STRENGTHENING CRYPTOGRAPHY USING QUANTUM PROPERTIES

Mr M. Krisnamoorthy, M.E., MBA. NAVEEN S R, PRADEISH C, MOHAN RAJ RISHI S

Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamilnadu, India

I. ABSTRACT

For any encryption we need randomness, but for the generation of pure random numbers from the classical computers, we must feed the seed to generate pseudorandom numbers. But anyone can perfectly predict all the random numbers generated by the computer with the seed of what we feed. So, in our project we introduce quantum computing, to create a true random bit so numbers by its superposition concept and due to its no-cloning property, if one tries to read the random numbers, the quantum state will be changed. But quantum machine is not accessible to all the computers. As of now the servers only can have the ability for generating pure random numbers, still user devices lack its ability. So, we also find method for user devices to get pure random numbers from server's quantum machine without compromising or it is the future development of our project.

II. INTRODUCTION

The Generation of pure random numbers from the classical computers. For any encryption we need randomness, we have to feed the seed to generate pseudorandom numbers. But anyone can perfectly predict all the random numbers generated by the computer with the seed of what we feed. So, in our project we introduce quantum computing, to create a true random bit so numbers by its superposition concept and also due to its no-cloning property, if one attempts to read the random numbers, the quantum state will be changed. But quantum machine is not accessible to all the computers. As of now the servers only can have the ability for generating pure random numbers, still user devices lack its ability. So, we also find method for user devices to get pure random numbers from server's quantum machine without compromising or it is the future development of our project. -Type of Technology used: Quantum computing - Fundamental unit of information: Qubit - Fundamental Theorem: No-cloning of Quantum mechanics.

III. EXISTING SYSTEM

A classical computer based on transistors that encodes data in binary digits (or “bits”) that can only be a “1” or a “0” (think “on” or “off), a quantum computer uses “qubits” where a single qubit is able to encode more than two states. (Technically, each qubit can store a superposition of multiple states, but the mathematics is far too complex for the purposes of this article!) There are two basic building blocks of all encryption techniques: substitution and transposition. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. The transposition technique is a cryptographic technique that converts the plain text to cipher text by performing permutations on the plain text. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems can be easily solved on a sufficiently powerful quantum computer running Shor's algorithm.

DISADVANTAGES IN EXISTING SYSTEM

If any one finds the SEED, What are the possible random numbers that the computer will generate can be predicted.

A Programmer gives the SEED(1,2,3,4) and user gives the SEED(1,2,3,4), What the person computer random numbers generated is as same as user computer generates. From this process anyone can easily crack the key for cryptography.

If a hacker finds the starting time of a computer, with that time he can calculate the seed with brute force method to find the SEED.

In Algorithmic, Somewhere the source code is leaked with algorithm they will reverse the code and find the SEED.

In manual, if the given random number is leaked they easily find the SEED.

IV. PROPOSED SYSTEM

In this project we can directly generate SEED (or) Cryptographic key using Quantum Computing. In Quantum computer we set the value in super position state, Hence the bits set the value on the go’s of 0’s and 1’s 50% equally.

The SEED generated in superposition state comes as definite random number. Quantum computer is the only source to generate true random numbers. Hence, No one can predict the SEED in Quantum computer because it is a true random.

NO-CLONING PRINCIPLE

This theorem says, if there may or may not be some chances of prediction of SEED in Quantum computing, and the only way is to clone the whole Quantum machine (may be).

No cloning theorem says there is no chances of clone this process.

Hence, No one can predict the random numbers at that time or starting point or algorithmic it is truly random. So, we use Quantum computing to generate random numbers.

V. ALOGORITHM

Algorithm to share pure random number to client without any compromise:

Step 1: Generate pure random prime number P

Step 2: Generate pure random primitive root G

Step 3: Share P and G to client

Step 4: Generate pure random server secret A

Step 5: Generate (pure random) X = G^A mod P and sent to client

Step 6: Client Generate pseudo random client secret B

Step 7: Client Generate Y = G^B mod P and sent to server

Step 8: Server Generate (pure random) R = Y^A mod P

Step 9: Client Generate (pure random) R = X^B mod P

Step 10: Uses pure random for cryptography

Thus the pure random number generated using quantum computer is shared to client.

