Global Journal of Computer Science and Technology
Cloud & Distributed
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secure Key Distribution using Quantum Cryptography

By S.G.K Murthy, MV Ramana Murthy, M. Shuaib Qureshi, Mohamed Asslam Madathilakath & Mahaboob Sharief Shaik

Osmania University, Hyderabad, India

Abstract - Cryptography plays a vital role in Internet based applications. Present cryptographic systems on classical computers are providing sufficient security by utilizing symmetric and asymmetric cryptographic technologies but the advent invention of quantum computer makes the present asymmetric cryptographic systems vulnerable. The Quantum theory, which makes present cryptographic systems vulnerable, provides an alternative approach for secure key distribution. This paper depicts various issue related to conventional as well as quantum cryptography and secure key distribution using quantum cryptography.

Keywords : cryptography, symmetric, asymmetric, security, key, quantum, photons.

GJCST-B Classification: D.4.6

Strictly as per the compliance and regulations of:

© 2012. S.G.K Murthy, MV Ramana Murthy, M. Shuaib Qureshi, Mohamed Asslam Madathilakath & Mahaboob Sharief Shaik. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction inany medium, provided the original work is properly cited.

Secure Key Distribution using Quantum Cryptography

S.G.K Murthy [α], MV Ramana Murthy [σ], M. Shuaib Qureshi [ρ], Mohamed Asslam Madathilakath [Ѡ]
& Mahaboob Sharief Shaik[¥]

Abstract - Cryptography plays a vital role in Internet based applications. Present cryptographic systems on classical computers are providing sufficient security by utilizing symmetric and asymmetric cryptographic technologies but the advent invention of quantum computer makes the present asymmetric cryptographic systems vulnerable. The Quantum theory, which makes present cryptographic systems vulnerable, provides an alternative approach for secure key distribution. This paper depicts various issue related to conventional as well as quantum cryptography and secure key distribution using quantum cryptography.

IndexTerms : cryptography, symmetric, asymmetric, security, key, quantum, photons.

I. Introduction

Information security is emerging filed in computing. Various security features are attained by using different cryptographic algorithms (symmetric and asymmetric). Present asymmetric cryptographic systems are based on certain hard problems, which cannot be solved in polynomial time. The key length is decided, such a way that it takes exponential time to break the key [1]. With the invention of quantum computers, proved that, it is possible to achieve enormous speed (computation) in solving certain hard problems. As a result current asymmetric cryptographic systems are not proficient of granting absolute security in near future. However the same quantum theory provides an alternative approach for absolute security [3]. This method of distributing, quantum key with the help of quantum physics can provide absolute security to information.

II. Present Cryptographic Systems

Presently there are two types of cryptographic systems available for confidentiality. In symmetric cryptographic systems, single key (secret key) is shared by the sender and recipient. These systems are not useful in large environment [2]. To overcome the with these systems, asymmetric cryptographic systems have been developed. In these systems pair of public and private keys is related mathematically with the property that the private key cannot be derived from public key.

Any information, which is encrypted by a public key, is decrypted only with the corresponding private key. This is a well-known method used by public key cryptographic systems to achieve confidentiality. As asymmetric cryptographic systems are based on very large number based computations and (unlike symmetric cryptographic systems) entire key is used directly in operation, the system becomes slower in encryption and decryption process. So these systems are used for secure key distribution as well as digital signatures.

Secure key distribution problem is solved by asymmetric cryptographic systems. Secret key can be used as a onetime pad. By using asymmetric cryptographic systems users can transmit secret key securely [5].

All asymmetric cryptographic algorithms are depending on a fact that certain mathematical functions can be done easily in one direction but not reverse. These types of functions are called trapdoor one-way functions.

