Cryptography and Network Security 2022-23
Quantum Cryptography Technique
College of Engineering, Pune
Guided by : V.K. Pachghare

Omkar Bankar 111903055

Pratik Bandre 111903063

Rajkumar Sawant 111903066

Riddhi Tharewal 111903068

Abstract

Cyberspace has become the most popular carrier of information exchange in every corner of our life, which is beneficial for our life in almost all aspects.Traditional cryptography methods use either public key which is known to everyone or on the private key. In either case the eavesdroppers are able to detect the key and hence find the message transmitted without the knowledge of the sender and receiver.Quantum cryptography concentrates on the solution of cryptography that is imperishable due to the reason of fortification of secrecy which is applied to the public key distribution of quantum. It is a very prominent technology in which 2 beings can securely communicate along with the sights belongings to quantum physics. This paper includes detailed insight into the quantum cryptography technique.

Keywords: Quantum Cryptography, QKD, photon polarization

1 Introduction

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

Two main Types of Cryptography:

1. Symmetric Key Cryptography: In these technique, single common key is used for both encryption and decryption.

2. Asymmetric Key Cryptography: In these technique,different keys are used for encryption and decryption.

In practice, due to significant difficulties of distributing keys in secret key cryptography, public-key cryptography algorithms are widely used in conventional cryptosystems.

Einstein writes, “It can’t believe God plays the cosmos dice,”! However, quantum mechanics showed him to be mistaken and an amazing crop for new in’s encryption schemes benefits from the dices that Einstein found so worrying. While most people assume that they are science fiction, quantum encryption systems now operate, with experiments shielding internet traffic in urban areas., QKD offers information-theoretical confidentiality, which is strongly founded on physics law, on the unproved basis of core public technology.

Quantum cryptography is an attempt to allow two users to communicate using more secure methods than those guaranteed by traditional cryptography.

2 Comparative Analysis

	Neural Cryptography	Quantum Cryptography
Methodology	Combination of neural network concept from biology and cryptography	Combination of laws of quantum physics and cryptography
	ANN is used to depict the neural network	Heisenberg’s uncertainty principle and the principle of photon polarization are the two fundamental laws on which whole technique is based
Used in	used for secret key exchange generated through tree parity machine by synchronization. And the encryption is done through various cryptographic encryption algorithms	used for the secret key generation through quantum cryptography protocols such as BB84 protocol, which is communicated over quantum channel, and finally the key is used for encryption with classical cryptography techniques
Advantage	The advantages of this system are that it is difficult to break without knowing the network architecture.	Random key generation
	Noise Tolerance	more secure cryptography than public key cryptography, can tackle big data effectively
	Message misrepresentation chances are very low	allows secure allocation of random key information among two partners
Disadvantage	Only effective where the key is the weight and the network architecture	High bit error rate
		point to point link
		lower key allocation rate
		serve up to limited distance

3 Methodology

3.1 Quantum Cryptography:

Quantum cryptography is based on the phenomena of quantum physics which allows secure data transmission between sender and receiver. Quantum cryptography constitutes a revolution in the field of network security.

Quantum cryptography is a latest and advanced branch of cryptography its basis lays in the two beliefs of quantum technicalities: Heisenberg’s uncertainty principle and principle of photon polarization.

Heisenberg’s uncertainty principle says that some pairs of physical properties are related in a way that while measuring one property may prevent the person from knowing the other simultaneously. In particular, the selection of what direction to measure affects all successive measurements. When an unpolarized light enters a vertically aligned filter, it absorbs some of the light and polarizes

the rest in the vertical direction. A subsequent filter tilted at some angle q absorbs some of the polarized light and transmits the rest, giving it a new polarization. A pair of orthogonal polarization states used to express the polarization of photons, such as horizontal/vertical, is referred to as a basis.

In 1984, a quantum key distribution protocol called BB84 was developed. The BB84 protocol proceeds through the following steps: 1. Sender sends polarized photons to the receiver which could be rectilinear or in diagonal direction 2. The receiver then checks for the direction of the photons by randomly selecting the basis (rectilinear/diagonal) and saves the results. Basis selected for measurement by the sender and the receiver need not be the same. 3. Through a public channel the receiver informs the sender his basis of measurement. 4. Sender then sends the correct bits (bits whose basis are the same) over the public channel after comparing the actual basis with the received basis. The incorrect bits are discarded by the sender and receiver and the correct ones are taken as keys. If an attacker uses the same basis as that of the sender the he will be able to predict the original information and if not the by this activity of the attacker the information sent is affected and because of which the receiver will either get the hampered data or no data, in both the cases the presence of attacker is detected.