VI. LITERATURE SURVEY

Prashant Singh, Department d'Informatique et de recherche operationnelle, Universite de Montreal, Montreal, Canada. discussed about the study of the basics of Quantum computing. A New outlook to the Principle of Linear Superposition Modification of Wave function as a requirement of Quantum teleportation. He explained about the Measurement Problem by Symmetry breaking process. EPR Correlation: Interacting Hamiltonian Vs Non-Linear Wave function. Possibility of third paradigm in Quantum Mechanics.

Heng Fan, Yi-Nan Wang, Li Jing, Jie-Dong Yue, Han-Duo Shi, Yong Liang Zhang, and Liang-Zhu Mu

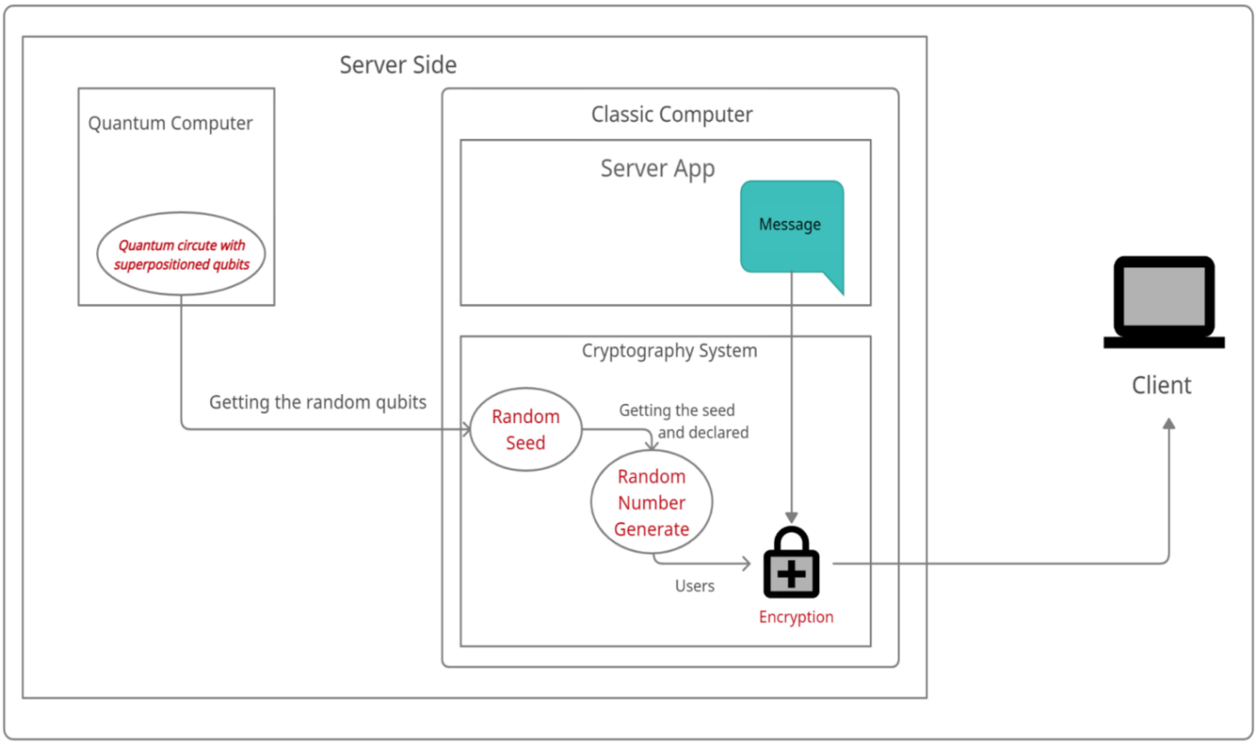
Beijing National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China Collaborative Innovation Center of Quantum Matter, Beijing 100190. China 3 School of Physics, Peking University, Beijing 100871, china.[2] discussed about the Quantum Cloning Machines and the Application and the Qubit and Quantum entanglement. They explained about the quantum gates and No-Cloning theorem.

VII. SYSTEM ARCHITECTURE

A system architecture is the conceptual model that defines the structure, behaviour, and more views of a system.[1] An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system.

A system architecture can consist of system components and the sub-systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture, collectively these are called architecture description languages (ADLs).

One can think of system architecture as a set of representations of an existing (or future) system. These representations initially describe a general, high-level functional organization, and are progressively refined to more detailed and concrete descriptions.



Quantum circuit and result.

