Applied ZKP Workshop #1

Shumo Chu

Credit: partially based on slides from Brain Gu (0xparc)

P0XEIDON LABS

About This Workshop

Goals

- Understanding concepts related to ZKP dev practice
- Learn how to use Circom to build a ZKP Circuit
- Learn the toolchain around Circom
- Learn how to build a zkDApp on Ethereum
- Learn the best practice in ZKP Security

Non-Goals

- Become a ZKP cryptographer

What is ZKP?

- Zero-knowledge proof is **encryption on computation** (Silvio Micali)
  - Cryptographic proof of the correctness (or validity) of computation
  - This proof doesn’t leak any information
- 3 element of a ZKP scheme
  - **Circuit**: description of computation, a.k.a statement
  - **Prover**: who generates zero-knowledge proof
  - **Verifier**: who verifies zero-knowledge proof

Example Circuits Used in Blockchain

- “*I know the private key that corresponds to this public key*”
- “*I know a private key that corresponds to a commitment which is a leaf of a merkle tree root*” MantaPay, ZCash
- “*I know the preimage of this hash value*”

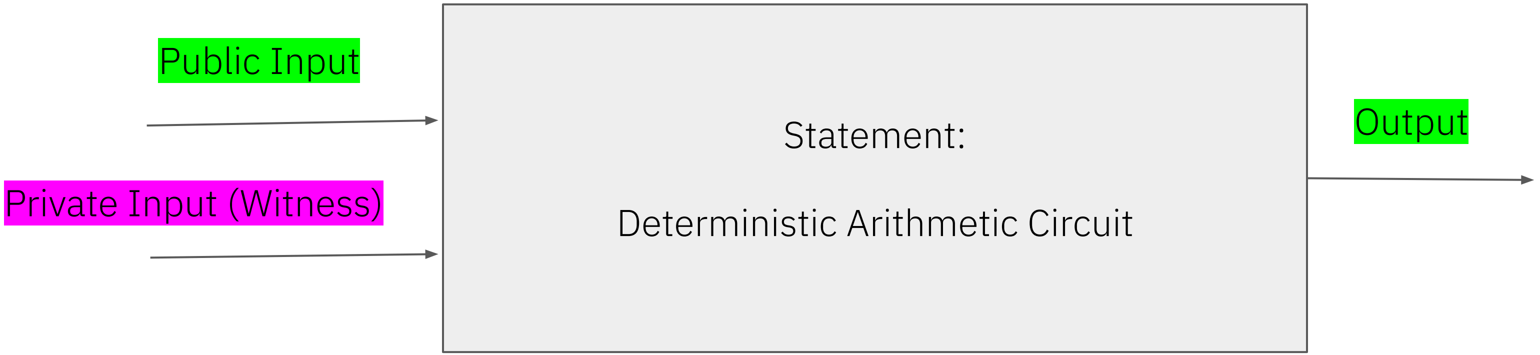
What is the common pattern?

Design Pattern of Circuits

- *"I know the private key that corresponds to this public key"*
- *"I know a private key that corresponds to a commitment which is a leaf of a merkle tree root"* MantaPay, ZCash
- *"I know the preimage of this hash value"*

Proving private knowledge against public facts.

Arithmetic Circuits Satisfaction



Public Input

Private Input (Witness)

Statement:

Deterministic Arithmetic Circuit

Output

Finite Field of Circuits

- Fp: Finite Field that the computation that the arithmetic circuit represents in on
- Groth 16 on Pairing Friendly Curves
  - Embedded curve: BabyJubjub
  - Ethereum native curve: BN254
- Two operations: × and + (modulo p)
- p (BabyJubjub) = 21888242871839275222246405745257275088548364400416034343698204186575808495617 (~2^254)

(https://learn.0xparc.org/materials/circom/prereq-materials/prereq-understanding/)

Arithmetic Circuits Representation

R1CS → QAP

Details ignored now, key point is Groth16 only support Quadratic Constraints System, i.e:

A * B - C = 0