IT352: INFORMATION ASSURANCE AND SECURITY

LAB 4 – Fiat Shamir Algorithm

3rd Mar 2021

Submitted by: Harsh Agarwal (181IT117)

Introduction:

One of the most well-known protocols identification using zero knowledge proof protocol is proposed by Amos Fiat and Adi Shamir, whose resistance is based on the difficulty of finding square root modulo a sufficiently large composite number n, the factorization is unknown.

Steps involved in the Algorithm:

1. Select the module sufficiently large number **n = p * q**, factored that difficult. p, q are primes and kept secret

2. Client chooses a **secret s** belonging to interval **(1, n-1)** and relatively prime with n.

3. Public key is then calculated as **V=s^2 mod n**.

4. The resulting v registered as a trust center's public key of Client, and the value of s is the secret of Client. It is the knowledge of this secret s necessary to prove to the Client side without disclosure for t rounds.

5. Each round consists of:

    a. Client chooses a **random r** in the interval **(1, n- 1)** and **sends x = r^2 (mod n) to Server**

    b. Server randomly selects a bit e aka **challenge (c) (0 or 1)** and sends it to Client.

    c. Client computes **y = x*v^e(mod n)** and sends it back to Server.

    d. Server checks the equality **y^2 = x*v^e(mod n)**. If it is true, it proceeds to the next round of the protocol, otherwise the proof is not accepted.