

Formally Verified Cryptographic Proof Systems in Lean

Quang Dao

Devon Tuma

Gregor Mitscha-Baude

October 26, 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 (Type Signature of an Interactive Protocol).

Definition 2 (Type Signature of a Prover).

Definition 3 (Type Signature of a Verifier).

Definition 4 (Type Signature of an Oracle Verifier).

Definition 5 (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 6 (Interactive Oracle Protocol). An (*interactive*) *oracle reduction* is an interactive protocol with a prover and a verifier.

Definition 7 (Completeness).

Definition 8 (Soundness).

2.2 Composition

We define *sequential* composition of two or more interactive protocols.

Definition 9 (Composition of Two Protocol Type Signatures).

Definition 10 (Composition of Two Provers).

Definition 11 (Composition of Two Verifiers).

Definition 12 (Composition of Two Oracle Verifiers).

Definition 13 (Composition of Two Interactive Protocols).

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 Ligerio Polynomial Commitment Scheme

Chapter 5

Supporting Results

5.1 Polynomials

Definition 14 (Multilinear Extension).

Theorem 15 (Multilinear Extension is Unique).

5.2 Coding Theory

Definition 16 (Code Distance).

Definition 17 (Distance from a Code).

Definition 18 (Generator Matrix).

Definition 19 (Parity Check Matrix).

Definition 20 (Interleaved Code).

Definition 21 (Reed-Solomon Code).

Definition 22 (Proximity Measure).

Definition 23 (Proximity Gap).

Chapter 6

References