A Survey on Recent Security Trends using Quantum Cryptography

T. Rubya[1]
Lecturer, Karpagam University,
Coimbatore, India.

N. Prema Latha[2]
Lecturer, Karpagam University,
Coimbatore, India.

B. Sangeetha[3]
Lecturer, Karpagam University,
Coimbatore, India.

Abstract: **Cryptography is the science of keeping private information from unauthorized access of ensuring data integrity and authentication, and it is the strongest tool for controlling against much kind of security threats. Role of cryptography appears in many secured area like government agencies, large banks, telecommunications companies and other corporations who handle sensitive or military data. Quantum cryptography is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. This paper consists of the main aspects of quantum cryptography and it investigates the information about where and all quantum cryptography takes place.**

Keywords- cryptography; photons; quantum key distribution; Protocols;

I. INTRODUCTION

In everyday life there are many situations when it is necessary to conceal the contents of confidential information conveyed over insecure communication line. Classical cryptography techniques have proved very helpful for this task. However, nearly all these techniques are merely computationally secure, that is they rely on limited advancement of computer power, technologies and mathematical algorithm in these foreseeable future. The construction of quantum cryptography can seriously threat their security. In the recent past, there has been a good deal of a new cryptographic method whose security is based on the fundamental laws of quantum physics, quantum cryptography. The main achievement is that it can solve the problem of key distribution. From the practical point of view, it is interesting that quantum cryptography may appropriately be realized by means of quantum optics and the optical fiber serves as a transmission channel. To encode information for example polarization (divergence, division) or phase can be used.

II. KEY DISTRIBUTION PROBLEM

Classical Cryptography suffers from Key Distribution problem, how to communicate the key securely between two pair of users. For years, it was believed that the only possibility to solve the key distribution problem was to send some physical medium – a disk for containing the key. In the digital era, this requirement is clearly unpractical. In addition, it is not possible to check whether this medium was intercepted – and its content copied – or not. Public key cryptography came as a solution to this, but these too are slow and cannot be used to encrypt large amount of data. Public key cryptography suffers because even though one way functions have not been yet reversed with technological and mathematical advances it is possible[1].

A. Quantum Key Distribution

The very efficient encryption algorithms exist and some have been proved to be unbreakable by Shannon's information theory. For instance, Vernam cipher, also called the one-time pad, assumes that two endpoints share a key as long as the message to be encrypted. Vernam encryption is just doing an XOR, i.e., addition modulo 2, between the clear message and the encryption key. The corresponding decryption is also performed by doing an XOR, but between the encrypted message and the encryption key. Reading the encrypted message does not give any information about the clear message. However, the required length of key, and the fact that the encryption key must be changed after each use, rule out Vernam cipher for an everyday usage. The modern Data Encryption Algorithms (DEAs) such as 3-DES, AES, and elliptic curves cryptosystems allow to have a good secure encryption using fixed-length keys[2][3]. They are considered as "unbreakable". But all these algorithms assume that a key is shared between the two endpoints. Thus, security is a problem of key distribution.

II. ELEMENTS OF QUANTUM THEORY

Light waves are made up of millions of discrete quanta called Photons. They are mass less and have energy, momentum and angular momentum called spin. Spin carries the polarization. These photons are indivisible much like Atoms it just that they are units of lights. Photons can be polarized from 0^o to 360^o and intermediate spin positions like 45^o or 90^o can be detected using filters inclined to certain directions.

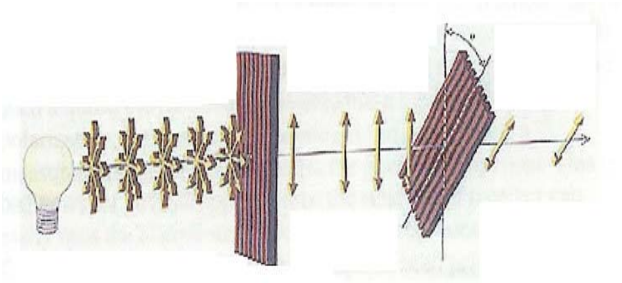

Fig 1. Polarization of Light

Fig 1 Polarization of Light In 1 we can see that light from a bulb passes through a polarization filter with is inclined to 90^0 so we get vertical ray of light out of it, if we place another filer that is inclined differently rays are again rotated. If the rays are at orthogonal angle to the filter we will get no output[6]. The advantage of this kind of polarized light is that once we pass the light through 2nd filter we don't know what the orientation of light rays was after 1st filter. So in that channel privacy is maintained.

