https://quangvdao.github.io/ZKLib https://github.com/quangvdao/ZKLib https://quangvdao.github.io/ZKLib/docs

Formally Verified Cryptographic Proof Systems in Lean

Quang Dao Devon Tuma Gregor Mitscha-Baude

October 14, 2024

Chapter 1

Introduction

The goal of this project is to formalize Succinct Non-Interactive Arguments of Knowledge (SNARKs) in Lean. Our focus is on SNARKs based on Interactive Oracle Proofs (IOPs). We plan to build a general framework for IOP-based SNARKs that can state specifications of the protocols and prove their security properties in a clean and modular way.

Chapter 2

Interactive Oracle Reductions

2.1 Definitions

2.2 Composition

Chapter 3

Oracle Commitment Schemes

3.1 Definitions

3.2 Composition

Chapter 4

Proof Systems

4.1 The Sum-Check Protocol

4.2 The Spartan Protocol

4.3 The Ligero Polynomial Commitment Scheme

Chapter 5

Supporting Results

5.1 Polynomials

5.2 Coding Theory

Chapter 6

References