

Zero-Knowledge Proofs

Goal: Peggy (prover) wants to convince Victor (verifier) of something

Convincing If true, an honest prover can always convince an honest verifier

No cheating If false, a dishonest prover can only rarely convince an honest verifier

Zero knowledge If true, a cheating verifier cannot learn anything more than that it is true.