RSA algorithm is a most famous asymmetric cryptographic algorithm that derives its strength from the hard problem, factorization of large composite numbers into two large prime integers. Factorization of very large integers is very difficult further it is exponentially growing, by adding each digit [4]. For a reasonable security, to be achieved, a 1024-bit key size is recommended in RSA cryptographic system. It is realized that for any asymmetric system, the ultimate strength lies on hard problem. Whether the hard problem is prime factorization or discrete logarithm, it takes enormous time for the present classical computers to break the key [6].

Presently, quantum and DNA based computing are newly emerging research areas, which facilitate faster computing. The invention of quantum computer has proved its strength in factorizing very large integers in polynomial time, which makes all asymmetric cryptographic systems vulnerable. To solve this problem, a new way of key distribution by using quantum physics has been proposed. This concept is based on certain fundamental properties of photons,

Author α : Scientist, D.R.D.O, Hyderabad, India.
Author σ : Chairman, Computer Science Department, Osmania University, Hyderabad, India.
Author ρ ¥ : Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Kingdom of Saudi Arabia. E-mail : qureshi.shuaib@gmail.com
Author Ѡ : Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Kingdom of Saudi Arabia.

© 2012 Global Journals Inc. (US)

like quantum entanglement, polarization of photons etc that provides absolute security.

An agreed random sequence of bits generated by quantum cryptography can be used as one time pad cipher, by using existing symmetric cryptographic system.

III. Quantum Physics

Photons (normal light) travel in the space with vibrations. The polarization of photon is the angle of vibration. The angle of vibration may vary in normal light even photons are travelling in the same direction. An un-polarized light is generated by normal light. We are considering four possible polarizations of photons in this paper, which are left, right, horizontal and vertical diagonals [1].

The orthogonal quantum states perception is raised by the two photons with vertical ('V') or horizontal ('H') polarization. 'V' and 'H' photons never pass from the polarizer that is destined for the other photon. Hence both 'H' and 'V' photons are two orthogonal quantum states of a photon [3]. Additionally 'H' and 'V' form a basis for the space of polarizations. Sending an un-polarized light through a Polaroid can generate a light of a particular polarization. The polarization of the polarized light is decided by the axis of the Polaroid.

In classical computers a bit has two logical states either 0 or 1. Unlike classical bits, quantum bits (qbits) can have two values at once. A qbit can exist in a coherent superposition of the two states. so that in quantum computers, one qbit can be encoded as 0 and 1 at any given moment. As L qbits are capable of storing 2^L numbers at time, a quantum computer performs massive parallel computation in a single operation on 2^L different numbers. To achieve the same task, it takes 2^L computations by classical computers. This feature helps quantum computers to factor large integers in polynomial time. Shor's algorithm facilitates efficient factorization of very large numbers by using quantum principles.

We cannot measure every aspect of a particle at the same time. The measuring of one aspect destroys the possibility of measuring the other aspect. This natural uncertainty is used as a concept to generate a secrete key. Further this secret key is used by utilizing symmetric cryptographic systems to achieve absolute security.

Considering the representation of binary numbers by orthogonal quantum states, quantum mechanics provide powerful new methods for information transmission.

IV. Quantum Concepts for Key Distribution

The author [7] states the photon polarization between Bob and Alice. If Alice polarized a photon in a given direction and Bob measured it in the same direction with Polaroid, the Bob acquires the photon with certainty. But random result will be acquired by Bob if he measures it is wrong direction depending upon the probability. So using quantum mechanics, how two parties could agree on a secret key is described as follows.

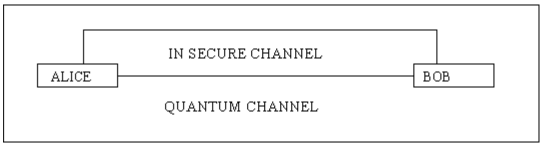

Fig. 1 : Key Distribution

Two communication channels i.e. insecure channel and quantum channel must be used by Bob and Alice for communication as shown in Fig.1.

