STRENGTHENING CRYPTOGRAPHY USING QUANTUM PROPERTIES

A PROJECT DONE BY

1. NAVEEN S R 211418104172 GitHub in
2. PRADEISH C 211418104196 GitHub
3. MOHAN RAJ RISHI S 211418104158

for partial fulfilment for the award of the degree of

BACHELOR OF ENGINEERING in COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

ABSTRACT

For most of the cryptography algorithms, randomness plays a vital role. But generation of pure random number is impossible in classical computer. Even for generating decent random numbers it needed a random seed. But since the seed is a number in source code or algorithm to generate seed which is also in source, it can be revealed to hacker if the system is compromised. Which made possible to predict all the random numbers the computer will generate by the hacker. So, to solve this issue we introduce quantum computer to create a true randomness using its superposition capability.

But quantum machines are not accessible to all the computers, especially to clients. So, we found that it possible to generate a pure random number on client side with the help of quantum computer on server side using Diffie Hellman Key Exchange. Even through un-encrypted channel with any compromise.

To Run

1. Activate Python VirtualEnv

Platform	Shell	Command to activate virtual environment
POSIX	bash/zsh	$ source venv/bin/activate
	fish	$ source venv/bin/activate.fish
	csh/tcsh	$ source venv/bin/activate.csh
Windows	PowerShell Core	$ venv/bin/Activate.ps1
	cmd.exe	> venv\Scripts\activate.bat
	PowerShell	PS > venv\Scripts\Activate.ps1

2. Run server script

```
python server_cli.py
```

```
(venv) ~/nk/mainproj >>> python server_cli.py -h
usage: server_cli.py [-h] [-1 | -2] [-g] [-s] [-p]

options:
  -h, --help  show this help message and exit
  -1          Use qmachine1
  -2          Use qmachine2
  -g          For GUI
  -s          Show Qcircuit
  -p          Plot Qcir result
```

3. Run client script

```
python client_cli.py
```

4. Start messaging from client

```
(venv) ~/nk/mainproj >>> python client_cli.py
Shared Key : b'\x04O\xceT\xfb\xd29'
Message to server : Hi
Response from server : Bye
Message to server : Exit
(venv) ~/nk/mainproj >>>
```

```
(venv) ~/nk/mainproj >>> python server_cli.py
I> Loading Modules ...
I> All Modules Loaded
Job Status: job has successfully run
I> Quantum Code done
Seed : b'\xe1(\xdbK3\\\x10,\x0e\xec\xd2N\x08\x85\xdf'
I> Seeding randomess done
I> Waiting for client to connect ...
client connected from : ('127.0.0.1', 38974)
I> Connected to client
I> Sharing pure randomness ...
Shared Key : b'\x04O\xceT\xfb\xd29'
I> Shared by diffie-hellman
Data from client   : Hi
Response to client : Bye
```

```
I> Socket closed
I> Quiting...
(venv) ~/nk/mainproj >>>
```

Repo

Link : https://github.com/nkpro2000/IVyearProject

To clone

```
git clone https://github.com/nkpro2000/IVyearProject.git
cd IVyearProject
```