ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

The Quantum Cryptography for Efficient Communication in Wireless Network

Kapil Vaidya [1], Shubhada Mathapati[2], Dipak V Ingle[3]

UG Student, Department of Computer Science and Engineering, Sanmati Engineering College, Washim, Maharashtra, India[1]

UG Student, Department of Computer Science and Engineering, Sanmati Engineering College, Washim, Maharashtra, India[2]

Assistant Professor, Department of Computer Science and Engineering, Sanmati Engineering College, Washim, Maharashtra, India[3]

ABSTRACT: Cryptography provides security for the information and personal details. Quantum cryptography is an approach to securing communications by applying the phenomena of quantum physics. Quantum cryptography is a new method for secret communications offering the ultimate security assurance of the inviolability of a Law of Nature. Unlike traditional classical cryptography, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography is focused on the physics of information. The combination of 3AQKDP (implicit) and 3AQKDPMA (explicit) quantum cryptography is used to provide authenticated secure communication between sender and receiver. The uses of computer communications networks technologies have increased the incidents of computer abuse. Because of these incidents, most organizations facing pressure to protect their assets. Most digital networks generally rely on modern cryptosystems to secure the confidentiality and integrity of traffic carried across the network. The current modern cryptosystems based on mathematical model introduce potential security holes related to technological progress of computing power, the key refresh rate and key expansion ratio, the most crucial parameters in the security of any cryptographic techniques. For that reason efforts have been made to establish new foundation for cryptography science in the computer communications networks. “I am fairly familiar with all forms of secret writings, and am myself the author of a trifling monograph upon the subject, in which I analyse one hundred and sixty separate ciphers; but I confess that this one is entirely new to me. The object of those who invented the system has apparently been to conceal that these characters convey a message ...”

KEYWORDS: Quantum cryptography, Security Quantum, hacking.

I. INTRODUCTION

It is a process of protecting information by converting the information into unreadable format known as cipher text. It can be converted into readable format if and only if proper secret key is entered then only it can decrypt. Encryption is a process converting of original data (called plain text) into unintelligible form by means of reversible translation i.e. based on translation table or algorithm, which is also called enciphering. Decryption is the process of translation of encrypted text (called cipher text) into original data (called plain text), which is also called deciphering. This is the meaning of the term cryptography. In this paper we shall review the theory of quantum cryptography, its potential applications and the development of an experimental prototype at Los Alamos. We shall answer the questions: What is “quantum” about quantum cryptography? Why we need it? Or, is there if anything is “wrong” with conventional cryptography? What are the limitations imposed by “practical” issues such as losses and noise? What are the prospects for future improvements? What hardware developments are desirable? And, what kind of secure communications problem could it is used for? The two main goals of cryptography are for a sender and an intended recipient to be able to communicate in a form that is unintelligible to third parties, and for the authentication of messages to prove that they

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

were not altered in transit. Both of these goals can be accomplished with provable security if sender and recipient are in possession of shared, secret "key" material.

II. RELATED WORK

Alfred Jo De Santk et.al has proposed visual cryptography schemes in which two pixels combine in XI arbitrary way and analyse the pixel expansion and the contrast of *(2,* n)-threshold visual cryptography schemes. In this scheme, any pair of n shares can visually reconstruct the secret image, but any single share has information on the secret image.

