ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 5, Issue, 02, pp. 3473-3475, February, 2015

International Journal of
DEVELOPMENT RESEARCH

Full Length Review Article

USE OF QUANTUM CRYPTOGRAPHY IN COMMERCIAL APPLICATION

***Sihare Shyam, R.**

Silvassa College, Govt. (Aided) College of Arts, Comm and Science, Silvassa, Dadra and Nagar Haveli-396235, India

ARTICLE INFO

Article History:
Received 15th November, 2014
Received in revised form
26th December, 2014
Accepted 04th January, 2015
Published online 27th February, 2015

Key words:
Quantum cryptography,
Heisenberg's Uncertainty principle,
No-cloning photon,
Quantum computers.

ABSTRACT

Quantum cryptography is unconditional secure communication by using the phenomena of Heisenberg's uncertainty principle, no-cloning theorem of photon of quantum mechanics. Further, conventional cryptography susceptible at present computer computation but processing speed grow more rapidly and quantum computer abruptly launch then classical cryptography not so useful, it is easily breakable with the help of quantum computers. If it is implemented, then Quantum cryptography use in every sphere like ultra secure voting, secure communication with space, a smarter power grid, quantum internet etc. This paper aims to introduce different commercial application of quantum cryptography if it is implemented.

INTRODUCATION

Cryptography is a technique by which a message is encrypted by key at the sender side and it is decrypt with the same key at the receiver side. Cryptography used in "Julius Caesar" time also for message communication. Today, in computer world classical cryptography like RSA, DES, SHA-1 etc are used for unconditional secure communication from receiver to sender with the existence of third party. Classical Cryptography transferring message in encryption form and this technique well at this time because for breaking it into original message requiring integer factoring computation and today available computer are not capable to do with due time constraints. But, when the door open for quantum computer then integer factoring computation perform within a nanosecond then all the classical cryptography which is base on factoring and mathematical function are not so far usable. By using this technique, all the enterprise, organization, banking sector, education do their commercial transaction with believe as of confidentiality and reliability (Stallings, 1999). Such on situation, quantum cryptography play crucial role in unconditional secure communication in commercial application, governmental organization as well as military operation. Since, quantum key distribution depend on photon, which is light particles; photon behavior and its characteristics are uncertain at the particular time, that is if one characteristic is considered for accurate measurement another characteristic of photon alter their behavior. Hence, eavesdropper try to copy without knowing the sender and receiver then photon alter their properties. Due to this, Alice and Bob easily detect by threshold qubit error rate of photon (Bennett and Brassard, 1984). Thus, QKD doesn't rely on presenting interception or decryption but rather on detecting eavesdropping and self-destroying message a result[1]. Moreover, in early September of 2013, scientists in Japan announced the inauguration of the Tokyo QKD Network, an international collaboration between companies across Europe and Asia whose goal is to build quantum encryption networks that enables secure transmissions between as many as 64 computers within a network. Ultimately, this will increase the commercial viability of quantum encryption and open up the doors for wider use[1]. Today, the encrypted communications market is estimated to be worth $20 billion. Quantum encryption already protects both sensitive national security information in the

Corresponding author: Sihare Shyam, R.
Silvassa College, Govt. (Aided) college of Arts, Comm and Science, Silvassa, Dadra and Nagar Haveli-396235, India

[1] *http://digitaldisruption.com/4-real-world-uses-quantum-cryptography*

public sector and financial information in the private sector. Its security is tested and proven[2]. From above discussion, it is visible to us that, quantum key distribution is best alternative for secure communication rather than classical cryptography in commercial application. In Europe, Asia namely Japan and America it is implemented some extend in defense sector as well as banking sector which span between 10 km to 250 km ranges through fiber optics cable. Further, communicate through open space, some difficulties encountered in long distance due to photon decay, near future it is also implemented into open space due to technologies advancement[3]. Swiss Quantum's partner id Quantique and Magio technologies show interest into this technology and implemented into real world.

Break Classical Cryptography

Classical Cryptography is suitable today system resources and its performance. But, by quantum computer and corresponding quantum key distribution it is easy to break. Shor's algorithm is quantum algorithm of integer factorization for finding prime factor is used to break public key cryptography schemes such as the widely used RSA scheme (Bennett and Shor, 1998). Since, conventional cryptography depends on mathematical function and quantum computer work on photon behavior[3]. Hence, photon using quantum computers millionth times faster than traditional computer that's why is easily breaking the classical cryptography.

Quantum Protocol and Classical Protocol

Classical communication resources use for quantum key distribution. By which, original message encrypted using quantum key. At receiving side decrypt it with a help of same quantum key and recover original message. Quantum key, transfer through classical communication medium without modification or updating of already existing communication infrastructure.

Ultra-Secure Voting

With political upheaval and accusations of voter fraud rampant in developed and developing countries alike, it's clear that making the voting process more secure is a necessity. Since 2007, Switzerland has been using quantum cryptography to conduct secure online voting in federal and regional elections. In Geneva, votes are encrypted at a central vote-counting station. Then the results are transmitted over a dedicated optical fiber line to a remote data storage facility. The voting results are secured via quantum cryptography, and the most vulnerable part of the data transaction (when the vote moves from counting station to central repository) is uninterruptible. This technology will soon spread worldwide, as many other countries face the specter of fraudulent elections[4].

Quantum Internet

Internet is today life for searching and collecting information. But, today internet is not secure for transmission of confidential information. Confidential information hacking and cracking headlines frequently flash on the daily newspaper. If classical internet world transform into quantum internet world in some extend for secure purpose then its security and efficiency increase in many fold. Today switching techniques from classical to quantum is time consuming and get slow internet but technological advancement it improve far more as compare to classical cryptography.