3.1.1 Quantum key Distribution:

Key Distribution is a way of distributing encrypted keys between two parties. The simple way of key distribution is by meeting in person in a secure environment and exchanging keys. But now a days we can exchange at any distance by using Public keys like ciphers, RSA, Diffie- hellman and ecc to exchange keys .

The problems with the conventional key distribution is that they use simple mathematical calculations to transfer data these are easy to compute and can be accessed by third parties easily.

This classic key distribution approach has many challenges. They are like the classic key can only generate weak random numbers which can be obtained easily by third parties. Also, the CPU power, and these keys are vulnerable to new attack strategies as they need to be re programmed again if any new attack strategies were used. Quantum computers can make these classical encryption strategies unsafe as quantum computers can decode data present in classical keys easily if quantum computers become a reality. So, to stay ahead we need to use large Asymmetric keys to securely store and distribute our symmetric keys. All these things make us to rethink the security of cryptographic keys.

QKD addresses these problems faced by cryptographic keys by using all the quantum mechanics to transfer data or information from one point to another point The QKD uses a quantum channel of its own to transfer data from transmitter to receiver. It also needs a public Communication link so that it can access post processing. It also has a portal which calculates the amount of data lost through interception

3.1.2 Quantum Key Distribution Protocols Implementation:

A very nice online demonstration of the process of transferring information using quantum cryptography methods, created by Fred Henle, is located at `http://monet.mercersburg.edu/henle/bb84/`. The following is a specific step-by-step outline of the process, paraphrased and augmented from (3). Staying with the convention, Alice is used to refer to the sender, Bob to the receiver, and Eve to the eavesdropper in this description.

Sending

1. Alice determines the polarization (horizontal, vertical, left-circular or right-circular) of each burst of photons which she's going to send to Bob. Since a lot of this information will later be discarded, this can probably be done randomly. The goal is not to transfer a specific key, but to agree on a key that is common to both parties.

2. A light source from a light-emitting diode (LED) or from a laser is filtered to produce the desired polarized photons. Ideally, each pulse consists of a single photon. However, in real life it actually has to be a beam of light with very low intensity. If the intensity is too low, a pulse may be undetectable for the receiver, yet if it's too high, then the polarization of the photons can be detected discreetly (i.e. a photon from the beam can be measured by the eavesdropper with respect to both bases without any noticeable difference to the beam). Both cases are undesireable to say the least, so the intensity has to be regulated very carefully. (6)

Receiving and converting

3. Bob randomly generates a sequence of bases (rectilinear or circular), and measures the polarization of each photon with respect to one of them.

4. Bob tells Alice which sequence of bases he used, without worrying about other people hearing this information.

5. Alice publicly responds with which bases were chosen correctly.

6. Alice and Bob discard all observations except for those with the correctly-chosen bases.

7. The remaining observations are converted on to binary code (left-circular or horizontal is 0, and right-circular or vertical is 1).

Correcting errors - step 1

8. Alice and Bob agree on random permutations of bits in the resulting string, to randomize the positions of errors.

Two errors next to each other are very hard to detect, yet it is likely that an error with the instruments or because of random noise would alter a sequence of bits one after the other. Randomization helps account for that.

9. The strings are partitioned into blocks of size k, with k ideally chosen to make the probability of multiple errors per block very small. Note that if Alice's string contains 101100 and Bob's contains 101111, the parity is the same, 1, even though there are two mistakes in the block. Making k small is one of the steps taken to minimize the chance of this happening, since the chances of having two errors in a block of size 50 is much less than in a block of 500, especially after the errors are randomized.

10. Alice and Bob compute and exchange parities for each block. This information can be made public, but, to ensure security, the last bit of each block is then discarded, making the information useless for Eve.

11. Any block with different reported is broken down further and a binary search is used to locate and correct the error. Alternatively, if the length of the key is already sufficiently large, those blocks could even be discarded.

12. Steps 9-12 are then repeated with increasing block size, k, in an attempt to discover multiple errors that could've gone undetected within original blocks.

Correcting errors - step 2

13. Finally, to determine if additional errors remain, Alice and Bob do another randomized check. They publicly agree on a random assortment of half the bit positions in their string, and compare parities, followed discarding the last digit, as always.

