Mathematical Construction and Optimization of Zero Knowledge Proofs (ZKPs) and Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs)

Alyssa Brittany Chen

Dec. 18, 2023

Contents

1 Introduction

1.1 Abstract

What defines what constitutes a mathematical proof in the simplest manner? In its essense, a proof is a rigorous way to validate a proposition is true. Similarly, Zero Knowledge Proofs (ZKPs) are a way of validating something is true, without revealing the specificities. To illustrate with a simple example, consider the case of Bob and Alice trying to determine which person is richer without revealing their individual salaries.

2 The Construction of a Proof

In the context of ZKPs, there exists some prover, who tries to prove the statement is true to some verifier. This protocol consists of the following properties:

1. Completeness
2. Soundness
3. Zero-Knowledge

2.1 Properties of ZKPs

2.2 Computation

3 Non-Interactivity

4 Succinctness

References

[A] Maksym Petkus. Why and How zk-SNARK Works: Definitive Explanation

A Appendix