International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Secure Multiparty Computing: A Decentralized Approach to GPA Calculation

Sayed Mohammad Badiezadegan

CEO Dataman Co. Funder, M.S. Cryptography (Applied Mathematics)
Email: *ceo[at]dataman.ca*

Abstract: ***In a decentralized world, where the Internet thrives without a central server, the concept of decentralization finds applications beyond technology. This article explores the critical notion of decentralization, highlighting its potential to eliminate the need for potentially corruptible service departments. To illustrate the practicality of decentralization, we present a scenario where a group of students aims to calculate the average GPA of their class without revealing individual GPAs. We introduce and review the Secure Multiparty Computing SMC protocol, assuming the integrity of all participants. In a basic 4-node SMC protocol implementation, students share random numbers, and collectively, they compute the class GPA without divulging individual scores. This method can be scaled for larger class sizes. Furthermore, we delve into an SMC implementation using an electronics circuit, drawing parallels between GPA calculation and electrical circuitry, emphasizing the importance of connections in achieving accurate results.***

Keywords: Secure Multiparty Computation, Decentralization, GPA Calculation, Privacy, Electronics Circuit

1. Introduction

The Internet is a decentralized network and there is no central server to serve users worldwide. Decentralization strategy can be used in many sciences of human societies. The critical point of decentralization is that system users do not need to hire a distinct department to serve system users because that service department is susceptible to corruption.

For example, suppose that the students of a class of N students want to find the grade point average (GPA) of their entire class according to the following conditions:

a) Without the help of any other person, such as a teacher or manager or...
b) No student knows the GPA of another student.

This proposed scenario can largely explain the necessity of using the Secure Multiparty Computing (SMC) protocol[1]. In the following article, we will introduce and review the SMC protocol to find the average of a data set under the mentioned conditions. In the following text, it is assumed that all the people present were honest.

Basic 4-nodes SMC protocol implementation

Suppose the described school class consists of 4 students Ali, Britney, Cyrus, and Dora. Their GPAs are abbreviated as A, B, C, and D. Now, each of the people finds 4 random numbers whose sum is equal to their GPA, for example, each person finds the following random numbers with indexes from 1 to 4 for themselves:

$A=a_1 + a_2 + a_3 + a_4$
$B= b_1 + b_2 + b_3 + b_4$
$C= c_1 + c_2 + c_3 + c_4$
$D= d_1 + d_2 + d_3 + d_4$

Then, each student keeps one of their own 4 random numbers for themselves and gives the rest of the 3 numbers to other 3 students as follows:

$a_1 , b_1 , c_1 , d_1 \Rightarrow$ Ali
$a_2 , b_2 , c_2 , d_2 \Rightarrow$ Britney
$a_3 , b_3 , c_3 , d_3 \Rightarrow$ Cyrus
$a_4 , b_4 , c_4 , d_4 \Rightarrow$ Dora

Now all the students calculate the sum of their numbers and publish them as follows:

$A'= a_1 + b_1 + c_1 + d_1$
$B'= a_2 + b_2 + c_2 + d_2$
$C'= a_3 + b_3 + c_3 + d_3$
$D'= a_4 + b_4 + c_4 + d_4$

Finally, each person can calculate the summation of A', B', C', and D' and then divide the result by 4. The final number is the class average GPA (or $\overline{GPA}$) because:

$(A'+B'+C'+D')/4 =$
$(1/4)(a_1 + b_1 + c_1 + d_1 + a_2 + b_2 + c_2 + d_2 + a_3 + b_3 + c_3 + d_3 + a_4 + b_4 + c_4 + d_4)= (1/4)(a_1 + a_2 + a_3 + a_4 + b_1 + b_2 + b_3 + b_4 + c_1 + c_2 + c_3 + c_4 + d_1 + d_2 + d_3 + d_4)=$ $(A+B+C+D)/4$

The most important point is that none of the class members were informed about their classmate's GPA, but they were able to calculate the class $\overline{GPA}$

This method can be expandable to N classmates while each student calculates N random numbers and gives N-1 random numbers to N-1 classmates through the mentioned steps. Then, each student calculates the summation of his/her part and other students together. Finally, all students publish their sum values and then find the class average GPA by dividing the sum by N.

SMC implementation with the help of Electronics circuit

Let's look back to the 4 classmates scenario. If each student considers his/her GPA average to be equal to the

electromotive force (EMF) of a power supply while all 4 power supplies corresponding to the students have the same internal resistance(r) and are connected together in a circular circuit following this diagram:

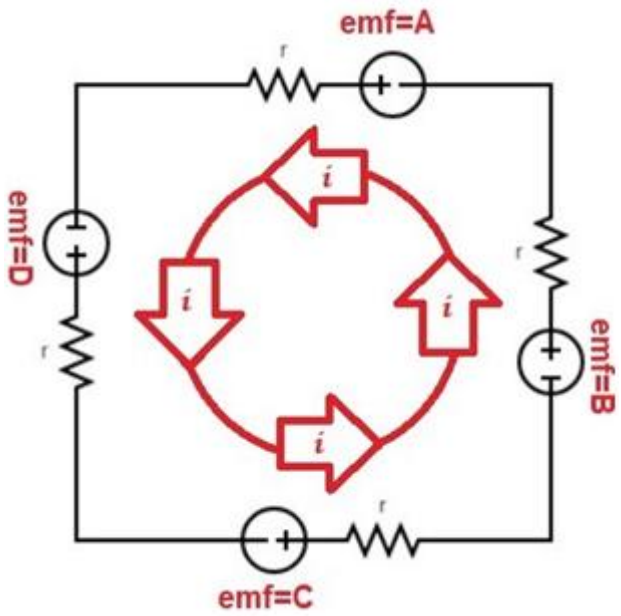

Figure 1: SMC-based electronics circuit

After considering the average value of power sources (emf) which is the average GPA of students or $\overline{GPA}$

$$\Sigma_{emf} = A + B + C + D = \overline{4\,GPI}$$

Also, According to the Ohm's law [2] in the Figure 1 circuit:

$$\Sigma_{emf} = 4\,ri$$

$$4ri = \overline{4\,GPI}$$

$$\overline{GPI} = ri$$

As a matter of fact, the class GPA would be calculated if each of students measure the current by Ampere Meter and this value is unique throughout the circuit.

The important point about elements connection is that neither power supply poles should not connect to same polarity of adjacent power supply.

References

[1] Cramer, R., Damga˚rd, I. B., & Nielsen, J. B. (2015). Secure multiparty computation. Cambridge University Press.
[2] Henry, T. (1992). OHM's Law, electrical math and voltage drop calculations. Tom Henrys Code Electrical.