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- the prover is able to convince the verifier of the statement's validity.
2. Soundness- a malicious prover is not able to prove to a verifier a false statement.
3. Zero-Knowledge- only the statement's validity is revealed.

Furthermore, a polynomial satisfies the following structure:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

where each a_n term corresponds to the n^{th} term-ed coefficient. A property of polynomials states that for two any arbitrary polynomials with degree at most d, it must intersect at at most d points.

2.1 Computation

For example, if we wish to prove a degree 3 polynomial with roots at $x = 1$ and $x = 2$, the Fundamental Theorem of Algebra allows us to write the polynomial as a product of linear terms. For example:

$$(x - 0)(x - 1)(x - 2) = x^3 - 3x^2 + 2$$

Therefore, the terms $(x - 1)$ and $(x - 2)$ are cofactors of the polynomial. In order to prove the polynomial $p(x)$ indeed has roots at 1 and 2 without disclosing the roots themselves, the prover must prove that $p(x) = t(x) \cdot h(x)$, where $t(x)$ corresponds to the target polynomial $t(x) = (x - 1)(x - 2)$ and $h(x)$ is some arbitrary polynomial.

2.2 Properties of ZKPs

2.3 The Role of Elliptic Curve Pairings

3 Succinctness & Non-Interactivity

3.1 Complexities of Achieving Succinctness and Non-Interactivity

4 zk-SNARKs in DeFi

4.1 Practical Challenges and Solutions in Implementation

References

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

A Appendix