International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2015 Volume 2, Issue-3
Email: editor@ijermt.org www.ijermt.

Enhancement of Security when Photon Invalidates Encryption using Quantum Cryptography

Madan Kumar
Assistant Professor
Department of Information Technology
SRM University, NCR campus, Modinagar, India

ABSTRACT-
Security is not something extra, but it is something essential. That is where cryptography comes along. Cryptography is the science of transmitting information while protecting the content from being understood by unintended recipients, thus, providing security of the information. The most basic problem in cryptography is establishing a secret key between two parties that have no previous common information, in the presence of an eavesdropper.
Behind the scenes, classical cryptographic technologies underpin a great deal of the security that we take for granted but the main problem with the classical cryptography is that hardness of underlying mathematical problems hasn't yet been strictly proven. This means that one day someone could invent better algorithms for factoring and finding discrete logarithms and that the whole cryptography would collapse instantly. Yet with ever more powerful computers called **quantum computers**, the encryption and decryption methods that underpin secure communications are under threat. Since Moore's law predicts the doubling of transistor density every 18 months it will become increasingly easy to break cryptographic keys as computational power doubles. Till now, popular methods like DES, AES and RSA which can be mathematically cracked in a duration of universe's age, have been proposed. But all of these methods future is at risk because of the studies in production of "Quantum Computers" of which computation speed is estimated to be very high so that no other existing super computers compete with them.With the threat of quantum computing shattering the protection that current encryption schemes had come to provide, it isn't a surprise that scientists shifted to a new focus for unbreakable security: **Quantum Cryptography.** Quantum cryptography is a new method for secret communications offering the ultimate security assurance of the inviolability of a Law of Nature. In this paper we shall describe the limitations of existing cryptography techniques used, along with the benefits of the **Quantum Cryptography.** Quantum cryptography is a set of cryptographic primitives which rely on laws of quantum physics rather than on unproven mathematical puzzles. Quantum key distribution(QKD), a more appropriate name for Quantum Cryptography, is a method to establish a (highly) secret key between two communicating parties which do not share a secret initially. Should an eavesdropper, spy on their communication, the laws of quantum physics stipulate that leakage of information will affect the quantum bit error rate. This alerts the two parties that their communication has been compromised. Thus it can be concluded, QKD is 'unconditionally secure,' meaning that eavesdropper can use all present and future technologies to devise his/her measurement apparatus (including quantum computers, digital computers, and perfect software algorithms) and still not be able to break QKD.

KEYWORDS: Quantum-Cryptography, AES, DES, Photon

INTRODUCTION

Here, we shall answer the questions: Will we need Quantum Cryptography? or, what if anything is "wrong" with conventional cryptography?

'**Cryptology**'(Greek term for 'cryptography'), the mathematical science of secret communications, is becoming more and more important in everyday life.

MANUSCRIPT DETAILS:L

With the growth of computer networks for business transactions and communication of confidential information there is an ever increasing need for encryption to ensure that this information cannot be acquired by third parties. 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 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. Thus, key material, which is a truly random number sequence, is a very valuable commodity even though it conveys no useful information itself. One of the principal problems of cryptography is therefore the so-called "**key distribution problem."**How do the sender and intended recipient come into possession of secret key material while being sure that third parties ("eavesdroppers") cannot acquire even partial information about it? It is provably impossible to establish a secret key with conventional communications, and so key distribution has relied on the establishment of a physically secure channel ("trusted couriers") or the conditional security of "difficult" mathematical problems in public key cryptography. Thus, it compels us:

1. To rely on the trusted third parties for key distribution, in case of conventional cryptographic systems, who, however may provide to the intruders for eaves dropping.
2. And, to rely on the insolvability of conditional mathematical security in case of public key cryptographic systemswhich is not a big deal now through Quantum Computing.However, provably secure key distribution becomes possible with quantum communications. It is this procedure of key distribution that is accomplished by **quantum cryptography**, and not the transmission of an encrypted message itself. Hence, a more accurate name is **quantum key distribution (QKD).**

The most obvious security feature of QKD is that it is impossible to "tap" single quantum signals in the conventional sense. At a deeper level, QKD resists the interception and retransmission by an eavesdropper because in quantum mechanics, in contrast to the classical world, the result of a measurement cannot be thought of as revealing a "possessed value" of a quantum state. Moreover, Heisenberg's uncertainty principle ensures that the eavesdropper's activities must produce an irreversible change in the quantum states ("collapse of the wave function") before they are retransmitted to the intended recipient. These changes will introduce an anomalously high error rate in
the transmissions between the sender and intended recipient, allowing them to detect the attempted eavesdropping.

