# Zero Knowledge Protocol

Akash Patel (SJSU)

# Zero Knowledge Protocol

- Zero knowledge proof or protocol is method in which a party A can prove that given statement X is certainly true to party B without revealing any additional information [1].

- Lets say Alice and Bob want to communicate over shared network. Alice initiate the communication and sends secret to Bob. Bob verifies the secret so he can be certain that he is communicating with Alice. Once he verifies the secret ,he sends conformation.

- In the above scenario, Bob must know Alice's secret so he can verify Alice's identity but now Bob can impersonate Alice.

- Zero knowledge protocol allow Alice to prove Bob that she knows the secret without revealing the secret.

- In this protocol ,verification is performed for many executions and each time Alice need s to pass the verification.

# Zero Knowledge Protocol[4]

- Zero knowledge protocol is 3 pass identification protocol. First message is Commitment or witness sent from Alice to Bob, a second message is challenge sent from Bob to Alice and a final message is response sent from Alice to Bob .

- Zero knowledge protocol must have three properties.
  1. Completeness: If the statement is true, the honest verifier will be convinced by honest prover.
  2. Soundness: If the statement is false, Trudy can not convince the verifier that it is true , except with some small probability.
  3. Zero-knowledge: If the statement is true no cheating verifier learns anything other than this fact.

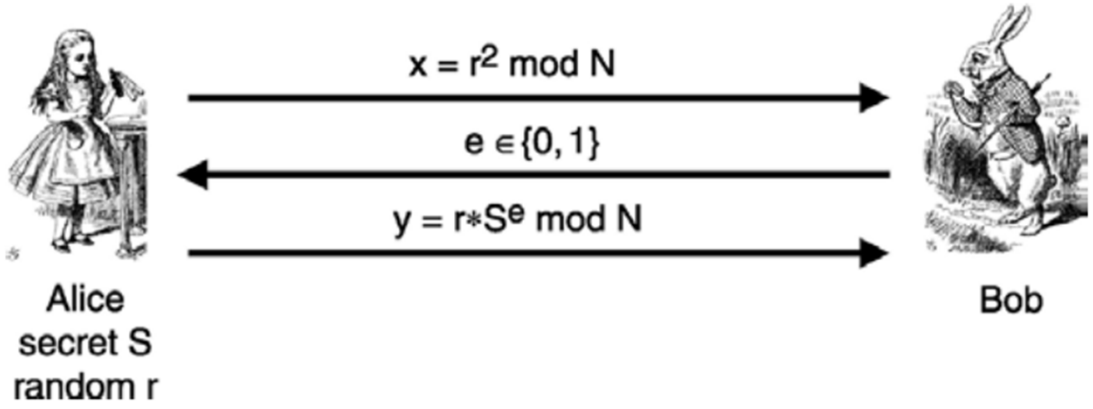
- Randomness is also an important property of Zero knowledge protocol.

- Randomness in the commitment and challenge message are use to hide the secret information.

# Fiat-Shamir Protocol[4]

- Goal of  protocol is to prove Alice knows secret s in n executions.
- This is probabilistic protocol with probability of $2^{-n}$ for adversary to fool the verifier.
- Usually the number of executions are around 20 to 40

# How Fiat-Shamir Protocol works?[2]




**One time Set up:**

1. In this protocol, Trusted center selects RSA like modulus N = p* q , where p and q are secret prime number and N is public.
2. Alice select secret S such that S is coprime to N and 1<=S<=N-1, computes $V = S^2 \bmod N$. S is private and V is public.

**Protocol:**

1. Alice select random number r and sends $x = r^2 \bmod N$ to Bob.
2. Bob sends either 0 or 1 to Alice.
3. Alice sends $y = r * S^e \bmod N$ to Bob.

**Verification:**

1. Bob verifies it with $y^2 = x * v^e \bmod N$.

# Why randomness is necessary?[2]

- Bob might request Alice to perform the experiment as many times as she desires until she's certain of Alice's authority. Throughout the entire process, Bob will only need to work with the publicly known number x, e, & v and will learn nothing about the secret S.