14. If the strings are different, then there is a probability of a disagreement of parities. Then a binary search is used to find and eliminate error, as described above.

15. After r repetitions of step 13 without disagreements, Alice and Bob can conclude that their strings disagree with probability (1/2)r, which can obviously be made arbitrarily small by increasing r.

4 Real World Applications of Quantum Computing

The exponential development in processing power that accompanies the advancement of a feasible quantum PC looks set to change a wide scope of businesses and applications. Many processing applications with enormous datasets are ready to profit by the appearance of the quantum PC and a lot of what the world does depends on the standards of science – from reproduction to application. The difficulty is, maths can be hard. A few counts required for the successful re-enactment of genuine situations are essentially past the ability of traditional PCs – what's known as immovable issues. Quantum PCs, with their tremendous computational force, are obviously fit to tackling these issues. To be sure, a few issues, as are considering, "hard" on an old-style PC, yet are "simple" on a quantum PC. This makes a universe of chances, across pretty much every part of present day life.(Spector, Barnum et al. 1999)

4.1 HealthCare

4.1.1 Research:

Traditional PCs are restricted as far as the size and multifaceted nature of particles they can mimic and look at (a basic procedure in early medication improvement). In the event that we have a contribution of size N, N being the quantity of particles in the inquired about particles, the quantity of potential associations between these molecules is exponential (every iota can interface with all the others). Quantum PCs will permit a lot bigger particles to be reproduced. Simultaneously, scientists will have the option to show and re-enact connections among medications and every single 20,000+ protein encoded in the human genome, prompting more prominent headways in pharmacology.(Mohseni, Read et al. 2017)

4.1.2 Diagnosis:

Quantum innovations could be utilized to give quicker, progressively exact diagnostics with an assortment of uses. Boosting AI abilities will improve AI – something that is now being utilized to help design acknowledgment. High-goals MRI machines will give more noteworthy degrees of detail and furthermore help clinicians with screening for ailments.

4.1.3 Treatment:

Directed medicines, for example, radiotherapy, rely on the capacity to quickly demonstrate and mimic complex situations to convey the ideal treatment. Quantum PCs would empower advisors to run more reproductions in less time, assisting with limiting radiation harm to sound tissue.

4.2 Circuit, Software, and System Fault Simulation

At the point when one grows huge programming programs with a huge number of lines of code or enormous ASIC chips that have billions of transistors, it can get horrendously troublesome and costly to confirm them for rightness. There can be billions or trillions of various states and it is inconceivable for an old style PC to check each and every one in recreation. In addition to the fact that one wants to comprehend what will happen when the framework is working ordinarily, yet one likewise needs to comprehend what occurs if there is an equipment or other mistake. Will the framework recognize it and does it have a recuperation system to alleviate any conceivable issue? The expenses of a mistake can be high since a portion of these frameworks can be utilized where lives or a huge number of dollars may be reliant on their being sans blunder. By utilizing quantum processing to help in these recreations, one can conceivably give a vastly improved inclusion in their re-enactments with an enormously improved chance to do as such.

4.3 Cyber-Security

Digital security is turning into a bigger issue each day as dangers around the globe are expanding their capacities and we become increasingly powerless as we increment our reliance

upon computerized frameworks, get familiar with cybersecurity in 2019 over at locales, for example, Upskilled and others. Different procedures to battle digital security dangers can be created utilizing a portion of the quantum AI approaches referenced above to perceive the dangers prior and moderate the harm that they may do.

4.4 Logistics and Scheduling

Numerous basic advancements utilized in industry can be characterized under coordination's and booking. Think about the carrier coordination's administrator who needs to make senseof how to arrange his planes for the best assistance at the most minimal expense. Or then again the industrial facility chief who has a regularly changing blend of machines, stock, creation requests, and individuals and requirements to limit cost, throughput times and expand yield. Or on the other hand the evaluating administrator at a car organization who needs to make sense of the ideal costs of the considerable number of handfuls vehicle alternatives to expand consumer loyalty and benefit. Albeit, old style registering is utilized intensely to carry out these responsibilities, some of them might be unreasonably convoluted for a traditional processing arrangement while a quantum approach might have the option to do it.

