Social, Ethical and Legal aspects of Yao technique and alternatives

Alessandro Castelli

Matriculation number: 12246581

Outline

1. Introduction

In this paper, you will find initially a brief introduction of the Yao protocol and the Multy-Party computation. After, I will discuss my implementation. Finally, I will show a few use cases.

1.1 A brief history of MPC and Yao

Cryptography was born in ancient times with the aim to hide the information. Over the centuries, the encryption techniques have evolved. The Multy-Party computation was born in the economic boom of the eighties and has been in development for the last decades.

Below a brief history of its evolution (1), (2):

- In 1982, Andrew Yao[1] introduced MPC with the Garbled Circuits Protocol, allowing two parties to jointly compute data without revealing inputs.
- In 1987, Oded Goldreich, Silvio Micali, and Avi Wigderson introduce the Goldreich-Micali-Wigderson (GMW) protocol, adapting two-party computation to multi-party.
- In 2008, First large-scale commercial application
- In 2010, MPC is first utilized by digital asset custodians and wallets for digital asset security

1.2 My function

In the project, I implemented a series of functions to calculate the maximum value of two protagonists (Alice and Bob), considering they both don't know the other's input. This problem is very similar to "Yao's problem millionaires" 2.1.

There are both negative and positive aspects of my implementation. If the two protagonists decide to use my code to calculate the maximum of two sets of values, they can do this by keeping anonymity on their inputs sets, but there is a problem: the final result is both returned, so this implies that at least one of their will know the maximum value of both.

This is against the principle of anonymity that the protocol underlies, in fact neither of the two protagonists should know the other's input.

I have identified two aspects that point out this problem:

1. The maximum function by its nature returns one of the inputs values
2. There are only two protagonists, this implies that if the maximum does not belong to your set of values, then it definitely belongs to the other person.

[1] Andrew Chi-Chih Yao is a Chinese computer scientist and computational theorist (9).

2. Use cases

In our day, there are a lot of two-party and multy-party computation use cases. We can find this technology in a lot of different aspects of our society, for example: medicine, economy, commerce, genetics, research and many other.

In the following sections, I will show the use cases that I found most interesting, and I will discuss in depth the topic that in my opinion is more interesting.

2.1 Yao's problem millionaires

This is a toy problem. I used it as first example because I think that it is useful to understand the potential of two-party computation.

The problem is as follows: "Two millionaires wish to know who is richer; however, they do not want to find out inadvertently any additional information about each other's wealth."

To resolve this problem is possible to use Yao protocol that calculates the maximum considering the two millionaires don't know the other's heritage. With this technique the protagonists can maintain their privacy.

2.2 Genetic Testing

In the last few years genetics has assumed an central role in the international scientific panorama. The Multy-Party computation can be used in this science (3). To make genetic tests it often is necessary to have data of people who have the desired genetic requirements (for example people who have a particular disease) but it is necessary to ensure the anonymity of the people who share their data.

Public health care does not exist in many countries and people must pay insurance. In a similar context it is essential to protect sensitive information about your health because insurance companies could use them to charge a higher insurance policy.

To avoid this many research labs use protocols like Yao or similar to collect personal data of patients. This implies that if the studies point out some disease of particular relevance, it could be very difficult for researchers to warn the people who shared their data.

2.3 Analysis of road traffic

The advent of connected autonomous vehicles provides opportunities for safer, smoother, and smarter transportation (4). In this scenario, it's easy to imagine how multy-party computation can be used.

Using the multy-party computation you can get real-time information about traffic conditions in a certain area and it will be possible for self-driving cars or drivers to choose the best itinerary.

Furthermore, with the multy-party computation the sensitive information on the location of the vehicle will be kept private. This could lead to decrease the road traffic and therefore to decrease the accidents caused by it, but it requires large computational resources.

2.4 Blockchain and digital currency

Briefly, a blockchain is a public distributed database. The blockchain is very important for many reasons, but today it is fundamental to make a cryptocurrency system (for example Bitcoin). Blockchain is a shared database that, different from classic database, stores data in blocks that are linked together (5).

You can image a blockchain as a chain in which every block contains:

- A personal hash code
- The hash code of the previous block
- Data

You can see in “Figure 1” (6) a simple example of Blockchain.