- In ZK protocol, Random value is used by Alice during commitment phase and used by Bob during challenge phase.

- Lets say Bob does not use random value for e in second message. Bob uses fixed value either 0 or 1.

- Case 1: e = 0 . Trudy send x = r2 mod N in the first message and y = r mod N in the third message so she followed the protocol and convince the Bob she knows the secret
- Case 2: e = 1. Trudy will send $x = r^2v^{-1} \bmod N$ in the first message and y = r mod N in the third message. Bob tries to calculate $y^2=r^2$ and $xv^e = r^2v^{-1}v = r^2$ and Bob convince that Trudy knows the secret

- So it is necessary for Bob to chose random value for e. Trudy can only fool Bob with probability ½ and, as with Bob's Cave, after *n* iterations, the probability that Trudy can fool Bob is only ( $1/2^n$ ).

# Why Alice needs to chose the random value?[2]

- Alice also needs to chose random value for r at each iteration. Suppose Alice uses same value for each iteration.
- Lets say Bob sends e = 0 and Alice sends r mod N in third message
- Now Bob sends e = 1, Alice sends r*S mode N
- Trudy records entire communication and she knows r mod N and r*S mod N
- It is very easy for Trudy to find the value of S from r mod N and r*s mod N
- So it is necessary for Alice to select random value for r at each iteration.

# Does it really Zero Knowledge?[2]

- Let s say Bob wants to learn about Alice's secret.
- In $V = S^2 \bmod N$ , V and N are public.
- Bob gets $r^2 \bmod N$ in message 1.
- If e = 1 Bob receive: r*S mod N.
- If Bob can find r from $r^2 \bmod N$ then he can find s from r*S mod N.
- We have assumed that finding a modular square root is computationally infeasible.

# Is Zero Knowledge completely anonymous?

- Lets say Bob and Alice wants to communicate.
- Alice does not know Bob's public Key.
- Bob sends his certificate to Alice. Certificate can reveal Bob's identity.
- Trudy can determine Bob is part of any communication.
- It is difficult to maintain anonymity when public keys are used.