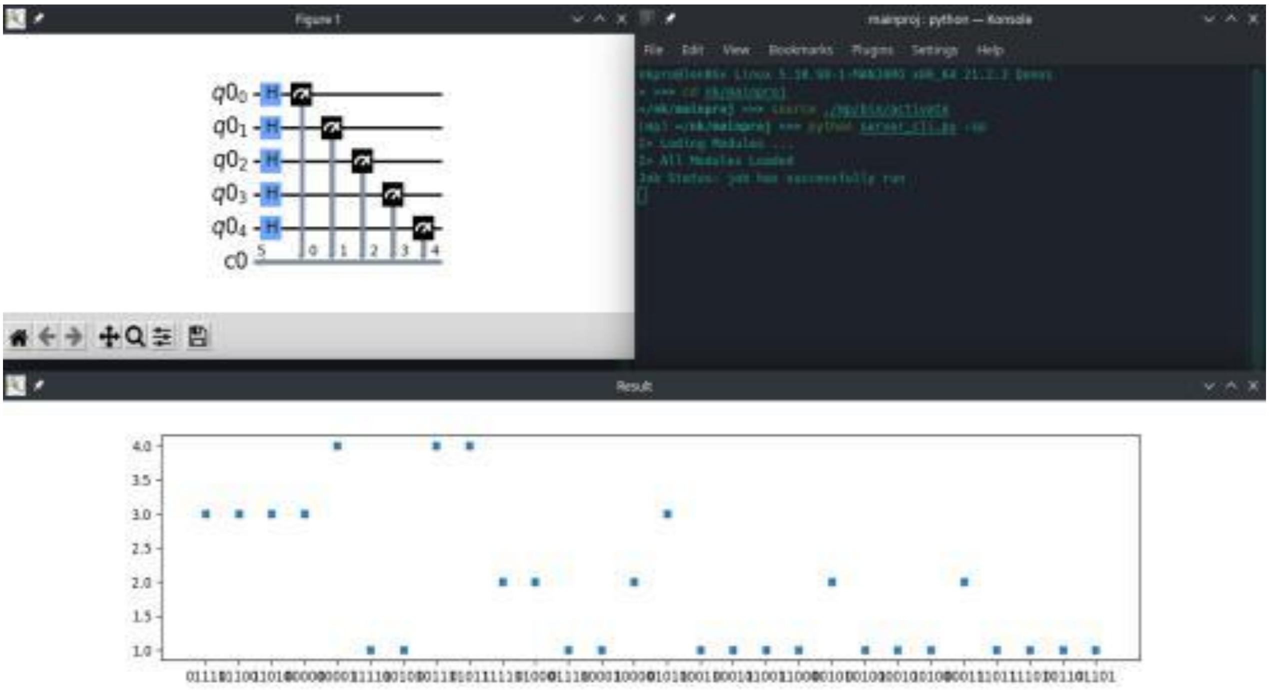


Figure 1
q0₀ q0₁ q0₂ q0₃ q0₄ c0
H
5 0 1 2 3 4
mainproj : python — Konsole
File Edit View Bookmarks Plugins Settings Help
Result
4.0
3.5
3.0
2.5
2.0
1.5
1.0

```
[illegible] Linux 5.10.[illegible] x86_64 21.[illegible]
~ >>> cd [illegible]/mainproj
~/mk/mainproj] >>> source ./[illegible]/bin/activate
(mk) ~/mk/mainproj] >>> python server_cli.py -[illegible]
I> Loading Modules ...
I> All Modules Loaded
Job Status: job has successfully run
```

VIII. Future Enhancement

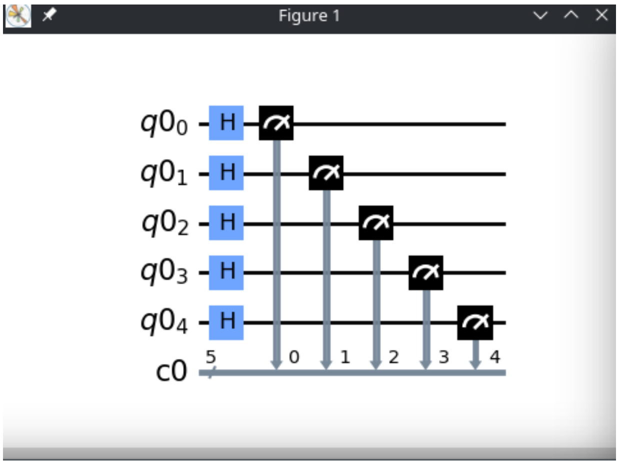
To create a generic algorithm to support all type of server-client protocols and cryptography techniques using the pure randomness (which is shared using proposed method)

To find out the efficient way to implement both the quantum computer and the previously mentioned algorithm to all the domestic and commercial servers.