Author considered all the possible ways to perform pixel sharing and expansion under contrast analysis**.** Chin-Chen Chang et.al [2] has presented a visual cryptography scheme for color image hiding. By means of little additional computations, it goes through a color index table to hide and recover a secret image. A secret color image hides itself in two arbitrary color images, which can be constructed and then are kept by two participants, separately. This paper proves that only one of the two camouflage color images cannot reveal the secret image. Thus, the hidden information is recurred. In sharing and recovering a secret image, very small memory space and simple computations are required, and that indeed deserves today's common mobile communication platform. Chin-Chen Chang et.al [3] Has proposed colored visual cryptography schemes based on modified visual cryptography. By means of a few additional computations, users can hide a colored secret image into some shares. However, the size of the shares and the implementation complexity in these schemes depend on the number of colors appearing in the secret image. Author defined a work on secret color image generation using visual cryptography. The size of the shares is fixed; it does not vary when the number of colors appearing in the secret image differs. Since the newly proposed scheme has the advantage of low computation and avoids the drawbacks mentioned in the previous approach, it is indeed suitable for today's requirement of low power. Stelvio Cimato et.al [4] has defined an effective Visual cryptography scheme that allow the encoding of a secret image into *n* shares which are distributed to the participants, such that only qualified subsets of participants can "visually" recover the secret image. In colored threshold visual cryptography schemes the secret image is composed of pixels taken from a given set of c colors. This paper shows the c-color (k, n)-threshold visual cryptography schemes and provides a characterization of contrast-optimal schemes. Constructive proof of optimality, with respect to the pixel expansion, of c-color *(n, n)* -threshold visual cryptography schemes. Author has defined a construction method for c-color *(n,* n)-threshold schemes. Indeed, once we have fixed an arbitrary value for p (p, n), and finally gives the values for all other multiplicities of the scheme. Zhi Zhori and Gonzalo et.al
[5] Has proposed the method of Visual cryptography that encodes a secret image SI into n shares of random patterns. If the shares are Xeroxed onto transparencies.

III. TEXT IN PAINTING

Key authenticity: only the centre can generate a session key.
Data authenticity: the users can distinguish among the data sent by the centre and the malicious data sent by an attacker. In the communication network the Key Distribution is used by providing sharing secret session keys between users. By using these shared secure keys we can have a secure communications over insecure networks. Trusted centre (TC) is in some cases users establish a verifies the secured keys and allow access these condition is called three party where we have two users and one trusted center.

Classical Cryptography
Cryptography is the art of rendering a message unintelligible to any unauthorized party. Although example or application of cryptography is the confidentiality, it is used nowadays to achieve broader objectives, such as authentication, digital signatures.
These classical cryptosystems come in two flavours: symmetric systems, and asymmetric systems [The security of public key cryptosystems is based on computational complexity. The idea is to use mathematical objects called one-way functions. So far, no one has proved the existence of any one-way function with a trapdoor; so, the existence of secure asymmetric cryptosystems is not proven.
This poses a serious threat to these cryptosystems. For instance, an overnight breakthrough in mathematics could make

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

electronic money instantly worthless. To limit such economic and social risks, there is no alternative but to turn to symmetrical cryptosystems. QC has a role to play in such alternative systems.

Asymmetrical (public-key) cryptosystems

Depending on whether Alice and Bob use the same key Cryptosystems come in two main classes. Asymmetrical systems involve the use of different keys for encryption and decryption. They are commonly known as public-key cryptosystems. Their principle was first proposed in 1976 by Whitfield Diffie and Martin Hellman, who were the nat Stanford University in the US. Ronald Rivest, AdiShamir, and Leonard Adleman of the Massachusetts Institute of Technology in 19784 whose are the first actual implementation were then developed. It is known as RSA and is still widely used. If Bob wants to be able to receive messages encrypted with a public key cryptosystem, he must first choose a "private" key, which he keeps secret. Then, he computes from this private key a "public" key, which he discloses to any interested party. Alice uses this public key to encrypt her message. She transmits the encrypted message to Bob, who decrypts it with the private key. Public-key cryptosystems are convenient and they have thus become very popular over the last 20 years. The security of the internet, for example, is partially based on such systems. They can be thought of as a mailbox, where anybody can insert a letter. By opening his private key the legitimate owner can then recover it.

This form of encryption makes use of one public key which is available to all users and a private key which is known only by the message recipient. The public key can be exchanged between users who can use it to encrypt data being transmitted to another user, the private key which should be kept secret, is used to decrypt the encrypted data to produce the original unencrypted data. This form of key cryptography is used by the rivets, Shamir, and Adleman (RSA) encryption algorithm.

Symmetrical (secret key)

For encryption and decryption Cryptosystems Symmetrical ciphers require the use of a single key. The symmetrical cryptosystems in use for routine applications such as e-commerce employ rather short keys. Like asymmetrical cryptosystems, they offer only computational security. However, for a given key length, symmetrical systems are more secure than their asymmetrical counterparts.

This form of encryption is also known as the secret key cryptography. Symmetric key cryptography makes use of the same private key while performing an encrypted communication between two users. The same secret key is used for the encryption and decryption of data being transmitted between the two or more users. This form of cryptography makes use of stream ciphers and block ciphers for encrypting plain text. A stream cipher is an encryption method that is used to encrypt plain text or digits one character at a time while block ciphers encrypts blocks of data. Symmetric Key cryptography example is the Data Encryption Standard (DES) algorithm.