# Pros and Con of Zero- knowledge[6]

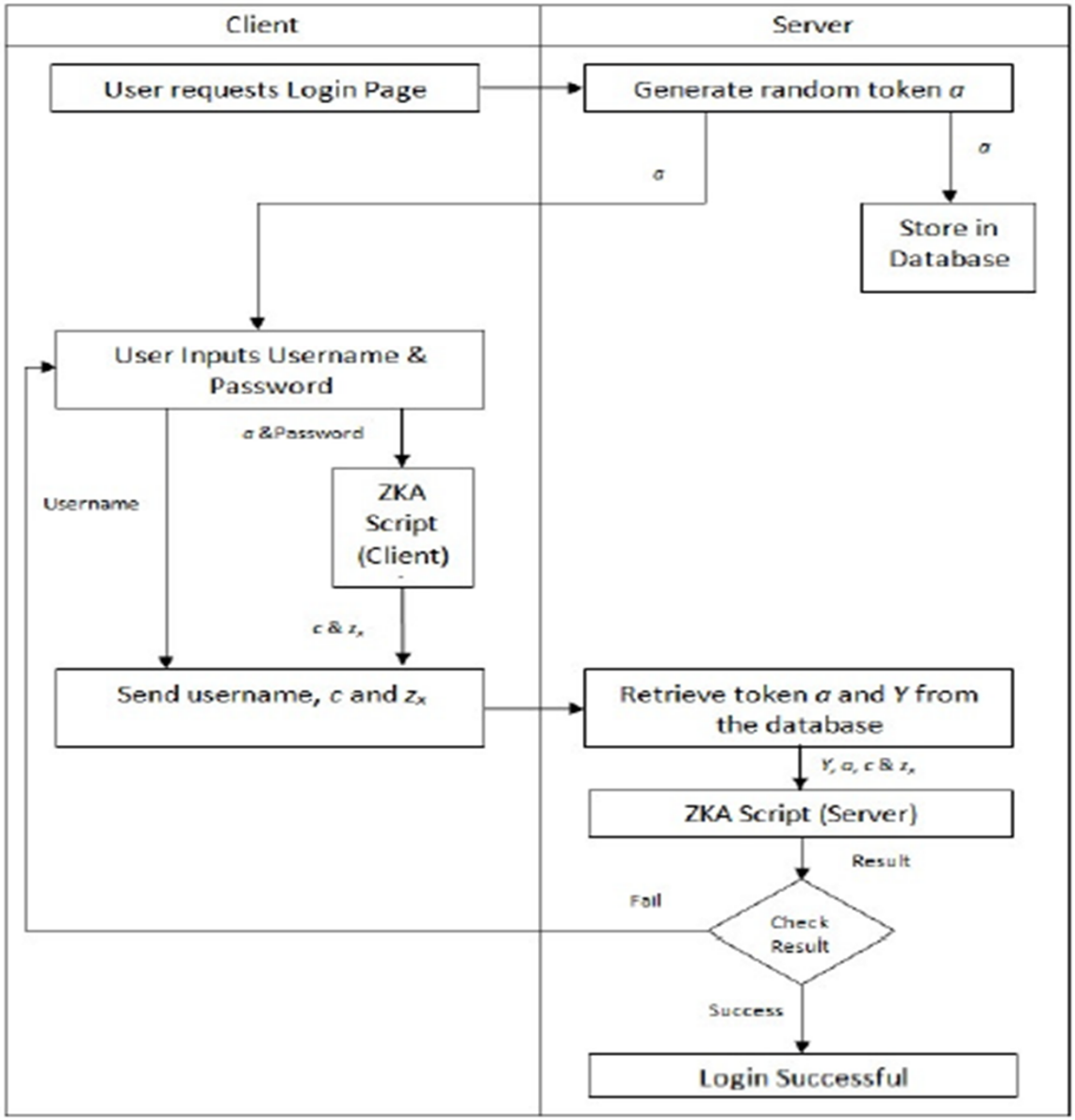
**Pros:**

- Secured – Not requiring the revelation of one's secret.
- Simple – Does not involve complex encryption methods.

**Cons**:

- Limited – Secret must be numerical, otherwise a translation is needed.
- Lengthy – There are 2k computations, each computation requires a certain amount of running time.
- Imperfect – The Malice can still intercept the transmission (i.e. messages to the Verifier or the prover might be modified or destroyed).

# Web Authentication based on ZKP[5]



# Web Authentication based on ZKP[5]

**Authentication Process**

| No | User (Prover) | | Verifier (Server) |
|---|---|---|---|
| 1 | | | Generate random a |
| 2 | Receive a | ← | Send a |
| 3 | | | |
| 4 | Calc. x=H(password) | | |
| 5 | Calculate $Y=g_0^x$ | | |
| 6 | | | |
| 7 | Randomly generate $r_x$ | | |
| 8 | Calculate $T_1=g_0^{rx}$ | | |
| 9 | Calculate $c=H(Y,T_1,a)$ | | |
| 10 | | | |
| 11 | Calculate $z_x=r_x - cx$ | | |
| 12 | Send c, $z_x$ | → | Receive c, $z_x$ |
| 13 | | | Calculate $T_1=Y^c g_0^{zx}$ |
| 14 | | | Check if c= H(Y,T1,a) |

# References

1. http://en.wikipedia.org/wiki/Zero-knowledge_proof

2. Section 9.5 of Information Security Principles and practice by Dr. Mark Stamp ,Published by JohnWiley & Sons, Inc

3. Technical Paper: How to Explain Zero-Knowledge Protocols to Your Children. Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings

4. Technical Paper: Overview of Zero-Knowledge Protocols by Jeffrey Knapp. http://www.cs.rit.edu/~jjk8346/paper.pdf

5. Technical Paper: Implementing Zero-Knowledge Authentication with Zero Knowledge (ZKA_wzk) by Lum Jia Jun, Brandon. http://ojs.pythonpapers.org/index.php/tppm/article/view/155/142

6. Zero knowledge Protocol paper presentation by J. Chu http://jason.mchu.com/ZKP.ppt