IV. QUANTUM COMMUNICATION

In telecommunication networks, light is routinely used to exchange information. For each bit of information, a pulse is emitted and sent down an optical fiber – a thin fiber of glass used to carry light signals – to the receiver, where it is registered and transformed back into an electronic signal. These pulses typically contain millions of photons. In quantum cryptography, one can follow the same approach, with the only difference that the pulses contain only a single photon. A single photon represents a very tiny amount of light (when reading this article your eyes register billions of photons Quantum cryptography solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. This key can then be used with conventional cryptographic algorithms.

Quantum Communication is based on two features of Quantum mechanisms and photons

- State indeterminacy based on Heisenberg principle
- Entangled based protocols that mean two entities can be defined such that their properties are entangled altering one effect the value of other. If an entangled object like a key is shared between two parties it maintains integrity of the key

A. *Heisenberg Uncertainty Principle*

For any two observable properties linked together like mass and momentum

$$\langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq \frac{1}{4} \| \langle [A, B] \rangle \|^2 ,$$

where

$$\Delta A = A - \langle A \rangle \quad \text{and} \quad \Delta B = B - \langle B \rangle ,$$

and where

$$[A, B] = AB - BA.$$

According to the principle two interrelated properties cannot be measured individually without affecting the other. The principle is that since you cannot partition the photon into two halves measuring the state of photon will affect it value. So if someone tries to detect the state of photons being send over to the receiver the error can be detected[9].

B. *Qubits*

The most important unit of information in computer science is the *bit*. There are two possible values that can be stored by a bit: the bit is either equal to "0" or equal to "1." These two different states can be represented in various ways, for example by a simple switch or by a capacitor: if not charged, the capacitor holds the value zero; if charged, it holds the value one.

V. QUANTUM KEY DISTRIBUTION – BB84 PROTOCOL

Each photon carries one "qubit" of information. Polarization can be used to represent a 0 or 1. A user can suggest a key by sending a stream of randomly polarized photons. This sequence can be converted to a binary key. If the key was intercepted it could be discarded and a new stream of randomly polarized photons sent. This protocol, known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information. However, any two pairs of conjugate states can be used for the protocol, and many optical fibre based implementations described as BB84 use phase encoded states

Now the steps of the protocol are as follows.

- Alice communicates with Bob via a quantum channel sending him photons.
- Then they discuss results using a public channel.
- After getting an encryption key Bob can encrypt his messages and send them by any public channel.
- One with the 0-90 degree basis and one with 45-135 degree basis .

- Alice uses her polarizer's to send randomly photons to Bob in one of the four possible polarizations 0, 45, 90,135 degree.
- Bob uses his polarizer's to measure each polarization of photons he receives.
- He can use the basis or but not both simultaneously.

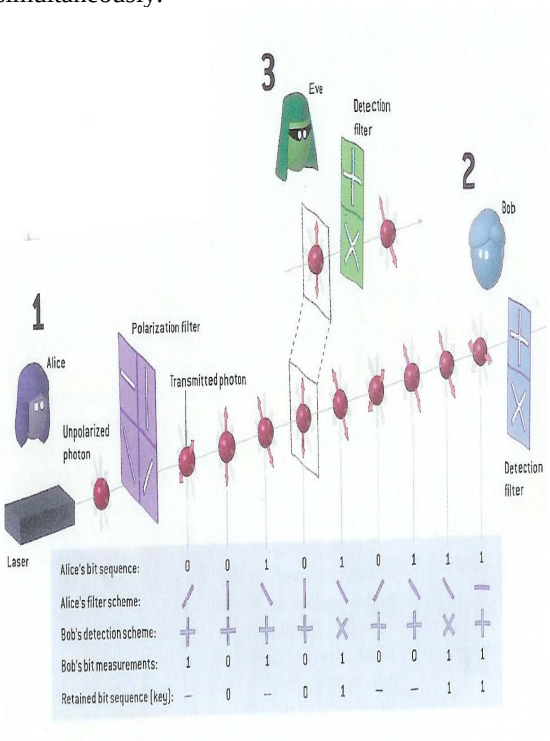

Fig 2. Quantum Communication

The quantum cryptography will put to practical use on many places like ATN, video conferencing, finance and life science, which required advanced information security[12].

VI. AGT TELECOMMUNICATION SECURITY USING QC

Aeronautical Telecommunication Network (ATN) is the network used by the Air Traffic Authorities, the Air raffic Controllers (ATCo), the aircrafts and all Ground Stations (GS) to communicate voice and data[19]. And how the ATN can be secured by using Quantum Cryptography (QC), either fiber-based QC or free-space QC, instead of classical PKI. ATN is a good example of special-purpose dedicated networks that could be secured by QC.

