Brief Study of Quantum Cryptography Applications

Bhavesh Prajapati
Assistant Professor, IT Department, L. D. College of Engineering, Ahmedabad, India

ABSTRACT

Quantum cryptography is gaining importance among IT security practitioners day by day. Theory of quantum cryptography is quite sound and its practical implementations are also becoming mature day by day. With mature technology many applications can use quantum cryptography as backbone like secure key distribution, secure direct communications, large prime factorization, e-commerce, e-governance, quantum internet and many more. In this paper we are discussing possibilities of quantum cryptography applications.

Keywords: Cryptography Applications, Quantum Cryptography Quantum Key Distribution Protocol, Quantum Internet, E-Governance, E-Commerce, Space Communication.

I. INTRODUCTION

Quantum information applications for cryptography are more than fifty years old. Wisner has proposed first ever application of quantum physics to quantum cryptography as quantum money and later oblivious transfer, a key concept of today's cryptography.

Quantum theory is more mature than practical implementations. Shor's algorithm and Grover's algorithm have proved classical cryptography can be broken in few seconds as being based on mathematical problems and its computational security. In 1994, Shor proposed a quantum algorithm for integer factorization which reduces time spent on factorization to a great extent. RSA algorithm which previously taking nearly 13 months with latest computational power takes only 1 second to decrypt the encryption.

In 1996, Grover came with algorithm which reduce the searching time from unsorted databases to a great extent. For a dataset of 1024 records, Grover's algorithm which uses quantum properties gives search result just in 32 comparisons. This advances threatens DES and AES security.

Any information system is made secure with cryptographic applications and network security. Quantum cryptography is based on Heisenberg's uncertainty principle and no cloning theorem. Many practitioners are eyeing to quantum cryptography for future proof solutions.

II. METHODS AND MATERIAL

Quantum Key Distribution

Quantum key distribution is also known as QKD in short. Quantum key distribution uses basic microscopic particles known as photon. Alice encodes these photons and then sent to Bob. Eve can intercept such particles over the channel but as per no cloning theorem she can not copy them or duplicate them. When we try to measure any quantum bit, it will change its state. So when Eve try to measure quantum bits, it will generate error in measurements at receiver side. Alice and Bob can calculate QBER- Quantum Bit Error Rate.
Error Rate and can gain knowledge of Eve's learning of information.

The idea of quantum cryptography as quantum money was first coined by Stephen Wiesner in 1970. Bennett and Brassard in 1984 proposed a QKD protocol that was later named the BB84 protocol.

The idea of quantum cryptography as quantum money was first coined by Stephen Wiesner in 1970. Bennett and Brassard in 1984 proposed a QKD protocol that was later named the BB84 protocol.

**III. RESULTS AND DISCUSSION**

**Quantum cryptography applications**

Practical implementation of quantum cryptography is becoming mature day by day. And with advancement in low cost implementations many real world domains are trying to use quantum cryptography applications.

**A. Banking and finance**

Online banking and digital transactions are future of banking and gaining increasing popularity day by day. Quantum cryptography protocols can be used to provide privacy, security and authentication. Bank and customer need to establish an authentic channel which provides unconditional security. Only quantum key distribution can provide unconditional security which is future proof. As we discussed no third party can intercept the communication because of properties of quantum cryptography like no cloning and principle of uncertainty. By using quantum key distribution for key exchange bank can provide high level of unconditional security to customers.

**B. Open space communication and Quantum Internet**

Quantum phenomena of entanglement can be used to carry message securely over long distances. China is planning to launch quantum satellite which in turn make inter continent quantum communication
possible. Success of this project will open the way for quantum internet. Still scientists are facing problems on quantum memory and quantum repeaters. We cannot actually store quantum information so need to work on quantum memory. Furthermore we cannot send quantum signals for long distances. So quantum repeaters required for signal transmission. There is also a requirement to connect classical world of computation to quantum world of computation.

C. E-governance and Secure Voting

Quantum cryptography and key distribution can be used for many government functionalities and can be used for secure election procedures. SSL/TLS protocol is required for any transaction or service required for e-governance. Quantum cryptography need to be embedded to SSL/TLS to upgrade it to next version called QSSL(Quantum SSL). QSSL aims to provide secure communication and unconditionally secure authentication. The same can be efficiently used for voting in elections. This can also be used to provide many services like Government to Government, Government to Business, Government to Citizens and many more effectively.

D. Future E-Commerce

Similarly as discussed for E-governance, quantum cryptography can be applied to E-commerce also. It can be used for business to business (One to one model) or Business to Consumer (One to many model). Quantum cryptography can be used for security, authenticity and non-repudiation.

IV. CONCLUSION

As discussed quantum cryptography can be used for almost all today’s application where security and authenticity are prime concerns. All discussed applications can effectively use quantum cryptography to tighten the security. Still practical implementations of quantum cryptography is lagging for to be used at commercial level. Quantum cryptography is still point to point and hence more appropriate for business to business communication. Not suitable for business to consumer applications.

V. REFERENCES

[6]. Papanikolaou, N., 2004, "Techniques For Design And Validation Of Quantum Protocols"
[8]. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., 2004 , "Quantum cryptography"
[10]. Petra Pajic, 2013, "Quantum Cryptography"
[12]. Bhavesh Prajapati, 2014, Quantum Cryptography: A comprehensive study, IJSRSET