Using the concept of **threshold cryptography** to solve **congestion** in **routing** of **vehicles**

Shaswata Raha

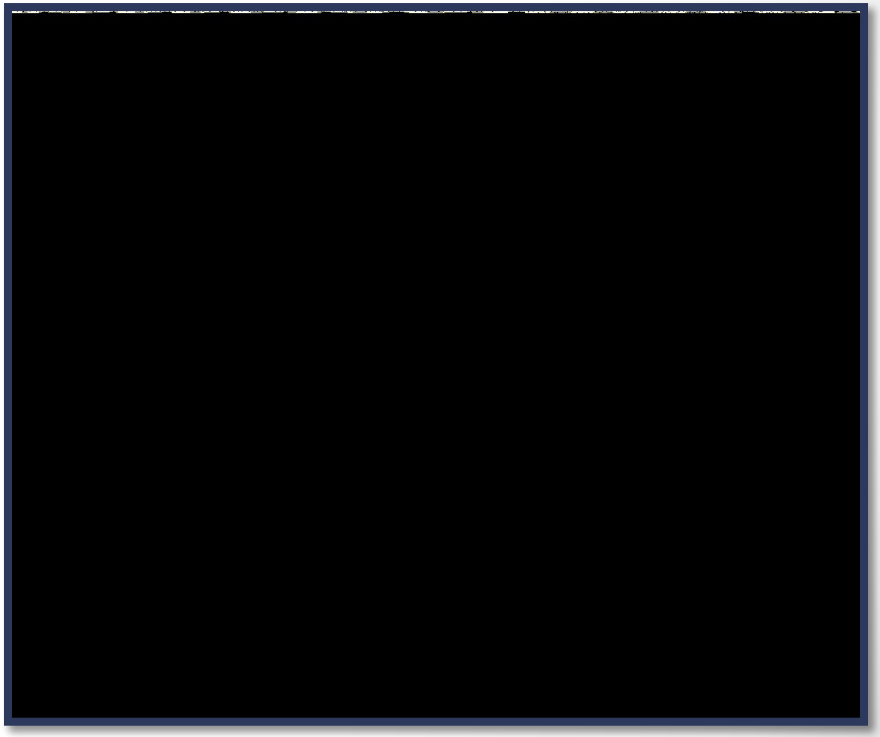
Vikas Patel

Manish Kundu

Threshold Cryptography

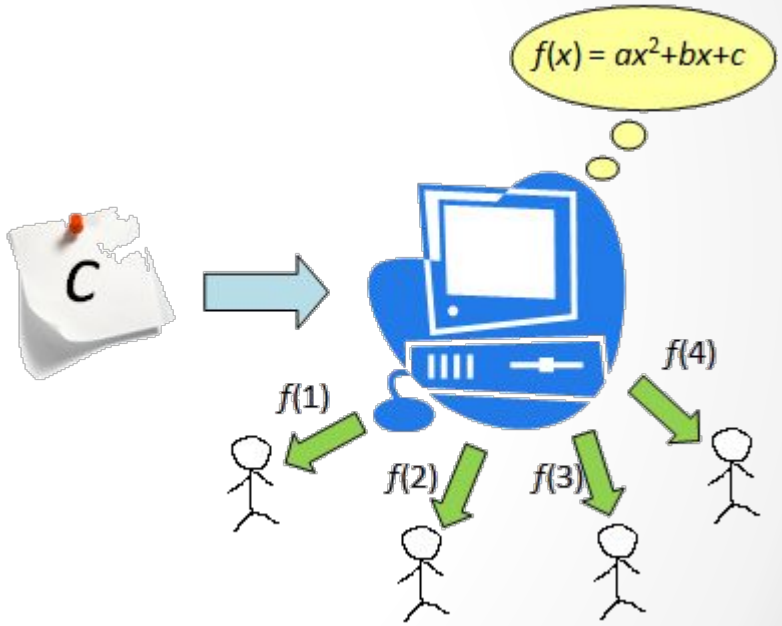
- In threshold cryptography, information is encrypted using a “public key”, and the “private keys” are distributed correspondingly to all clients.

- To decrypt this information, a certain minimum number of clients are needed to co-operate together. Also called the “threshold” amount.



Shamir's Secret Sharing Algorithm

- The simulation uses this algorithm for encryption and decryption.
- The secret is divided into N "shares" and a minimum of K shares are needed to decrypt it.
- The idea is to build a polynomial with the degree (K–1) such that the constant term is the secret code.
- This secret can be found using any K points out of the N generated points (using Lagrange interpolation).



Example:

- Let, secret S = 65, N = 5, K = 2.
- Our polynomial must be of degree K-1 = 1, with constant term being S. Let's say the polynomial is: **y = 15x + 65** .
- Generate N random points: say (1, 80), (2, 95), (3, 110), (5, 140) and (10, 215).

- To generate the secret from any K points, we form the Lagrange identities first and then the sum of these identities gives us the required polynomial.

$$l_i = \frac{x - x_0}{x_i - x_0} \times \ldots \times \frac{x - x_{i-1}}{x_i - x_{i-1}} \times \frac{x - x_{i+1}}{x_i - x_{i+1}} \times \ldots \times \frac{x - x_{k-1}}{x_i - x_{k-1}}$$

$$f(x) = \sum_{i=0}^{K-1} y_i l_i(x)$$

Example (contd.):

- Now say we have the points (1, 80) and (3, 110) and wish to find the secret. Then the steps are:

$$l_0 = \frac{x - x_1}{x_0 - x_1} = \frac{x - 3}{1 - 3}$$

$$l_1 = \frac{x - x_0}{x_1 - x_0} = \frac{x - 1}{3 - 1}$$

$$f(x) = y_0 l_0 + y_1 l_1$$

$$f(x) = 80\left(\frac{x - 3}{-2}\right) + 110\left(\frac{x - 1}{2}\right)$$

$$f(x) = -40x + 120 + 55x - 55$$

$$f(x) = 15x + 65$$

- Hence, with any K points it is possible to obtain the secret.

The simulation

- In the simulation, the vehicles are represented using "nodes".
- Each node initially contains a message, a node number and most importantly, a private key.
- Some of these nodes are "malicious" nodes which we attempt to identify.

- The malicious nodes try to create a fake congestion scenario by sending false messages with the real nodes.
- There is also a traffic light node where we check for any congestion.
- After using Shamir's secret sharing algorithm, we decrypt the message and check if the result matches our original secret key.
- If it does, then the congestion is real and we let the message pass through. Otherwise, the malicious node is detected and the message is blocked.

- This type of attack where the nodes contain various cryptographic keys and the malicious node poses as a real node is called Tampering.

- Thus, with the help of threshold cryptography, we successfully solve the problem of congestion in the routing of vehicles.

Thank you.