Thus, the two important security features of QKD are that eavesdroppers cannot reliably acquire key material, and any attempt to do so will be detectable.

The remainder of this paper is organized as follows. In Sections 3 and 4 we introduce the different efforts exist to solve the 'key distribution' problem, how Quantum Computing provides a better solution than these efforts and how it works? The following sections include evaluating the degree of how much better quantum computing is, than other solutions.

RELATED WORK

In modern "secret key," or "symmetric" cryptosystems, the general nature of the encryption algorithm, E, by which a plaintext message, P, is rendered into a cryptogram, C, can be publicly known, because in any particular communication it depends on a parameter, known as a "key", K, which is a secret shared only by the sender (known generically as "Alice") and intended recipient (known as "Bob"). Thus, Alice generates the cryptogram

$$\mathbf{C = E_k(P)\ ,}$$

and sends it to Bob, who decrypts it

$$\mathbf{P = E_k^{-1}(C)\ ,}$$

recovering the plaintext. The transmission of the cryptogram takes place under the nose of an eavesdropper ("Eve") who clearly must not be able to acquire the key, K, or she will be able to read Alice and Bob's communications. Once Alice has generated enough key material to encrypt any anticipated communications she must arrange for Bob to receive a copy of the key without Eve being able to obtain even partial knowledge of it. If Alice and Bob are able to meet beforehand they can accomplish this key distribution in secrecy. But if they are unable to meet, and they share no secret key material beforehand, Alice cannot simply transmit the key material to Bob because by the main assumption of cryptography this transmission is susceptible to passive eavesdropping, which would allow Eve to also acquire the key.

The conventional approach to this key distribution problem is for Alice and Bob to establish a secure channel, relying on "physical security" which in reality can make it "difficult" but not impossible for third parties (Eve) to acquire key information, and they must store the key material securely until it is to be used. See the following figure 1,

Thus,

1. The necessity for generating, distributing and storing the key material in advance renders the secret key
2. cryptosystems vulnerable to the "insider threat." Trusted individuals with access to Alice's or Bob's stored key material could copy it and provide it to Eve. Furthermore, the cumbersome logistics of generating the huge quantities of key and transporting it securely make the secret key systems susceptible to misuse, undermining their security.
3. are some of the reasons proving the point that the solutions existing for 'key distribution' problem are not perfect or totally secure from eaves dropping

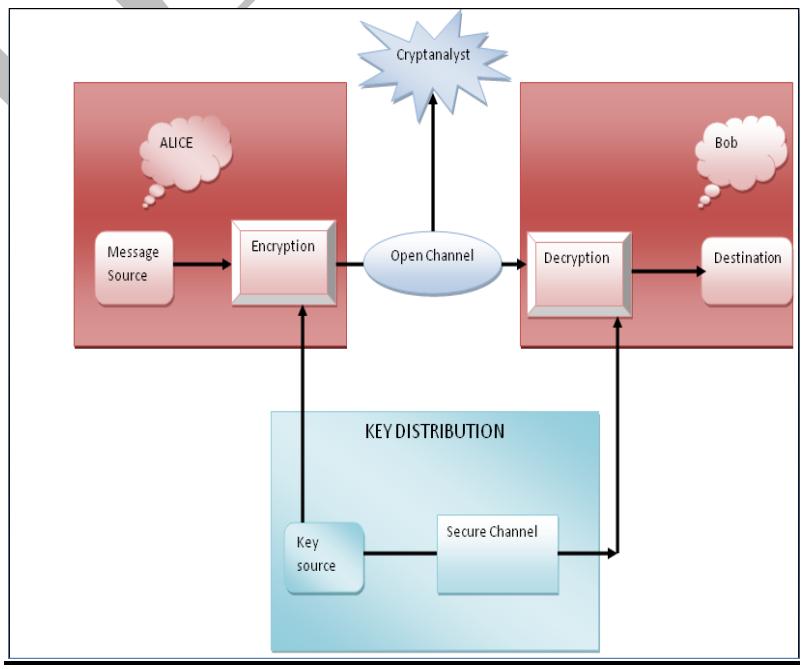

Figure1. Key Distribution center using open channel

IMPLEMENTATION:

QUANTUM KEY DISTRIBUTION:

Quantum Cryptography is "a method for secure key exchange over an insecure channel based on the nature of photons". Since the amount of information that can be transmitted is not very large but is provably secure, it can be used as a replacement for the Diffie-Hellman key exchange algorithm.

