650.030 – Introduction to Cybersecurity Summer Term, 2022/23

Project Write Up

Gabriele Voltan 12245815

1 Introduction

This project aims to provide a Secure Multi-Party Computation (SMPC) model using the Yao protocol [1]. Specifically, the parties, which are two in the project (Alice and Bob), will calculate the sum of their integer numbers without knowing the numbers of the other participant.

In the model, Alice plays the part of the *garbler*, i.e. the one who creates the circuit, while Bob is the *circuit evaluator*. Then, Alice creates the circuit and sends it to Bob, along with her encrypted inputs. Once Bob receives this, he calculates the results and sends them to Alice.

The model supports the *8-bit integers sum*. This, as specified in the project documentation, is a hard constraint which implies that the sum of the numbers of each individual participant must not be greater than 255 (maximum number that can be represented with 8 bits). The output of the model instead will have 9 bits, since the ninth bit will be that of the possible carry.

In order to implement this model, I used the code proposed by Olivier Roques and Emmanuelle Risson, available at the following address `https://github.com/ojroques/garbled-circuit`.

The rest of the document is structured as follows: section 2 briefly describes the proposed implementation and analyzes its fundamental properties (correctness and security) in order to verify its suitability for a real use; finally, in the 3 section some SMPC use cases are listed, analyzing the social 3.1.1 and legal aspects 3.1.2 of one of them, i.e. that of e-voting.

2 Implementation

This section briefly explains what the model implements and analyzes the correctness and safety of its operation, in order to consider its possible use in a real scenario.

This model implements the addition of two 8-bit numbers. Specifically, Bob and Alice, after entering their numbers, calculate the sum. Subsequently, with the two partial sums, the final sum will be calculated. The operation, constraints and description of the circuit are explained in more detail in the project documentation.

2.1 Analysis

The goal of Secure Multi-Party Computation is to compute a function, across multiple participants, without revealing information about their input data. Consequently, the aspects we are interested in considering are the *correctness* of the calculated result and the *privacy* of the input data.

Correctness Correctness means that the result calculated using Yao's protocol is equal to the result calculated normally.

In order to guarantee this property a Checker has been implemented, which through the *get_result* function returns the correctness or otherwise of the result calculated by the model.

Privacy of data Data privacy means that participants must not disclose information about their own sets of numbers.

In the proposed solution, each participant calculates the sum of their numbers locally. Subsequently, to calculate the final sum, the two partial sums are used. In doing so, no informations are released about the values of the set, nor about the number of elements in the set.

3 Use cases

Secure Multi-Party Computation is an excellent technology as it allows to calculate a result in a distributed way, preserving the privacy of the input data. The application of Yao's protocol is extended to many areas such as finance, statistics, government, military and medical. Here are some SMPC use cases:

- **Blockchain:** the private keys of a crypto wallet can be split (shards) among several parties in such a way that for any function to be performed, a minimum number of people holding key shares have to be involved [2].
- **Cryptographic key protection:** in this application MPC is not run between different parties holding private information. Rather, a single organisation uses MPC to generate keys and compute cryptographic operations, without the key ever being in a single place where it can be stolen. By placing the key shares in different environments, it is very hard for an adversary to steal all shares and obtain the key [3]. This use from a social point of view is very useful since very often passwords/keys are stolen. This could lead to the subsequent theft of classified data, creating major damage for the affected organization.
- **Collaboration between intelligence agencies:** for security reasons, intelligence agencies cannot give free access to their confidential information [4]. For this, through the use of the SMPC they can exchange information in order to combat

terrorist and digital threats. This use brings an enormous advantage in terms of collective security, while respecting the confidentiality standards required by the military domain.

- **Medical use:** in this field there are many possible uses. One use can be the collection of data in order to perform a statistic on some medical parameter (eg: calculation of the national average of the amount of cholesterol in the blood). Another use could be to use remote self-diagnosis tools [5]. In both uses, the privacy of health data is very important and is regulated by law (see article 9 of the GDPR).

- **Data analysis:** a statistical use is that of calculating the average salary of a specific category, within a country or continent [6]. For this application, the leak of data regarding salary data could trigger competition mechanisms between companies in the same sector. So from a social point of view, preventing this from happening is very important. There are many others applied to the financial sphere, for example.

- **Voting system:** a very important application is for voting systems. These systems can be used both for political voting and for other types of voting such as those within a company. Thanks to the MPC we can avoid cases of corruption and vote buying [7].

The use cases listed above are just a few of the possible use cases for MPC. In the literature there are a lot of use cases, all with a common goal, which is to maintain the privacy of the participants' input data. In the subsection 3.1 we explore the case of using the MPC for electoral systems, analyzing the social effects and the legal aspects of its use.