For quantum bits communication, quantum channel is used, while as for symmetric cryptographic and general encryption, insecure channel is used.

Step 1 – Alice starts communication with the Bob by sending a series of randomly polarized photon.

Assume Alice communicates with the Bob by sending photons in the following polarizations.

| | \ — — \ — | / / | —

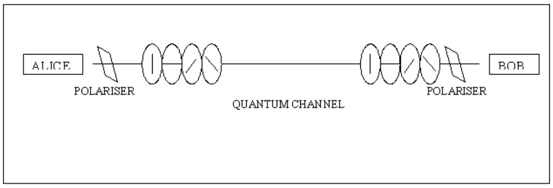

Fig. 2 : Quantum Channel Communication

Step 2 – At the Bob's side, there is a photons detector called as polarizer that detects the photons. For measuring the diagonal polarizations or rectilinear, Bob can amend the polarizer in any one direction. But due to the natural uncertainty of photons, this process is not doable for both.

Suppose Bob adjust his polarizer in the following directions corresponding to each photon.

Z + Z Z + + Z + Z + + Z

If the polarizer setting and the corresponding photon's polarization are matched with each other, then Bob gets the photon through the Polarizer. Suppose Bob acquires the below result,

/ | \ / — | \ | / | | \

Step3 – Now Alice is informed by the Bob about the adopted setting using in-secured channel.

Step4 – Alice notifies Bob which settings are approved.

Step5 – Those polarizations are considered by Alice and Bob who were appropriately measured.

☆ | \ ☆ — ☆ ☆ | / ☆ | ☆

Then the photons polarization measurements are translated into bits using pre arranged code. The below string of bits is generated by translating the above commonly agreed polarizations,

0 0 1 0 1 0

0.5 is the average probability of estimating the correct polarizations. 2n photons are needed by Alice for generating n bits for transmission.

Step 6 – The integrity of the bit string is checked by Alice and Bob using testing.

Step 7- If the integrity test is verified, the same bit string is used as one time pad. Else the above procedure is repeated.

Using the above scheme, Bennet and Brassard proposed an operational model of quantum key distribution. Quantum cryptography provides absolute security by exchanging a series of qbits through fiber optic link.

V. Conclusion

In this paper the factorization issue created by quantum computers and the way that quantum cryptographic system providing a method to achieve absolute secrecy by utilizing quantum key distribution is discussed. Presently quantum cryptography has already been demonstrated by using optical-fiber networks. Over long distance, transmission of polarized photons without the use of fiber optics is proved by the latest experiments, but digital signature is one of the important features, widely used for internet related applications, achieved by asymmetric cryptographic systems. As the invention of quantum computers makes the present asymmetric cryptographic systems vulnerable, there is a need to form a method to create quantum digital signatures. In comparison to classical bit storages, storing quantum states is more difficult and generation and verification of quantum digital signatures requires extensive research in this direction.

References Références Referencias

1. Singh, S. Code, The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography, Doubleday, 1999.
2. Schneier B, Applied Cryptography, John Wiley New York, 2000.
3. Zeilinger, A, Fundamentals of Quantum Information, Physics world, March 1998.
4. William Stallings, Cryptography and Network Security Principles and practices, Pearson Education Ltd, Delhi, 2003.
5. Stinson, D, cryptography: theory and Practice, CRC Press, 2002.
6. Omar M.B, A. Irshad Khan, Mahaboob S. Shaik, MV Ramana Murthy, “Secure Communication using Symmetric & Asymmetric Cryptographic Techniques” I.J. Information Engineering and Electronic Business, pp. 36-42, 2012.
7. SGK Murthy, M.V.Ramana Murthy, P.Ram Kumar, New Trends in Cryptography by Quantum Concepts, Advances in Computer and Information Sciences and Engineering, pp. 428-432, 2008.

© 2012 Global Journals Inc. (US)

This page is intentionally left blank

© 2012 Global Journals Inc. (US)