Project documentation

Lorenzo Zanolin

May 10, 2023

1 First section

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*.

2 Second section

This is the content of the second section. This section contains the algorithms of my implementation

Data: this text
Result: how to write algorithm with LaTeX2e
initialization;
while *While condition* **do**
    instructions;
    if *condition* **then**
        instructions1;
        instructions2;
    else
        instructions3;
    end
end
for $i \leftarrow 0$ **to** 8 **by** 2 **do**
    Do something
end

Algorithm 1: How to write algorithms

2.1 A subsection

A subsection is created to organise some information togather within a section. This includes the example of how to include a figure. This shows how we refer to algorithm 1.

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.