SOME TERMS ABOUT QUANTUM CRYPTOGRAPHY:

QUANTUM:

Smallest unit of energy. Quantum is named as "Quanta" in plural form.

PHOTON:

Smallest unit of energy that can be transmitted in a wavelength. It is referred as quantum of light.

POLARIZATION:

The direction of electromagnetic field that a quantum particle has. For Quantum Cryptography, polarization of a photon is a characteristic feature that is used for secure transmission.

QUBIT:

Bit value of a photon that is assigned according to photon's polarization. Quantum bit.

BASES:

Special filters with polarization angles of 0, 45, 90 or 135 degrees which are used to polarize a photon generated by a beam source like a laser.

Figure2: Polarization bases with 0, 45, 90 and 135 degree polarization angles in order.

Filter: A form that is constituted of two crosswise bases. It is used to read last polarization of a polarized photon. There exists two filters: " Diagonal Filter " and " Rectilinear Filter ".

"Diagonal" and "Rectilinear" filters in order.

PHYSICAL BASIS OF QUANTUM CRYPTOGRAPHY:

Quantum Cryptography is related to Heisenberg's "Uncertainity Principle" which issues that a measurement process on a quantum particle randomizes results of following measurements. For instance, a photon passing through a polarization filter with 0 degree polarization angle, is 0 degree polarized and if this photon is directed to a second polarization filter which has such a polarization angle like $\theta = 45^{\circ}$ then it may pass through it with the probability of %50. In this situation it can be said that the first measurement randomized the result of second measurement.

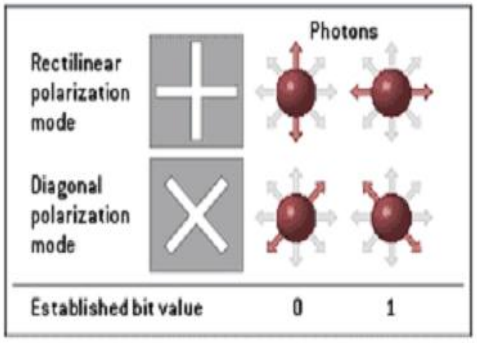

Figure3: Rigorous trial design technique

In Fig3 Rigorous trial design at a macro level can be further refined by developing more accurate modeling inputs to the design process. These additional enabling models include patient retention and recruitment, resource optimization, site selection, and drug supply. Importantly, these methodologies can also function independently as part of the overall trial execution process, even if data-driven designs are not being used.
The general approach to quantum transmission of information is as follows:

A. Alice (sender) sends Bob (receiver) a stream of photons, each with a random polarization, in a random basis. She records the polarizations.
B. Bob measures each photon in a randomly chosen basis and records the results.
C. Bob announces, over an authenticated but not necessarily private channel (e.g., by telephone), which basis he used for each photon.
D. Alice tells him which choices of bases are correct.
E. The shared secret key consists of the polarization readings in the correctly chosen bases.

