Zero Knowledge Protocol

AK Bhateja

Zero-knowledge proof or zero-knowledge protocol (ZKP)

- It is a method by which one party (the prover) can prove to another party (the verifier) that they know the secret, without conveying any information apart from the fact that they know the secret.
- ZKP must satisfy three properties
  - Completeness: If the statement is true, the honest verifier will be convinced by honest prover.
  - Soundness: If the statement is false, the verifier would not be convinced, except with some small probability.
  - If the statement is true no cheating verifier learns anything other than this fact.

Fiat Shamir Identification Protocol

- It is a 3 message Protocol
- Alice A, the prover and Bob B, the verifier
- A trusted third party chooses two large prime numbers p and q to calculate $n = p \times q$.
- The value of n is made public, while p and q are kept secret.
- The prover A chooses a secret x between 1 and n-1, coprime to n.
- A then calculates $v = x^2 \ mod \ n$ and registers it publically.

Fiat Shamir Identification Protocol verification of the secret by B

Alice A		Bob B
Choose $r \in [0, n\text{-}1]$		
Compute $h = r^2 \ mod \ n$	$h \longrightarrow$	h
		Randomly choose $b \in \{0, 1\}$
b	$\longleftarrow b$	
Find $s = r.x^b \ mod \ n$	$s \longrightarrow$	s
		calculate $s^2 \ mod \ n$ and $h.v^b \ mod \ n$ Is $s^2 \equiv h.v^b \ mod \ n$

Fiat Shamir Protocol (continued)

- B accepts the response if $s^2 \ mod \ n$ and $h.v^b \ mod \ n$ are congruent.
- If the two values are congruent then B assumes
  - either A has the secret
  - or A has calculated the value of *s* by some other method.
- Justification of working of this protocol

$$h.v^b \ mod \ n \equiv (r^2 \ mod \ n)(x^2 \ mod \ n)^b$$

$$\equiv (r^2 mod \ n)\left(x^{2b} mod \ n\right)$$

$$\equiv \ r^2.x^{2b} \ mod \ n \equiv s^2 \ mod \ n$$

Fiat Shamir Protocol (continued)

- The verification is repeated several times with the value of *b* equal to 0 or 1 (chosen randomly).
- A must pass the test in each round to be verified.
- If A fails one single round, the process is aborted and A is not authenticated.
- A can be honest if A knows the secret *x* and passes all the rounds successfully, and can be dishonest if A does not know the secret *x* but can still clear the rounds by predicting the secret.

Case 1: If A is honest

- If B sends the challenge $b = 1$ then

$$h.v^b \ mod \ n \equiv (r^2 \ mod \ n)(x^2 \ mod \ n)$$
$$\equiv (r.x)^2 \ mod \ n$$
$$\equiv s^2 \ mod \ n$$

Therefore, prover cannot cheat the verifier.

- If B sends the challenge $b = 0$ then

$$h.v^b \ mod \ n \equiv (r^2 \ mod \ n)$$
$$\equiv s^2 \ mod \ n$$

Thus, prover can cheat because without knowing x, prover can prove that she has the secret.

Case 2: If A is not honest, then A can cheat using the following protocol

- Prover A chooses a random number *r* between 0 and *n*-1.
- A calculates $h = r^2 v^{-1} \; mod \; n$ and transmits it to the verifier B
- B sends a challenge *b* either 0 or 1 to A.
- A send $s = r$ to B.
- B calculates $s^2 \; mod \; n$ and $h.v^b \; mod \; n$ and checks if the two values are congruent. If the two values are congruent then B assumes that either A has the secret or A has calculated the value of *s* by some other method

- If $b = 1$ then, $h.v^b \; mod \; n \equiv (r^2 v^{-1} \; mod \; n)(v \; mod \; n)$
$$\equiv (r^2 mod \; n) \equiv s^2 \; mod \; n$$
- $b = 0$ then, $h.v^b \; mod \; n \equiv (r^2 v^{-1} \; mod \; n) \neq s^2 \; mod \; n$

Probability of Authentication

- The dishonest claimant has a maximum 50% chance of fooling the verifier and passing the test.
- If the process is repeated *r* times with random choices of *b*, then the minimum probability for the authentication of the prover is $1- (½)^r$.

Zero knowledge proof for discrete log

- Let p be a large prime, g be the generator of the cyclic group Z_p^*.
- Discrete log of $v \in Z_p^*$ with base g over Z_p^* is x s.t. $v = g^x \bmod p$.
- Here x is the secret. v, p and g are public.
- Zero knowledge protocol
  - Prover A chooses a random number r between 0 and p-1.
  - A calculates $h = g^r \, mod \, p$ and transmits it to the verifier B
  - B sends a challenge b either 0 or 1 to A.
  - A calculates s by the formula $s = (r + bx) mod (p - 1)$ and transmits the value of s to B.
  - B calculates $hv^b \, mod \, p$ and $g^s \, mod \, p$ and checks if the two values are congruent. If the two values are congruent then B assumes that either A has the secret or A has calculated the value of s by some other method.

Zero knowledge proof for discrete log

- The verification is repeated several times with the value of b equal to 0 or 1 (chosen randomly).
- A must pass the test in each round to be verified.
- If A fails one single round, the process is aborted and A is not authenticated.

Case 1: If A is honest

- If B sends the challenge $b = 1$ then

$$h.v^b \ mod \ p \equiv hv \ mod \ p$$

$$\equiv (g^r mod \ p)(g^x \ mod \ p) \equiv g^s \ mod \ p$$

Therefore, prover cannot cheat the verifier.

- If B sends the challenge $b = 0$ then

$$h.v^b \ mod \ p \equiv (h \ mod \ p)$$

$$\equiv (g^r mod \ p) \equiv g^s \ mod \ p$$

Therefore, prover can cheat because without knowing x, prover can prove that he has the secret.

Case 2: If A is not honest, then A can cheat using the following protocol:

- Prover A chooses a random number r between 0 and p-1.
- A calculates $h = g^r v^{-1} \, mod \, p$ and transmits it to the verifier B
- B sends a challenge b either 0 or 1 to A.
- A sends $s = r$ to B.
- B calculates $g^s \, mod \, p$ and $h.v^b \, mod \, p$ and checks if the two values are congruent. If the two values are congruent then B assumes that either A has the secret or A has calculated the value of s by some other method.

- If B sends the challenge bit $b = 1$ then

$$h.v^b \, mod \, p \equiv (hv \, mod \, p)$$
$$\equiv (g^r v^{-1})(v \, mod \, p) \equiv g^s \, mod \, p$$

- If B sends the challenge bit $b = 0$ then

$$h.v^b \, mod \, p \equiv h \, mod \, p \equiv (g^r v^{-1} \, mod \, p)$$
$$\equiv (g^s v^{-1} \, mod \, p) \neq g^s \, mod \, p$$

Probability of Authentication

- The dishonest claimant has a maximum 50% chance of fooling the verifier and passing the test.
- If the process is repeated *r* times then the minimum probability for the authentication of the prover is $1 - (½)^r$.

Applications

- Zero Knowledge proofs can be applied where secret knowledge too sensitive to reveal needs to be verified
- Key authentication
- PIN numbers
- Smart Cards