3.1 Voting system

A topic on which much research has focused over the years is that of electoral systems. In particular, an attempt was made to find a digital solution that was safe and reliable. By correctly representing the votes, the MPC allows us to achieve our goal.

However, Yao's protocol, used in the project, allows you to create a secure communication between two parties. An electoral system requires communication between n parties, as there are usually more than two voters. Beaver, in [8], has proposed a protocol, called BMR, which adapts Yao's to many parts.

How to represent the votes Suppose we have to carry out elections in which there are 50 voters and 3 candidates (which we will call a, b, c): each vote will be represented by 18 bits, $x_{a1}, ..., x_{a6}, x_{b1}, ..., x_{b6}, x_{c1}, ..., x_{c6}$.

In general, the total number of bits is given by the number of bits needed for each candidate ($\lceil log_2(num\_electors) \rceil$), multiplied by the number of candidates. So, the formula

will be

$$num\_bits = \lceil log_2(num\_electors) \rceil * num\_candidates$$

A vote assigned to candidate a will be expressed by the binary sequence 000001 000000 000000, one to candidate b will be 000000 000001 000000, while one to candidate c will be 000000 000000 000001.
The downside to this representation is that it uses a large number of bits.

How to obtain the result of the elections Summing all the votes we would always obtain a number with 18 bits (considering the previous example). Specifically, the first 6 bits on the left will represent the votes of candidate a, the next 6 bits those of candidate b and the last 6 bits those of candidate c.

3.1.1 Social Aspects

One problem of this technology is related to the usability of the system by elderly voters or those with a very low level of "digital literacy". If not all voters are able to use the digital voting system, a hybrid system (classical + digital) must be used to guarantee everyone the right to vote. From a technical point of view, we can consider the physical polling station as a user of the system.

In the context of the political elections, I quote the European Charter of Fundamental Rights, which regulates this aspect.

Article 39.1 - Right to vote and stand as a candidate in elections to the European Parliament

Every citizen of the Union has the right to vote and stand as a candidate in elections to the European Parliament in the Member State in which he resides, under the same conditions as nationals of that State.

An advantage of using this technology, in the context of political elections, is that it makes it easier to manage the votes of voters domiciled abroad, eliminating the physical transport of ballot papers. In addition to simpler management, e-voting also eliminates another problem related to the transport of ballot papers of residents abroad, i.e. the manipulation/replacement of these ballot papers.

Finally, another huge advantage is the fact that a voter is not able to prove who he has by voting, thus eliminating any possible coercion attempt.

3.1.2 Legal Aspects

A fundamental requirement that almost all states require is secrecy of the ballot. I quote the Italian and the Austrian law.

Article 48 - Italian Constitution

Voting is personal and equal, free and secret. Its exercise is a civic duty.

Article 60 - Austrian Federal Constitution

The Federal President is elected by the people of the Federation on the basis of secret, personal, direct and equal voting rights.

Even if not regulated, the secrecy of the vote is also important in contexts other than the political one (such as the corporate one), as it eliminates possible social problems related to a user's vote. For example, consider a scenario where employees have to elect a department head from among several area heads. If an employee of an area did not vote for her boss and the vote was not secret, the employee in question could experience job repercussions caused by his vote.

As repeatedly stated in this document, one of the objectives of the MPC is the secrecy of the participants' input data. In this scenario the input of the participants is represented by their vote. So, the application of MPC for the creation of a digital electoral system would respect the aforementioned laws.

References

[1] A. Yao, How to Generate and Exchange Secrets. In 27th IEEE Symposium on Foundations of Computer Science, pp 162-167. *IEEE Symposium on Foundations of Computer Science*, 1986.

[2] Pantther Team, A Deep Dive Into Secure Multi-Party Computation (MPC). https://blog.pantherprotocol.io/a-deep-dive-into-secure-multi-party-computation-mpc/#applications-of-multi-party-computation

[3] Yehuda Lindell, Secure Multiparty Computation (MPC), *Cryptology ePrint Archive*, 2020.

[4] Yehuda Lindell, Secure multiparty computation for privacy preserving data mining, *Encyclopedia of Data Warehousing and Mining*, 2005.

[5] Li, Dong and Liao, Xiaofeng and Xiang, Tao and Wu, Jiahui and Le, Junqing, Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation, *Computers & Security*, 2020.

[6] Frikken, Keith B, Secure multiparty computation, Algorithms and theory of computation handbook: Special topics and techniques, 2010.

[7] Nair, Divya G and Binu, VP and Kumar, G Santhosh, An improved e-voting scheme using secret sharing based secure multi-party computation, arXiv preprint arXiv:1502.07469, 2015.

[8] Beaver, D. Secure multiparty protocols and zero-knowledge proof systems tolerating a faulty minority. J. Cryptology 4, 1991.