Advanced Production and Industrial Engineering
R.M. Singari and P.K. Kankar (Eds.)

doi:10.3233/ATDE220779

Using Quantum Cryptography for End-to-End Encryption

AKSHAT TIWARI[1] and MAYANK SINGH
Dept. of Applied Physics, Delhi Technological University

Abstract. These days almost everyone is involved in online communication. With the advancement in quantum computing the messaging system brings the current state of major public encryption systems into mind which can be hacked to be broken. Many developers working in the industry are just discovering this and will soon be looking at changing their communication systems to be protected in quantum time. This paper documents the tried-and-tested constructions of the encryption system used in the real-life android application. Implementation of Quantum Key Distribution is shown to work well with a quantum computer that is monitoring the whole process of sharing the transferred key. It will detect any third-party interaction and take instant action. This paper states tried and tested way of encrypting systems with the help of QRNG application and Qiskit SDK.

Keywords. Quantum Computing, Encryption Systems, Quantum Key Distribution (QKD) technology.

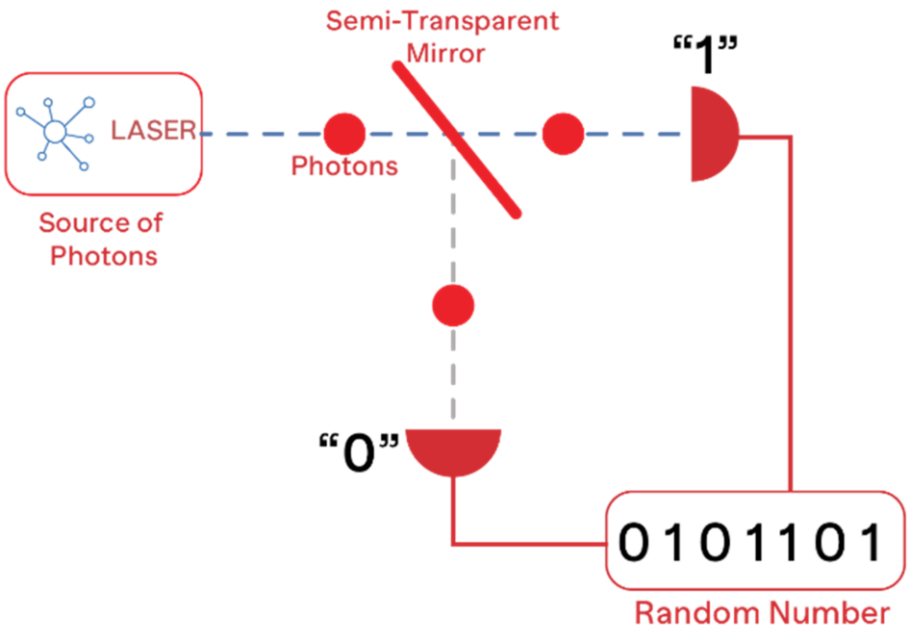
1. Introduction

Quantum Key Distribution (QKD) involves random sequence sharing between sender & receiver. In cryptography if a normal message is combined with an encrypted key, it results as a cipher text. The ciphertext will be decrypted if the key is seen again. The chances of identifying the message by a foreign body by any means will be very less. The Quantum Random bits are used as the encryption tool to remove text encryption between the two ends because everything sent is translated into totally unpredictable numbers generated using Quantum Random Number Generator. For example, in the case of Alice and Bob. When Alice sends an encrypted text with some random number, it will only be shown with the same number that has been associated with the two users. After the receiving end has successfully identified the key, shifting is done to transfer the data between the two. The data transferred would first be checked and then stored as a raw material tool.

QKD is one of the ways which uses the algorithm to implement a security-based system associated with quantum mechanics knowledge of generating a random key. It ensures a secure communication between the end users. The random key generated is used to encrypt or decrypt the cipher text. Quantum Computing systems has the ability to identify whether the random key has been accessed by any third party or not. If

[1] Akshat Tiwari, Mayank Singh, Department of Applied Physics, Delhi Technological University.

someone trespass the connection, the current random number will be exchanged with a new number.



The communication method uses properties of quantum physics to exchange cryptographic keys in a way that is provable and guarantees security. Quantum Key Distribution (QKD) is a secure communication method for the exchange of encrypted keys that are known only between shared users. Qiskit helps in establishing an environment for secure transmission of data from one end to another. It provides the perfect tools to help putting a quantum-based program into simulation.

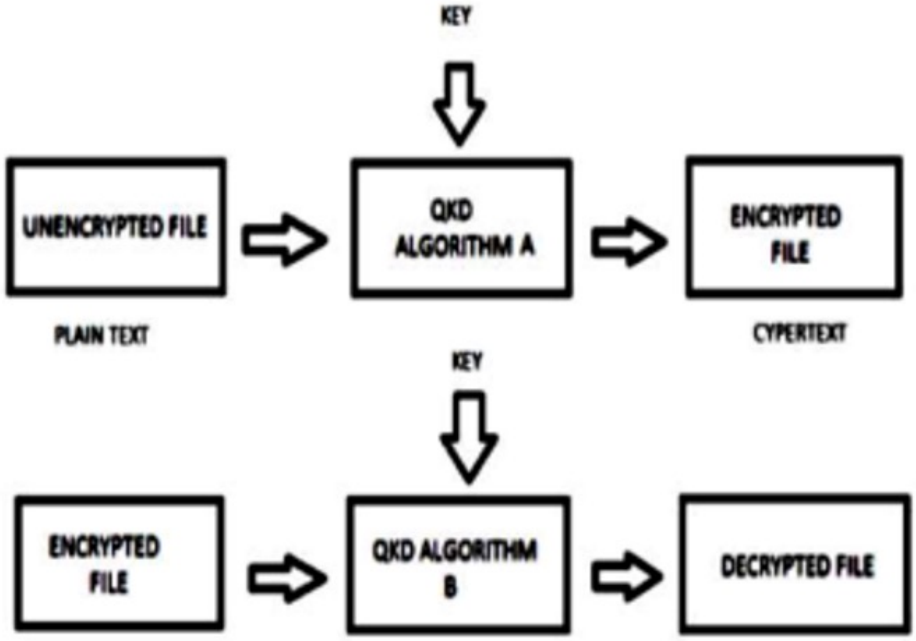
The way we are putting this project forward is the easiest way as compared to the photon level transmission using optical fiber for a finite distance. In that way, the end user will reflect the loss of efficiency due to long distance. The photon particle establishes random quantum bits using spin angular momentum.

