Zero Knowledge Proofs

05-03-2025: MATH408 Draft 1

Trevor Nichols

Abstract

The concept of zero knowledge proofs (ZKPs) has gained significant attention in recent years due to its potential applications in cryptography, privacy-preserving systems, and secure multiparty computation.

The idea behind ZKPs is to provide a method for proving the truth of a statement without revealing any additional information about the statement itself. This process typically involves two parties, called prover and verifier, engaging in a series of communication steps. This communication can be two way, as long as the verifier cannot learn anything other than the truth of the statement. Some ZKPs cannot mathematically prove the truth of a statement, but can be significantly statistically proven.

Brief

Development

References

- https://decrypt.co/resources/zero-knowledge-proofs-explained-learn-guide
- https://crypto.stanford.edu/pbc/notes/crypto/zk.html
- https://zkp.science/
- https://ethereum.org/en/zero-knowledge-proofs/
- https://www.cs.princeton.edu/courses/archive/fall07/cos433/lec15.pdf