and Telecommunication Engineering from Shri Govindram Seksaria Institute of Technology and Science, Indore, India in 1994 and M.Tech. degree in Computer Science and Engg. From RGPV Bhopal, India in 2010. He is pursuing PhD on "Design of Secure Multiparty Computation Protocols for Privacy Preservation". He has 25 years of teaching experience. He is the program committee member of international conferences WOCN2012 and CONSEG2012. His subjects of interest include Computer Architecture, Computer Networking, Operating Systems, Network Security and Assembly Language Programming. He has published nine research papers in International Conferences and Journals. His research areas are Secure Multiparty Computation. He has authored of three books on Computer Organization and Architecture.

Dr. Durgesh Kumar Mishra, has received M.Tech. degree in Computer Science in 1994 and PhD degree in Computer Engineering in 2008 from DAVV, Indore. Presently, he is Professor (CSE) and Director at Shri Aurobindo Institute of Technology, Indore, India. He has 28 years of teaching and 15 years of research experience. He has published more than 90 papers in refereed international/national journals and conferences like IEEE, ACM conferences. He has organized many such conferences like WOCN, CONSEG and CSIBIG as conference General Chair and editor. He is a Senior Member of IEEE and held many positions like Chairman, IEEE MP-Subsection, and Chairman IEEE Computer Society Bombay Chapter, Chairman CSI Division IV Communications. He has delivered invited talk in Taiwan, Bangladesh, Singapore, Nepal, USA, UK and France. He is the author of a book "Database Management Systems". He was a consultant to sales tax and labour department of government of Madhya Pradesh, India. He has been awarded by CSI with "Paper Presenter award at International Level". He also visited MIT Boston and presented his talk on Security and Privacy, and chaired a panel on "Digital Monozukuri" at "Norbert Winner in 21st century".