Zero Knowledge Proofs

Zero Knowledge Proofs (ZKP) are instances of interactive proof systems. They allow a Verifier to be convinced of a piece of information held by a Prover without the Prover exposing the piece of information itself.

ZKPs are used to create Identification and Authentication Protocols that are used in real-world situations. The idea is that in a ZKP, the Prover sends *commitments*, then the Verifier sends a *challenge* to which the Prover must respond; the mathematics involved ensure that a fake Prover would not be able to respond correctly to all possible challenge values; the zero-knowledge property ensures that any cheating verifier learns nothing about the proof system. This also ensures that cheating verifiers cannot impersonate as a Prover to a third party.

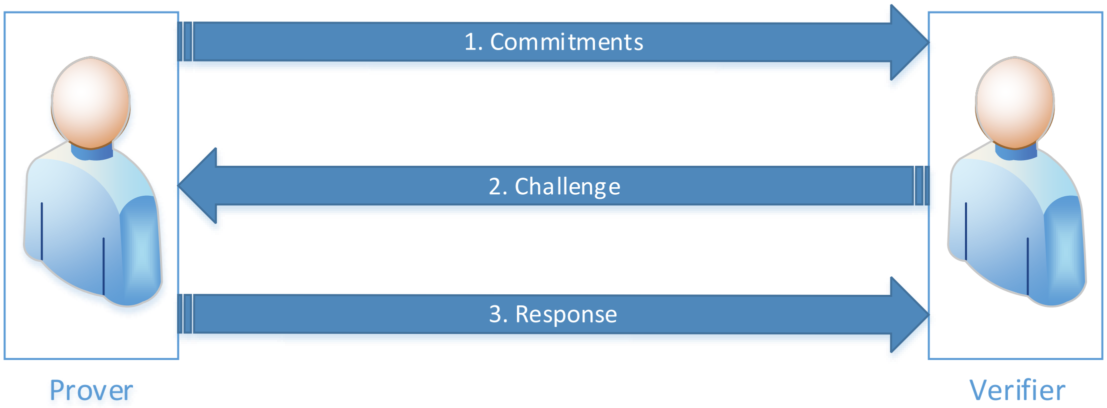

Fig: An Interactive Proof System

It is generally possible to turn any ZKP into an equivalent signature scheme. The Schnorr Signature scheme is an example – The Digital Signature Algorithm (DSA) is derived from it. It is used extensively for secure communication – specifically in the TLS protocol.

Rounak Das, BCSE-IV

Roll: 0012105010**36**