Quantum Mechanics always consolidate its way of implementing the unpredictable nature in various application. Let it be cryptography or Quantum key distribution or quantum random number generation, Quantum Computing always has an edge over the standard algorithmic encryption systems. It will always make most of today's public key an insecure way of encryption and will omit the usage of other methods of security really soon.

2. Working

As soon as the connection is established between the two users, a key is generated using QRNG. This key is shared among the users only either using the Bluetooth way or for a distance communication as a local key to the end user. The program will match the shared

key at the end and a successful communication bridge will be formed. This whole process is thoroughly monitored by a system server. By any chance if a third party tries to trespass the security system, the shared key will be deleted and a new random key will be assigned to the end users.



3. Advantages and disadvantages of using a quantum method of encryption

The implementation of quantum computing is like the latest in the bookshelf. There are many reasons that states how quantum computing can pose a problem and since they have recently been into process to give rise to super computers many people have their beliefs over the success with negligible errors. The current working algorithmic based encryption system claims an end-to-end encryption technology, but fails each time. Although there are many different reasons why quantum computing can pose a problem for the cyber security landscape, the biggest being that classical cryptography techniques can be broken in hours rather than years. The algorithmic based big sized numbers can slow the processing speed but it will not let the algorithms to be cracked, whereas the QRNG applications can process within seconds. The Application Programming interface of QRNG contains some pre-programed data which was once performed via laser diodes to polarize the photons into binary digits, thus these random binary digit forms a series of unpredictable numbers.

4. Practical Implementation

In this paper we continued our study about quantum methods to set up an end-to-end encryption-based system and try to provide best encryption technology for real life and introduce it to the world of social media and personal chat. We wanted to develop a method using the IBM Quantum API and the Qiskit library. We have developed a protocol and engaged them to create an untraceable key to encrypt and decrypt the communication between two devices and their interactions.

Compared to classical methods of implementing end-to-end encryption, quantum cryptography has an ultimate advantage of unconditional security and sniffing detection. It promises to solve critical problems including cyberspace security and many more. Our analysis focuses on providing security and the sniffing concept of quantum encryption, hence making it the future of the internet. Our experimental analysis results reveal the unconditional security and sniffing of quantum cryptography, making it suitable for the Internet of the future.

5. Quanage

Quanage for Android is a mobile app for the application of Quantum Encryption on the Android platform. Here we set up two randomly generated keys and keep track of them, taking advantage of the quantum computer provided by IBM Quantum using their API. The app is a live demonstration of QKD concepts and is the first truly secure application for exchanging data over the Internet.

In order to share messages with someone, the users first generate a random key using QRNG, the Qiskit SDK and IBM Quantum APIs, which is then shared amongst them through peer-to-peer networks for the first time. After this, the keys are monitored by a server and read/write access to the key is only provided to the app and any foreign interaction will trigger a function call to reset the key and discard the previous one. We are happy to say that the demonstration works and is currently implemented in the application which we have made.

6. Future Work

Perhaps the era of quantum computing in this upbringing technology has gained a lot of attention in the market. Let it be the multinational electronics and information technology company like Samsung or intel, quantum processors are taking over the market. In the near future, there can be events of hacking into the quantum servers to initiate the malware attacks, people may take advantage of quantum computers but it is just a matter of time before applications like Quanage will be there to help with its unconditionally well operated and secured systems. Quanage is yet setting up the barriers of advance and secure communication. We expect to improvise the user interface and generate higher quantum bits so that the communication can be as quick as possible. With more people joining us with Quanage, we can expect a wide range of communication methods other than the simple texts.

7. Conclusion

We did the literature review of quantum encryption techniques, after studying them, we decided to work on the QKD method of encryption. With our application "*Quanage"* we were able to implement the system between two end users using Qiskit SDE and QRNG method. Our implementation has an edge over the significant transmission of photon particle with the help of optical cable. These optical cables are limited to quite a distance before it's too dim to be received and decrypted at the other end. That method includes a huge investment, which for a normal private conversation is not a value at all. Quantum computing is not just the game changer, but the future relies on this.

References

[1] https://en.wikipedia.org/w/index.php?title=Quantum_cryptography&oldid=1068868060
[2] https://cloud.ibm.com/quantum/services
[3] K. G. Paterson, F. Piper, R. Schack | why quantum cryptography? Cryptology e-Print archive: report 2004/156, http://eprint.iacr.org/2004/156
[4] https://www.idquantique.com/quantum-safe-security/overview/quantum-key-distribution/#:~:text=Quantum%20cryptography%20is%20a%20technology,light%2C%20across%20an%20optical%20link
[5] Ines Duits- "The Post-Quantum Signal Protocol" | Secure Chat in a Quantum World | Thesis, February 5, 2019
[6] https://www.sciencedirect.com/science/article/pii/S0304397514006963