Proof of Achievement

Modules for basic types and their opertations

Our language now supports some basic types such as `Bool`, `ByteString`, `UInt`, and `UTCTime`. These types and their operations can now be handled by our compiler that produces proper arithmetic circuits for computations invlolving those types. Modules:

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/Bool.hs

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/ByteString.hs

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/UInt.hs

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/UTCTime.hs

Modules for equality and comparison checks

These modules enable compilation of equality and comparison tests. Modules:

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/Eq.hs

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/Ord.hs

Implementation of branching computations

These modules enable branching computations in ZK programs:

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Data/Conditional.hs

https://github.com/zkFold/zkfold-base/blob/main/src/ZkFold/Symbolic/Compiler/ArithmeticCircuit/Instance.hs

Implementation of SHA2 and MiMC hash functions

We now have SHA2 and MiMC hashes that one can use in ZK programs:

https://github.com/zkFold/zkfold-base/blob/vks4git_hash/src/ZkFold/Symbolic/Algorithms/Hash/SHA2.hs

https://github.com/zkFold/zkfold-base/blob/vks4git_hash/src/ZkFold/Symbolic/Algorithms/Hash/MiMC.hs