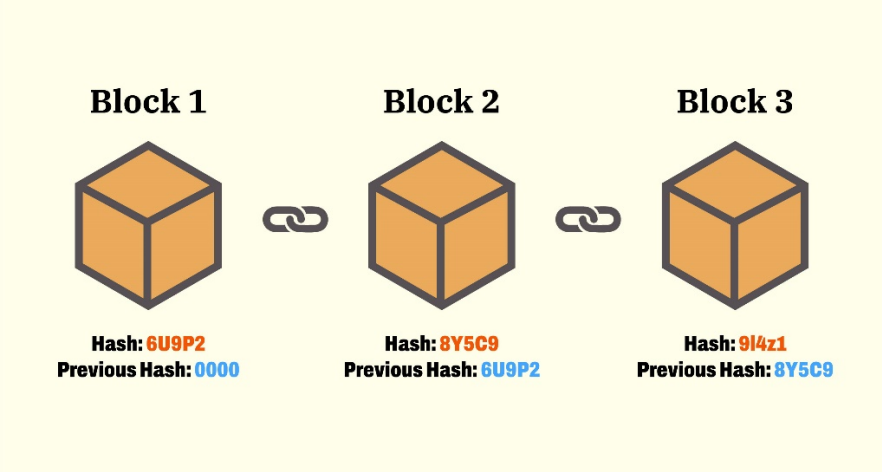

Figure 1

The power of the blockchain is that all data relating to a transaction are permanent and located in one "place" (in one block of blockchain). When you insert a transaction in a blockchain this is irreversible.

Transactions are validated by those who perform them through a digital signature procedure, this implies that the user must pay close attention about the private key that you use to validate the transaction is produced (7).

In this context, the Multy-Party computation is very important because the users can use it to calculate the digital signature in a distributed way. Therefore, the user avoids to keep their sensitive information in a single device.

When a transaction signature is required, all participants will start the multi-party protocol for the creation of a distributed signature. This represents a multy-party computation protocol to sign the transaction (8).

It’s obvious that multy-party computation has revolutionized the world of cryptocurrencies and blockchain.

This method requires a lot of computational resources and time, especially if we compare it with the classic digital signature method but it is one of the methods that allow you to do it safely and without trusted third parties.

Probably, the multy-party computation has changed the way of exchanging information or digital money.

3. Conclusion

In this article, I studied some cases of use of the multy-party computation and I tried to point out the advantages and the weaknesses of this technology.

I focused on how multi-party computation combined the world of blockchain and cryptocurrencies that I consider a “hot topic” of this historical moment. I analysed how important multy-party computation is for the protection of secret keys and digital signatures.

Of course, there are many other tasks where you can apply this technology, for example:

- Data collection for training of neural networks
- Extracting Intersection of Data Records
- Medical research
- And many others

In all this, you can find advantages and disadvantages.

The main advantages are:

- Preserve input privacy
- Correctness
- You don’t need a trusted third party
- High accuracy and precision
- Quantum-safe

The main disadvantage are:

- Computational overhead
- High communication costs between players

References

1. **Qredo.** What is multy-party computation. [Online] https://www.qredo.com/blog/what-is-multi-party-computation-mpc#andrewyoa.

2. **What is MPC (Multi-Party Computation)?** ***Firevlocks.*** **[Online] https://www.fireblocks.com/what-is-mpc/.**

3. Tamara Dugan, Xukai Zou. www.researchgate.net. [Online] https://www.researchgate.net/publication/306301560_A_Survey_of_Secure_Multiparty_Computation_Protocols_for_Privacy_Preserving_Genetic_Tests.

4. Tao Li, Lei Lin, Siyuan Gong. ***AutoMPC: Efficient Multi-Party Computation for Secure and Privacy-Preserving.***

5. HAYES, ADAM. Blockchain Facts: What Is It, How It Works, and How It Can Be Used. [Online] https://www.investopedia.com/terms/b/blockchain.asp.

6. What is Blockchain? ***money.com.*** **[Online] https://money.com/what-is-blockchain/.**

7. Blockchain, l'impatto del multi-party computation sulle cripto valute. ***NetworkDigital.*** **[Online] https://www.agendadigitale.eu/documenti/blockchain-limpatto-del-multi-party-computation-sulle-cripto-valute/.**

8. Secure Multi-Party Computation: applications within blockchain technology. ***eternacapital.medium.com.*** **[Online] https://eternacapital.medium.com/secure-multi-party-computation-applications-within-blockchain-technology-e07c727281e1.**

9. Wikipedia. Andrew Yao. [Online] https://en.wikipedia.org/wiki/Andrew_Yao.