Barriers of Classical cryptography

Secret key cryptography

- For key distribution we can requires secure channel.
- Every classical channel can be monitored passively in the principle.
- The complicated non proven algorithms which is used for providing the mostly security.

Public key cryptography

- Also non- proven mathematical assumptions (e. g. in RSA cipher, difficulty of factoring large numbers) useful for providing security.
- The renders messages insecure retroactively through break.

.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

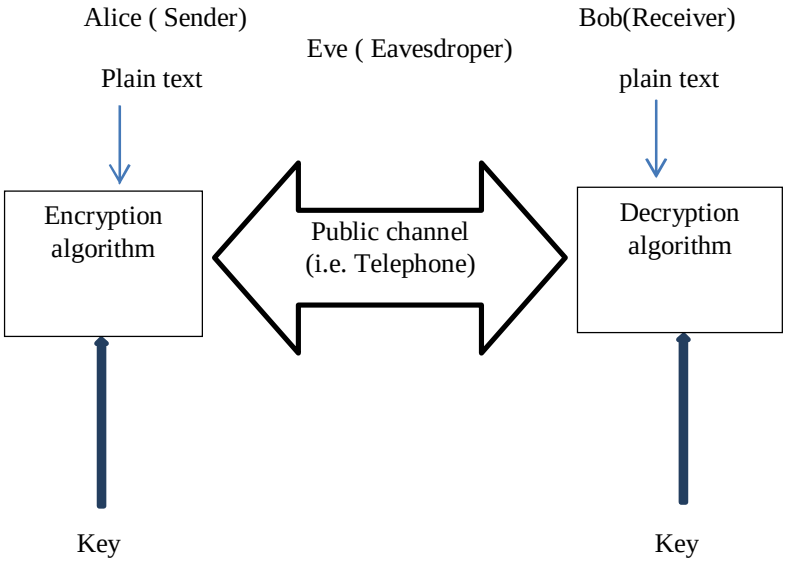

Fig. A quantum cryptographic communication system for securely transferring random key

Quantum key distribution

The Quantum cryptography provides a surprisingly elaborate suite of specialized protocols, which we term "QKD protocols." The QDK the first move away from the traditional key distribution metaphor of Alice sending particular key data to Bob for understand it. Instead , we should have in mind a more symmetrical starting point, in which Alice and Bob initially generate their own, independent random number sets, than they need for the key material that they will ultimately share we can need more numbers. Next, they compare these sets of numbers to distil a shared subset, which will become the key material. It is most important to appreciate that they do not need to identify all of their shared numbers, or even particular ones, because the only requirements on the key material are that the numbers should be random and secret. They can attempt to accomplish a secret distillation if Alice prepares a sequence of tokens, one kind for a "0" and a different kind for a "1", and sends a token to Bob for each bit in her set. Bob proceeds through his set bit-by-bit in synchronization with Alice, and compares Alice's token with his bit, and replies to Alice telling her whether the token is the identical as his number (but not the value of his bit). With Bob's information Alice and Bob can identify the bits they have in common. They keep these bits, forming the key, and discard the others. If in case of Alice's tokens fails to reach Bob this does not spoil the procedure, because it is only tokens that arrive which are used in the distillation process.

QKD is a means of distributing keys from one party to another, and detecting eavesdropping. QKD is allows two parties to establish a common random secret key by taking advantage of the fact that quantum mechanics does not allow for distinguishing non-orthogonal states with certainty. Within the framework of classical physics, information encoded into a property of a classical object, can be acquired without affecting the state of the object. However, in that case if information is encoded into a property of a quantum object, any attempt to discriminate its non-orthogonal states inevitably changes the original state with a nonzero probability and since eavesdropping is also governed by the laws of quantum mechanics, these changes cause errors in transmissions and reveal the eavesdropper. It enables legitimate users to discover it but QKD cannot prevent from eavesdropping, If any eavesdropping is detected, the key is simply thrown away and a new one is One class of proofs, by Dominic Mayer's and subsequently by others, including Eli Biham and collaborators and Michael Ben-Or, attacks the problem directly and proves that the standard BB84 protocol is secure. Another approach, by (HKL) and H. F. Chau. The security of a new QKD protocol that uses quantum error-correcting codes and the various algorithms. The two approaches have been unified by Peter Shor and John Preskill, who showed that a quantum error-correcting protocol could be modified to become BB84 without compromising its security.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

