622.755 – Introduction to Cybersecurity Summer Term, 2022/23

Project Write Up

Lorenzo Zanolin 12245822

1 Outline

Please write a general overview explaining the structure of your report. This can be brief (one paragraph), but it should make it clear how the report is structured. The overall length of your report must not exceed 5 pages (including figures, algorithms, tables, and references). This report is structured as follows: I will provide a brief overview of the the written project in Section **??**. Then I will explain how I would suggest you use your time to achieve a good write up in Section **??**, and finally I will explain and illustrate the marking scheme in Section **??**.

2 Yao's protocol

This project covers the Yao's protocol[3]; more precisely the *Secure Multi-Party Computation*. This protocol allows two parties, Alice who knows x and Bob who knows y, to compute jointly the value of $f(x, y)$ in a way that does not reveal to each side more information than can be deduced from $f(x, y)$[2]. In this scenario Alice is the garbler, while Bob is the evaluator. Another important role is the use of the OT[2], which is responsible to let Bob knows his encrypted input. An example of functioning is represented in figure 1.

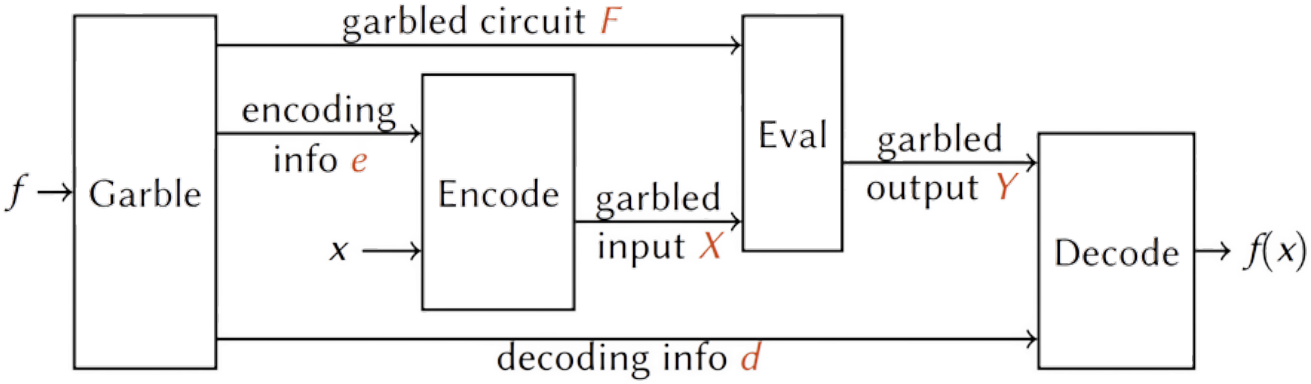

Figure 1: Steps of the SMPC

[1]

[1] 1 was taken from `https://web.engr.oregonstate.edu/~rosulekm/cryptabit/1-overview.pdf`

There are two principles that must be respected[1]:

- *privacy*: nothing is learned from the protocol other than the output;
- *correctness*: the output is distributed according to the prescribed functionality.

The request was to implement a program for which two user can sum up their set of values without sharing them with the opposing party; in this case we decided to create a 8-bit adder circuit. The circuit uses 7 full adders, 1 half adder and 1 if-then-else, represented in figures 2 3 4, concatenated together; the implementation of the entire circuit is represented in figure 5.

