

# 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

# Oracle Reductions

### 2.1 Definitions

**Definition 1** (Interactive Protocol). An  $n$ -round *interactive protocol* between two parties  $P, V$  is a sequence of messages  $c_0, m_0, \dots, c_n, m_n$  where:

- $c_i$  is a challenge sent by  $V$  to  $P$  in the  $i$ -th round.
- $m_i$  is a message sent by  $P$  to  $V$  in the  $i$ -th round.

Each message  $m_i$  and challenge  $c_i$  may be of different types. We bundle them all together as a `ProtocolSpec` structure.

**Definition 2** (Oracle Reduction). An (*interactive*) *oracle reduction* is an interactive protocol with a prover and a verifier.

**Definition 3** (Completeness).

### 2.2 Composition

## Chapter 3

# 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 Liger Polynomial Commitment Scheme

## Chapter 5

# Supporting Results

### 5.1 Polynomials

### 5.2 Coding Theory

## Chapter 6

## References