

# Zero Knowledge Compilers

John McCall

Division of Science and Mathematics  
University of Minnesota, Morris  
Morris, Minnesota, USA

November 13, 2013

# Overview

# Interactive Proof

Must satisfy:

- *Completeness*: For every  $x \in S$ , the verifier always accepts after interacting with the prover on common input  $x$ .
- *Soundness*: For every  $x \notin S$ , the verifier rejects with probability at least  $\frac{1}{p(|x|)}$ .

# Zero Knowledge Proof

# Magic Cave

# Hamiltonian Cycle

# Compilers

# Sigma-Protocols



# ZKCrypt

# ZKPDL

# Electronic Cash

# Final Thoughts

# Acknowledgments

# Questions