The generated SEED in superposition state comes as definite random number.

Thus the true random numbers can be only generated in Quantum computers.

IX. Quantum Circuit



This quantum circuit can generate random bits of length 5 using hadamard gate in any quantum processor.

X. Conclusion

With this proposed system the SEED used for generate random number is secured and can't be revealed to any one because of we communication with quantum computer directly and not cached anywhere.

Also, with the help this method we can securely send true random number generated using quantum computer to client even in un-encrypted channel without any compromise.

Combination of retrieving server app source code and monitoring all the server communication can lead to a massive cyber-attack. Although these attacks are rare and hard to happen, there is no proof it can't happen in future. So to prevent these kinds of attacks this project uses the quantum properties.

XI. References

[1] Prashant Singh. A Study of the basics of Quantum Computing. Department d'Informatique et de recherché operationnelle, Universite de Montreal, Montreal. Canada, 2005.

[2] Heng Fan, Yi-Nan Wang, Li Jing, Jie-Dong Yue, Han-Duo Shi, YongLiang Zhang, and Liang-Zhu Mu Beijing. Quantum Cloning Machines and the Application. National Laboratory for Condensed Matter Physics, Institute of Physics, Chinese Academy of Sciences, Beijing 100190, China Collaborative Innovation Center of Quantum Matter, Beijing 100190, China 3 School of Physics, Peking University, Beijing 100871, China, 2014

[3] Saasha Joshi* and Deepti Gupta. Grover's Algorithm in a 4-Qubit Search Space. Department of Computer Science and Engineering, University Institute of Engineering and Technology, Panjab University, Chandigarh, 160014, India, 2021

[4]Pratik Roy*, Saptarshi Sahoo, Amit Kumar Mandal and Indranil Basu. Quantum Cryptography–A Theoretical Overview. Institute of Engineering and Management, Salt Lake Electronic Complex, West Bengal, Kolkata, 700091, India, 2021

[5] Prof. Dr. Jan Sładkowski. Quantum Computing and Quantum Information Processing. Institute of Physics, University of Silesia, 75 Pułku Piechoty 1, Pl 41-005 Chorzow, Poland, 2021

[6] Matheus Guedes de Andrade, Wenhan Dai; Saikat Guha and Don Towsley. A quantum walk control plane for distributed quantum computing in quantum networks. IEEE International Conference on Quantum Computing and Engineering, 2021

[7] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, M. P. de Almeida and A. Gilchri. Photonic quantum computing: Shor's algorithm and the road to

fault-tolerance. Institute of Electrical and Electronics Engineers (IEEE), 2018

[8] G Arun, Vivekanand and Mishra. A review on quantum computing and communication, 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking, 2014

[9] Jasmeet Singh and Mohit Singh. Evolution in Quantum Computing. International Conference System Modeling & Advancement in Research Trends, 2016

[10] Huanguo Zhang, Zhaoxu Ji, Houzhen Wang and Wanqing Wu. Survey on quantum information security. Wuhan University, Wuhan, China and Hebei University, Baoding, China, 2016

[11] Marcello Caleffi, Jessica Illiano, Seid Koudia and Angela Sara Cacciapuoti. The Quantum Internet: a Communication Engineering Perspective. University of Naples Federico II, Naples, Italy Laboratorio Nazionale di Comunicazioni Multimediali, CNIT: National Inter-University Consortium for Telecommunications, Naples, Italy, 2021

[12] Napat Thumwanit, Chayaphol Lortaraprasert, Hiroshi Yano and Rudy Raymond. The University of Tokyo, Tokyo, Japan, Keio University, Yokohama, Japan and IBM Quantum IBM Japan, Tokyo, Japan, 2021

[13] Sherry Wang, Carlisle Adams and Anne Broadbent. Password authentication schemes on a quantum computer. School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada, 2021

[14] Rohit De, Raymond Moberly, Colton Beery, Jeremy Juybari and Kyle Sundqvist. Multi-Qubit Size-Hopping Deutsch-Jozsa Algorithm with Qubit Reordering for Secure Quantum Key Distribution. Del Norte High School, San Diego, CA, USA, Faster Logic, LLC, San Diego, CA, USA and San Diego State University, San Diego, USA, 2021

[15] Laura Gatti and Rafael Sotelo. Quantum Computing for Undergraduate Engineering Students: Report of an Experience. Universidad de Montevideo, Montevideo, Uruguay, 2021