Aim: Login using password

Approach:

Since logging in using password is the aim, the algorithm should be non-interactive. The prover should not be required to send multiple messages to the verifier.

Non-interactive ZKP

Non-interactive zero-knowledge proofs are zero-knowledge proofs where information between a prover and a verifier can be authenticated by the prover, without revealing any of the specific information beyond the validity of the transaction itself. This function of encryption makes direct communication between the prover and verifier unnecessary, effectively removing any intermediaries. The core trustless cryptography "proofing" involves a hash function generation of a random number, constrained within mathematical parameters (primarily to modulate hashing difficulties) determined by the prover and verifier.

Non-interactive ZKP wiki

Elliptic Curve Based ZKP

Aim:

Given an elliptic curve E over a field Fn, a generator point G âˆˆ E/Fn and B âˆˆ E/Fn Prover wants to prove that he knows x such that B = xÂ·G, without revealing x.

Mathematical Explanation

â€¢ Prover generates random r âˆˆ Fn and computes the point A = r Â· G â€¢ Prover sends the point A to Verifier

â€¢ Verifier flips a coin and informs the Prover about the outcome

â€¢ In case of HEADS Prover sends r to Verifier who checks that r Â· G = A

â€¢ In case of TAILS Prover sends m = x + r(mod n) to Verifier who checks that m Â· G = (x + r) Â· G = x Â· G + r Â· G = A + B

Research paper on elliptical curve based zkp