Banking

In banking all transactions base on financial. All bank weather it is nationalized or internationalized are interconnected to one another for secure transmission of financial transaction. In presence of quantum computers banking financial transaction easily breakable weather it is dedicated transmission medium or private IP address. Hence, on that situation quantum key is well susceptible for secure communication for financial information among different banks.

Defense

Most of defense strategies, planning, technologies, and documents transferred from source one to destination through internet for security purpose. Risk of copying it by eavesdropper or enemy countries are more. By using quantum secure communication, send encrypted message without worrying about third party.

Open Space Secure Communication

Secure communication between satellite and astronauts is increasing concern. By using quantum key, it possible to secure communication as above mentioned end without concerning about advance technologies and intelligence. Since, main adversary effect of open space is that information available openly for each one.

Fast Searching Database Mechanism

Quantum computer searching mechanism fast as compare to conventional computer because it works on qubit. Qubit concept depends on quantum mechanical superposition principle. Like, telephone directory existing of 100 crore records of each individual. Conventional computer visit every record separately on the basis of particular entity viz. customer name. But in quantum computer, it require 10000 searching mechanism by qubit superposition principle.

Quick Solution of Undecidable Problems

Every sector exist different types of undecidable problems. In computer Salesmen Travelling Problem, Halting Problem, Busy Beaver Champion, Rice's Theorem, Post Correspondance Problem etc are easily and optimum way solve by using quantum algorithms. Like Shor's algorithms solve in some extend exponential factorization and

[2] *http://digitaldisruption.com/4-real-world-uses-quantum-cryptography*
[3] *Introduction to quantum Cryptography http://dx.doi.org/10.5772/56092*
[4] *http://digitaldisruption.com/4-real-world-uses-quantum-cryptography*

mathematical problems of traditional cryptography. Further, Grover's proposed about fast searching database.

Practical Business Application

Quantum computing is a practical tool for exteremely complex predictive analysis and machine searching where you need to access many variables and many patterns, test models against it. This is relevant in the area of drug discovery, cyber security, business, finance, investment, logistics and planning. Like drug discovery, trillions of combinations of amino acids to cycle through to find that single protein.

Ananlysis of Brain Function

The human brain is so complex entity interconnected by billions of neurons and glia cells. There is extracellular space between neuron filled with fluid. The neurons communicate one with another through classical synaptic transmission. Quantum computer play crucial role in above mentioned structure in microscopic ways. That is, analysis of neurons function and way of transform signal from neuron point to another neuron point and brain internal structure and functioning.

Analysis of DNA Structure

DNA molecular structure is represented by chemical and physical properties. By using this emerging technologies into this, predict molecular structure and its functions. By this, animations and molecular dynamics simulatiuons use for understanding the DNA chemical and physical properties.

Application of Genetic Programming

Genetic programming appears to be a useful tool for exploring the powers of quantum computing. Genetic programming can automatically discover new algorithms for quantum computers. Genetic programming creates three types of genetic programming for quantum computer.

1. Standard tree-based genetic programming.
2. Stach-based linear gnome genetic programming.
3. Stackless linear gnome genetic programming.

Many more application of quantum computer in commercial application as simulation of physical components, mathematical problems solution which yet not solved by conventional computer like operation research some problems viz. feasible solution, infeasible solution, optimum. In Nanotechnology, analysis of minute componenet behaviour and function for maintain accuracy and consistency among components interface.

Conclusion

Quantum cryptography depend on Heisenberg's Uncertainty Principle, no-cloning theorem of quantum mechanics by which secure communication establishes between Alice and Bob without worrying about Eve. That is, light particles behavior and its properties is main concern for communication. Hence it is used in every field as like classical cryptography used today if technology available for implement quantum cryptography. Its commercial application is wide like military, banking, photo detecting voting, quantum internet world etc. Hence, quantum computing appears in wide application as like conventional computer application appears wide today. But quantum computer commercial applications go beyond the limitiation of existing convetional computer in many folds.

REFERENCES

Stallings, W., 1999, Cryptography and Network

Bennett, C. H. and Brassard, G. 1984. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175--179.

Bennett, C. H., and Shor, P. W. 1998. Quantum information theory. IE Information Theory 44, 6, 2724–42.

Brassard, G., Lutkenhaus, N., Mor, T. and Sanders, B. C., 2000. "Limitations on Practical Quantum Cryptography", Physical Review Letters, vol. 85, no. 6, pp. 1330--1333.

Stephen Wiesner, Conjugate coding, ACM SIGACT News, v.15 n.1, p.78-88, Winter-Spring 1983

Brassard, G., Lutkenhaus, N., Mor, T. and Sanders, B. C., "Limitations on Practical Quantum Cryptography", Physical Review Letters, vol. 85, no. 6, 7 August 2000, pp. 1330--1333.

Bennett, C. H., Brassard, G. and Mermin, N. D., "Quantum cryptography with-out Bell's theorem", Physical Review Letters, vol. 68, no. 5, 3 February 1992, pp. 557--559.

Ekert, A. K., "Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, no. 6, 5 August 1991, pp. 661--663.

Bennett, C. H., "Quantum cryptography using any two nonorthogonal states", Physical Review Letters, vol. 68, no. 21, 25 May 1992, pp. 3121--2124.

Ekert, A. K., Rarity, J. G., Tapster, P. R., and Palma, G. M., "Practical quantum cryptography based on two-photon interferometry", Physical Review Letters, vol. 69, no. 9, 1992, pp. 1293--1295.

****