5 Challenges faced by quantum computing

Today Quantum computing is exactly at the same point as it was in the case of classical computer in 1960's which is used to be of a room size. The only difference is that the growth is exponential in terms of research, progress and results. The major challenges for quantum computing include Quantum computer needs absolute zero temperature to conduct super conductivity. The use is not widely accepted due to its size and limitations to the type of jobs it can do. The questions that needs to be answered are How superconductivity can be performed at non-absolute temperature, and how it can perform the multipurpose task for which we use the classical computers.

The strength of quantum computing lies within the basic model on which it operates "Qubits", it works on the principle of superposition which means the qubit can take either 0 or 1 at the same time. This property brings the increment in power for computation exponentially where n is number of qubits. The current practical achievable value of n is 53 by google and it claims quantum supremacy. In response to Googles claim a company called D-Wave has announced a 5,000-qubit quantum computer to achieve quantum supremacy. Imagine the power of a computer which can solve a problem with a complexity of 25000.

In a recent study, a team in UNSW Sydney lead by Prof. Andrew Dzurak said "New results open a path for real world application of quantum computing in business and governance". The researchers came up with the term "Hot Qubit" which operate at higher temperature compared to "Qubit" which works at a fraction below absolute 0. The researcher's quantum processing unit cell works at 1.5 kelvin or 15 times warmer than the chip-based quantum computers such as Google's and IBM's. Although 1.5 kelvin is still very close but it can save millions of dollars in just refrigeration of qubits (Bernstein 2009).The technology has the potential to make a valuable contribution to the network security among government, businesses, and academic environment.

Quantum memories are the place where we can store Q-bits. The storage of the bits require larger storage units and also these units must be highly efficient and also higher bandwidth requirements. This is the reason it is harder to build a quantum memory. Solid state quantum memories with rare earth materials can be used in building of quantum memories (Arun and Mishra 2014).

6 Conclusions

Based on quantum mechanics and classical cryptography, quantum cryptography is a novel one in the field of cryptography. Compared with classical cryptography, its ultimate advantages are the unconditional security and the sniffing detection. These characteristics can solve cyberspace security critical problem for the future Internet. In particular, quantum cryptography provides security for various applications (e.g., Internet of things and smart cities) in cyberspace for the future Internet. Our experimental analysis results show the unconditional security and sniffing detection of quantum cryptography, which makes it suitable for future Internet.

The future of quantum computing looks bright as quantum computing has many applications like quantum cryptography, Teleportation of information. It also can be used in development of medicines by studying molecular behaviour, It also can be used in satellite communications as well. However, we hope that the theory becomes practical someday so we can use its advantages in many other fields of science.

The conclusion of this paper is that quantum computing is one of the huge opportunities for the modern world to open up the doors for unanswered questions. It promises to solve problems which classical computers practically cannot. But the cost behind quantum computing is too high. The major challenges that stands right now is to reduce the cost so that it is more accessible for experiments. And a significant progress has been made in UNSW Sydney which will save millions of dollars. Other challenges include to make a hybrid computer which can operate high processing jobs simultaneous with classical computing jobs which will open the opportunity to business and commercial use.

7 References

1. Barrett, J., et al. (2005). "No signaling and quantum key distribution." Physical review letters 95(1): 010503.

2. Bernstein, D. J. (2009). Introduction to post-quantum cryptography. Post- quantum cryptography, Springer: 1-14.

3. Gisin, N., et al. (2002). "Quantum cryptography." Reviews of modern physics 74(1): 145.

4. GUANCO, F. (2015). ”What is Quantum Key Distribution.” Cloud Security Alliance.
5. Ma, X. (2008). ”Quantum cryptography: theory and practice.” arXiv preprint arXiv:0808.1385.

6. Wasankar, M. P. P. and P. Soni (2013). ”An invention of quantum cryptography over the classical cryptography for enhancing security.” International Journal of Application or Innovation in Engineering Management (IJAIEM), vol 2.

7. Zhou, T., et al. (2018). ”Quantum cryptography for the future internet and the security analysis.” Security and Communication Networks 2018.

8. Steane, A. (1998). ”Quantum computing.” Reports on Progress in Physics 61(2): 117.

9. Aaronson, S. (2008). ”The limits of quantum.” Scientific American 298(3): 62-69.

10. Arun, G. and V. Mishra (2014). A review on quantum computing and communication. 2014 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking, IEEE.

11. Bennett, C. H., et al. (1992). ”Experimental quantum cryptography.” Journal of cryptology 5(1): 3-28.

12. Gruska, J. (1999). Quantum computing, Citeseer.