The security of ATN is a crucial matter. For instance, Aircraft Communications And Reporting System (ACARS) Data Link (DLK) must be secured. Inter Domain Routing Protocol (IRDP) must be secured too. Airlines companies require secrecy too for economic reasons. ATN may be secured by using classical cryptography, which provides the so-called cryptographic security. Such security is based on the assumed but unproven intractability of some mathematical problems related to prime numbers or elliptic curves. Quantum Cryptography (QC) provides unconditional security relying on the quantum physics law. Such a security is called information theoretic security because it is proved by Shannon's theory of information. However, any solution for improving the planned security of ATN must be done inside the framework of ATN. It must take into account the existing infrastructure and the developing costs of new solutions. The existing infrastructure must be re-used. And any proposed solution that uses QC to secure ATN must be incremental.

VII. VIDEO CONFERENCING VIA QUANTUM CRYPTOGRAPHY

If we are working for a company and that we have to routinely discuss about Sensitive Future projects or the possible acquisition of another company, we need more security, and this new video conferencing system based on quantum cryptography is a tool we need. Accordingly, the researchers from Toshiba have developed a system which can generate 100 quantum 'keys' every second, fast enough to protect every frame in a video exchange. This technology, which today is working over a distance of about 120 kilometers, could become commercially available within two years at an initial cost of $20,000.(National Security Anarchists (hacker group)

This system is capable of generating 100 quantum 'keys' every second. This is fast enough for every individual frame of video to be protected by its own encryption. "This makes the system highly secure," says Andrew Shields, who leads the Cambridge team. "It would take an enormous computational resource to crack this frame by frame."

A. Limitations of classical Quantum Cryptography

Quantum cryptography, usually known as Quantum Key Distribution(QKD) provides powerful security. But it has some limitations. Following no-cloning theorem , QKD only can provide 1:1 connection. So the number of links will increase N(N-1)/2 as N represents the number of nodes. If a node wants to participate into the QKD network, it will cause some issues like constructing quantum communication line. To overcome this issues, SECOQC was started.

VIII. SECOQC NETWORK

A. Brief architecture of SECOQC network

SECOQC network architecture can by divided by two parts. Trusted private network and quantum network consisted with QBBs(Quantum Back Bone). Private network is conventional network with end-nodes and a QBB[25]. QBB provides quantum channel communication between QBBs. QBB is consisted with a number of QKD devices that are connected with other QKD devices in 1-to-1 connection.

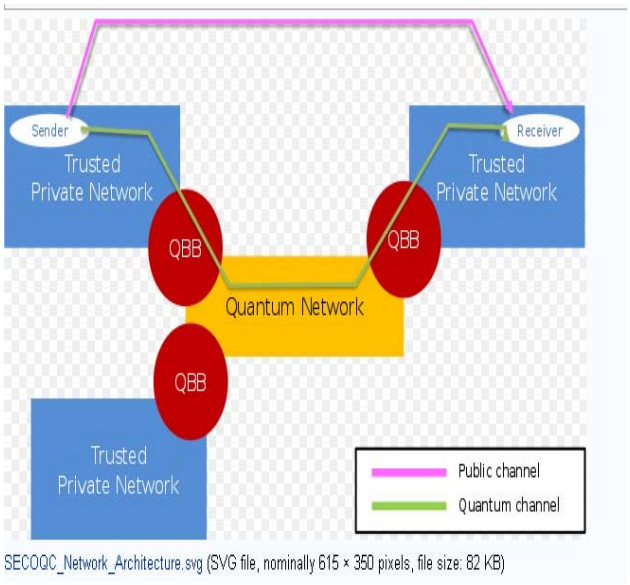

Fig 3. SECOOC Networl Architechture

From this, SECOQC can provide easier registration of new end-node in QKD network, and quick recovery from threatenings on quantum channel links.

SECOQC will provide the basis for long-range high security communication in a network regime that combines the entirely novel technology of quantum key distribution with solutions from classical computer science, network design and cryptography.

VIII. DEVICE FOR QUANTUM CRYPTOGRAPHY

One company named Fujitsu laboratories Ltd has been studying the advanced single-photon technology. They are developing technologies that improve the performance of single photon source.

In order to achieve quantum cryptography, a single-photon source that can limit the number of photon included in single pulse to one is needed. However the attenuated laser light was used in the experiment on the quantum cryptography of the past because the generation of the single photon at the wavelength used for the optical fibre communication is very difficult[19]. It was necessary to communicate at the remarkably slow speed to decrease the possibility of two-photon occurrence in the laser pulse. So the company has developing new technologies to improve the performance of single photon source.