Quantum Cryptographic Protocols

Recent interest has been stimulated by the fact that quantum algorithms in quantum cryptography, such as Shor's algorithms cryptographic protocols for key distribution, oblivious transfer and other problems have been extensively studied, bit commitment. Furthermore, the implementation of make a quantum digital signature, which is secure against all attacks allowed by quantum mechanics. For integer factorization and discrete logarithm, threaten the security of classical cryptosystems.

Eavesdropping

Eavesdropping is the intercepting and reading of messages and conversations by unintended recipients. One who participates in eavesdropping, i.e. someone who secretly listens in on the conversations of others, is called an eavesdropper. The origin of the term is literal, from people who would literally hide out in the eaves of houses to listen in on other people's private conversations.

Telephone lines, email, instant messages, and any other method of communication considered private can also be done with the help of eavesdropping. (If a message is publicly broadcast, witnessing it does not count as eavesdropping). Messages can be protected against eavesdropping by employing a security service of confidentiality (or privacy). This security service is usually implemented by encryption. An also be done over telephone lines, email, instant messages, and any other

Quantum channels

"Quantum channel" connected through the single photon source and the detectors. Such a channel is actually nothing especially quantum, except that it is intended to carry information encoded in individual quantum systems. Here "individual" doesn't mean "non- decomposable", it is meant in opposition to "ensemble".

The idea is that the information is coded in a physical system only once, contrary to classical communication where many photons carry the same information. Note that the present day limit for fiber-based classical optical communication is already down to a few tens of photons, although in practice one usually uses many more. With the increasing bit rate and the limited mean power – imposed to avoid nonlinear effects in silica fibres – these figures are likely to get closer and closer to the quantum domain.

Applications

1. Quantum Cryptography provides the applications as any e-mail message, telephone call, or financial transaction encrypted with these keys will be safe.
2. How can you protect your data from a quantum computer? Answered as you have to fight fire with fire using encryption based on quantum mechanics, quantum cryptography.

Advantages

1. The biggest advantages of public key cryptography are secure nature of the private key. In fact, it never needs to be transmitted or revealed to anyone with the help of using various algorithms.
2. It enables the use of digital timestamp and digital certificates and also which is a very secure technique of signature authorization.
3. The Quantum Cryptography is easy to handle.
4. It keeps your privacy is safe and hides your private message.

Weaknesses and Limitations of Q.C

1. Only works along unbroken and relatively short fiber optic cables. Record as of March, 2004 is120 km.
2. The weakness of this technics is that it doesn't solve authentication problem.

IV. CONCLUSION

In this research paper we can conclude that quantum cryptography developments promise to address some of the problems that plague classical encryption techniques such as the key distribution problem and the predicted breakdown of the public/private key system. Quantum cryptography operates on the Heisenberg uncertainty principle and random

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 3, March 2018

polarization of light. Another purely theoretical basis involves EPR entangled pairs.
Due to the high cost of implementation and the adequacy of current crypto logical methods, it is unlikely that quantum cryptography will be in widespread use for several years and also it provides the secure communications.

REFERENCES

3. C. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
4. A. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett. 67, 661 (5 August1991).
5. Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation –Oxford University. Conger. S., and Loch, K.D. (eds.). Ethics and computer use. Common. ACM 38, 12 (entire issue).
6. Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov.2002.
7. Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.
8. C. Elliott, "Building the quantum network," New J. Phys. 4 (July 2002) 46.
9. Pearson, David. "High! Speed QKD Reconciliation using Forward Error Correction." Quantum Communication, Measurement and Computing. Vol. 734. No. 1. AIP Publishing, 2004.
10. Curcic, Tatjana, et al. "Quantum networks: from quantum cryptography to quantum architecture." ACM SIGCOMM Computer Communication Review 34.5 (2004): 3-8.
11. Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." Physical Review Letters 85.2 (2000): 441.
13. Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." Optics Express 12.9 (2004): 2011-2016.