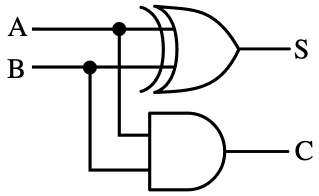

Figure 2: Half Adder

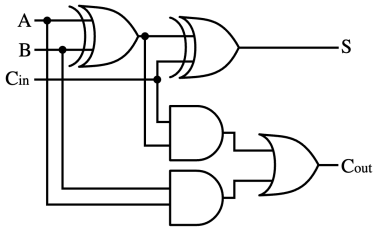

Figure 3: Full Adder

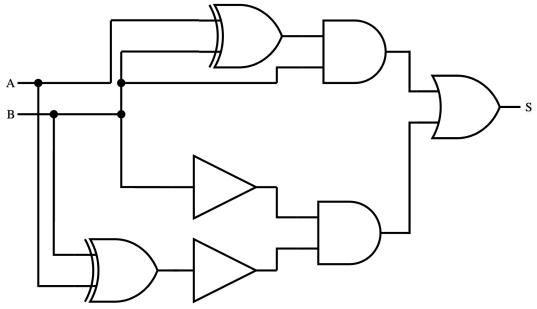

Figure 4: If then else

Full details of my implementation can be found at `https://github.com/lorenzozanolin/garbledCircuit`.

3 Real word application

Secure multiparty computation protocols permit to compliantly, securely, and privately compute on distributed data without ever exposing or moving it. It permits parties to collaborate without compromising sensitive information to each other or third parties,

Image 2 was taken from `https://upload.wikimedia.org/wikipedia/commons/1/14/Half-adder.svg` Image 3 was taken from `https://upload.wikimedia.org/wikipedia/commons/a/a9/Full-adder.svg`.

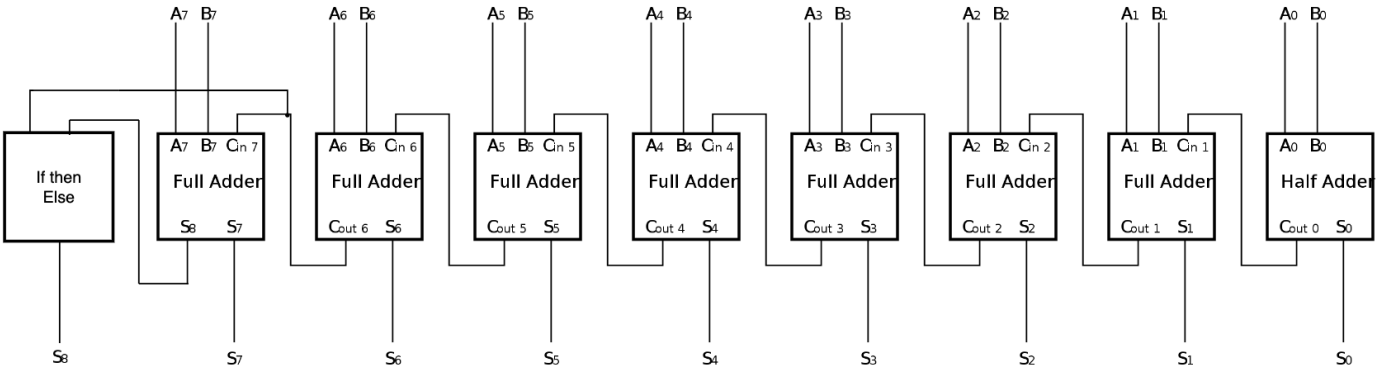

Figure 5: 8-bit Adder

enhancing trust and minimizing the episodes of data breaches. An important field where privacy is crucial is *healtcare*. Medical institutions frequently require access to patient data from other healthcare providers to provide better patient care; this informations must be kept private. SMPC is useful because it allows to perform a joint function, such as a *statistical analysis*, on patient data while keeping it private.

3.1 Average salary calculator

In the *sum* case, an example could be the following: imagine you are an employee in a corporation and you want to know the average salary without revealing to anyone your income. In this scenario you can the use the *SMPC* protocol to get everyone's data and compute the sum; then you can proceede by calculating the mean. In this example no one can understand values of other employees, thus *privacy* is respected.

4 Ethical, Legal and Social aspects

5 Final considerations

References

[1] Yehuda Lindell and Benny Pinkas. A proof of security of yao's protocol for two-party computation. *Journal of Cryptology*, 22, 2009.

[2] Moni Naor and Benny Pinkas. Computationally secure oblivious transfer. *Journal of Cryptology*, 18, 2005.

[3] Andrew C. Yao. Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 160–164, 1982.