Circuit optimization

Daira Hopwood

@feministPLT
daira@z.cash

Zcon0, Montreal, 27 June 2018

Content of this talk

- Layering of a proof system
- How to design statements
  - securely
  - efficiently
- Quadratic Constraint Programs
  - What are they?
  - How to optimize them
  - Using nondeterminism

Layering of a proof system

- Statements
- What are you trying to prove?
  - For given x, I know a witness w, such that P(x, w).
- Always use types
  - For given x : X, I know a witness w : W, such that P(x, w).
- Examples
  - For given h : Byte[32], I know w : Byte[64], such that BLAKE2s("Zcon0_ex", w) = h.
  - For given Merkle tree root rt : Hash, I know a path in the tree (path : Hash[Depth], pos : Nat) such that the leaf commits to m : M.
  - For given pk : Point, I know sk : Scalar such that [sk] G = pk.

How is a statement expressed?

- Many things to choose: proving system, pairing curve, …
- In this talk, we only consider proving systems that support "R1CS".
- Most parameters of the proving system, although they affect performance, don't interact with R1CS optimization.
- Exception: the finite field over which the R1CS is defined.
  - I'll call this field F.

Content of this talk

- Layering of a proof system
- How to design statements
  - securely
  - efficiently
- Quadratic Constraint Programs
  - What are they?
  - How to optimize them
  - Using nondeterminism

Content of this talk

- Layering of a proof system
- How to design statements
  - securely
  - efficiently
- Quadratic Constraint Programs
  - What are they?
  - How to optimize them
  - Using nondeterminism