And they have obtained the basic technology that enables the quantum cryptography with 100 kbps by demonstrating single photon source with the extraction efficiency of more than 10% at the wavelength of 1.55 micrometer. The main aim of this company is to demonstrate the quantum cryptography with the single photon source in near future by developing the mounting and the cooling technologies of the device that enables a downsizing and stable operation of the system.

X. CONCLUSION

Hence quantum cryptography is a new technology; it is surprisingly easy to integrate. The last three years have seen dramatic advances in experimental quantum cryptography systems and several companies have developed quantum cryptography prototypes because it is uncompromisingly secure key distribution, faster key refresh rate (than traditional approaches), truly random key generation, unconditional eavesdropping protection, proactive intrusion detection, lower total cost of ownership, future proof security, speedy set-up, with virtually zero maintenance. Thus Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology.

REFERENCES

[1] Gábor Erdé Lyi, Tim Meyer, Tobias Riege, And Jö Rg Rothe Quantum Cryptography: A Survey Dagmar Bruss, ACM Computing Surveys, Vol. 39, No.2, Article 6, Publication date: June 2007

[2] ICAO, “Manual of technical provisions for the aeronautical telecommunications network (atn) - standard and recommended practices (sarps),” Mars 2001.

[3] B. Witulski, “Key management,” in *Presentation at DLK Users Forum*, Brussels, Belgium, June 1995.

[4] J. McMath, “Aeronautical telecommunication network(atn): Security, key management and distribution security, key management and distribution,”in *AEEC Data Link Users Forum and ESC/GAD, Titan Corporation, Public Release: 03-0052 edition*, Hanscom, MA, USA, February 2003.

[5] C. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, 1984, pp.175–179.

[6] C. Bennett, F. Bessettee, G. Brassard, L. Salvail, and J. Smolin,“Experimental quantum cryptography,” September 1991.

[7] N. Gisin and al, “Quantum cryptography,” *Reviews Modern Physics*,vol. 74, pp. 145–195, January 2002.

[8] C. Elliott, “Building the quantum network,” *BBN Technologies (USA)*, June 2002.

[9] M. D. Dang and M. Riguldel, “Usage of secure networks built usingquantum technology,” 2004.

[10] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, “Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptographycriterion,” *Submitted to Electronics Letters*, 2004.

[11] W. T. Buttler and al, “Practical free-space quantum key distribution over 1km,” *Phys. Rev. Lett.*, vol. 81, pp. 3283–3286, 1998

[12] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, “Practical free-space quantum key distribution over 10 km in daylight and at night,”*New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[13] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity,and H. Weinfurter, “Long distance free-space quantum cryptography,”*In New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[14] Elliott, Chip. “Quantum Cryptography”, IEEE Security & Privacy, 2004

[15] D. Gottesman and H.-K. Lo, “Proof of security of quantum key distribution with two-way classical communications,” September 2002.

[16] D. Mayers, “Unconditional security in quantum cryptography,” *JACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[17] H. Inamori, N. L¨utkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," July 2001.
[18] Quoc-Cuong Le, Patrick Bellot "Enhancement of AGT Telecommunication Security using Quantum Cryptography" published in IEEE Research, Innovation and Vision for the Future International Conference. pp .7 – 16, Feb 2006.
[19] H.-K. Lo, "Communication complexity and security of quantum key distribution," April 2004.
[20] H.-K. Lo and H. Chau, "Unconditional security of quantum key distribution over abitrarily long distance," *Science*, pp. 2050–2056, 1999.
[21] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," April 2004.
[22] C. Guenther, "The relevance of quantum cryptography in modern cryptographic systems," December 2003.
[23] P. Bellot, M. D. Dang, and H. Q. Nguyen, "A new authentication scheme for quantum key distribution," 2004.
[24] D. L. A. H. Committee, "Ad hoc meeting on security, executivesummary for aeec general session 2002 membership," *ESC/GAD, Titan Corporation (Hanscom, MA, USA)*, May 2002.
[25] M. Pfennigbauer, W. R. Leeb, M. Aspelmeyer, T. Jennewein, and Zeilinger, "Free-space optical quantum key distribution using intersatellite link," November 2003.
[26] http://ec.europa.eu/research/fp6/index_en.cfm?p=0
[27] http://en.wikipedia.org/wiki/ Quantum_cryptography
[28] http://www.aip.org/tip/INPHFA/vol-10/iss-6/p22.html
[29] http://www.perimeterinstitute.ca/personal/dgottesman/QKD.html
[30] http://www.cs.brandeis.edu/~pablo/qbc/node4.html