Project documentation

Lorenzo Zanolin

May 10, 2023

1 Introduction

The aim of this project is the study of Yao's protocol [2] and an useful application of it. More precisely, we will implement Secure multi-party computation; this field has the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private [1]. In this project, the function we decided to implement is the *8 bit sum*.

1.1 Description of the circuit

We will present briefly the 8-bit sum circuit. There are two basic components in this construction:

- *Half Adder*: used to sum the right-most digit;
- *Full adder*: used to sum a generic digit in the number, ranging from position 1 to 8. It receives in input also carry of the previous sum.

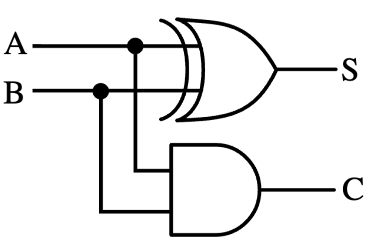

Figure 1: Half Adder

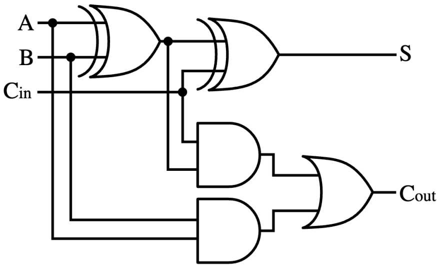

Figure 2: Full Adder

[1]

We then proceede creating the circuit by wiring 7 full adders and an half adder together, as represented in Figure 3.

[1] 1 was taken over https://upload.wikimedia.org/wikipedia/commons/1/14/Half-adder.svg
2 was taken over https://upload.wikimedia.org/wikipedia/commons/a/a9/Full-adder.svg.

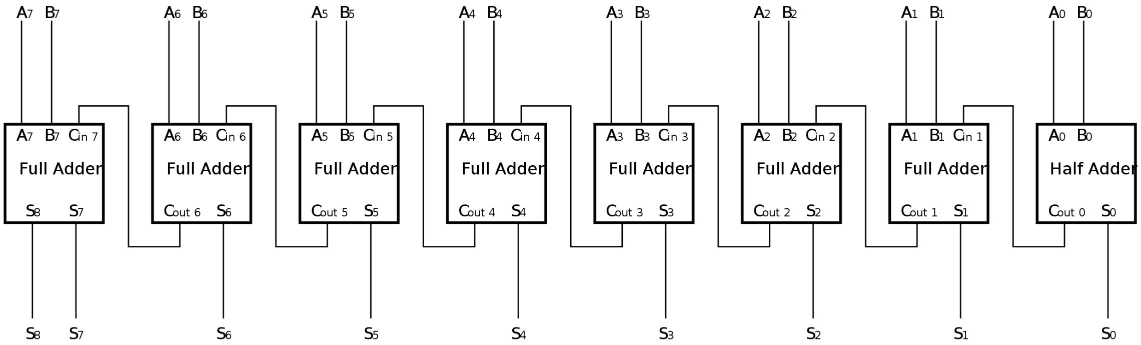

Figure 3: Full Adder

1.2 Implementation

The project will be developed using *Python 3.9.10* and we will use functions provided in the GitHub repo `https://github.com/ojroques/garbled-circuit`.

1.2.1 Project structure

The project is structured as follows:

```
src/.
 ├── Makefile
 ├── images                        This directory contains the images used.
 │    ├── 8-bit_full_adder.png
 │    ├── Circuit.png
 │    ├── Half_adder.png
 │    └── Full-adder.png
 ├── circuits                      This directory contains the circuit used.
 │    └── add.json
 ├── code
 │    ├── util.py
 │    ├── yao.py
 │    ├── ot.py
 │    ├── requirements.py
 │    └── main.py
 └── sets
      ├── alice.txt
      └── bob.txt
```

References

[1] Wikipedia contributors. Secure multi-party computation — Wikipedia, the free

encyclopedia, 2023. [Online; accessed 10-May-2023].

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