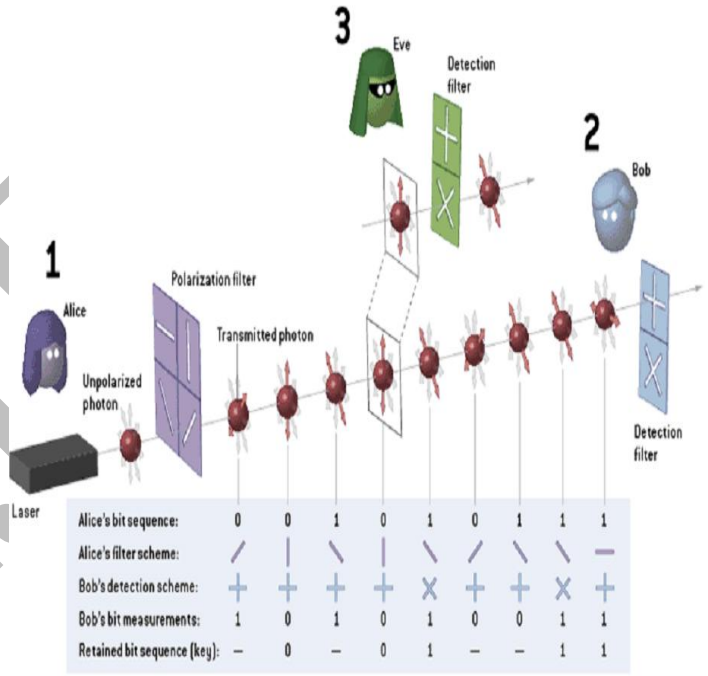

Figure 4. Operation on Quantum Cryptography basis

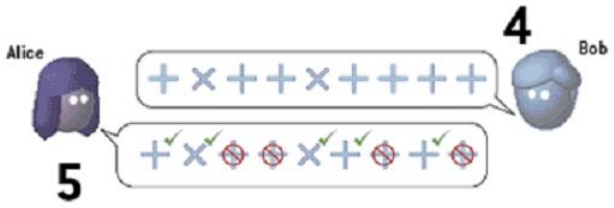

Figure 5. Message Transmitted from Sender to Receiver

Alice send to decrypted data for bobs . Bobs check the bit measurements how many bits required for transmitted bits. Bobs reply for acknowledgement checked the data received or not.

EVALUATION:

QKD enables Secret Key Establishment between two users, using a combination of a classical channel and a quantum channel, such as an optical fiber link or a free-space optical link. The essential interest of QKD that is intrinsically linked to the "quantumness" of the signals exchanged on the quantum channel, is that any eavesdropping, on the line can be detected. This property leads to the cryptographic properties that cannot be obtained by classical techniques; this property allows you to perform Key Establishment with an extremely high security standard which is known as unconditional or information-theoretic security. Highly security applications are thus the natural candidates for QKD-based security solutions.

Benefits of QKD over Trusted Third Party Courier Key Distribution (TCKD) a Symmetric Key Distribution Scenario are:

1. The first difference is really intrinsic to QKD and TCKD "physical realities". In the case of QKD, the "couriers" are quantum states of lights (flying qubits) travelling at the speed of light and on which eavesdropping can be detected with arbitrary high statistical certainty. On the other hand, TCKD cannot offer any of those guarantees and, whether one uses human beings or pigeons, trust or corruption of a classical courier cannot be proven nor tested.
2. Reliability, automation and cost effectiveness will, very likely, be one of the major advances offered by the development of QKD networks. On the other hand, reliability and cost of TCKD infrastructures are critical problems and there is no hope that such systems can ever be automated.
3. Thus, QKD has two attractive features for symmetric cryptosystems. It offers the ultimate security of the inviolability of a law of Nature for key distribution, and it introduces an "ease of use" aspect: key material can be generated when it is required, avoiding the cumbersome, time-consuming security measures of conventional key distribution and hence makes itself superior over them. QKD could be used to generate any shared key, from 56-bit DES keys, all the way to one-time pads for unbreakable encryption

CONCLUSION

1. Key material, which is a truly random number sequence, even though it valuable commodity conveys no useful information itself. One of the principal problems of cryptography is therefore the so-called "**key distribution problem."**
2. Provably secure key distribution becomes possible with quantum communications. It is this sequence of key distribution that is accomplished by **quantum cryptography** thus giving it the correct name **Quantum Key Distribution**.
3. Quantum Cryptography is presented as a %100 secure cryptographic method because of eavesdropping detection and being a physics based method rather than a mathematical method. Unless physics laws on which Quantum Cryptography depends are defeated, method is regarded as impossible to crack. This is a relatively correct approach but like every improperly applied method if Quantum Cryptography is applied improperly, it can turn into a very insecure method too.
4. **Future Scope:** QKD is the first practical application of the foundations of quantum mechanics, and as such it attests to the value of basic science research. However, if QKD is to ever be used in practice its security must be certified, and so we should examine with great thoroughness the aspects of quantum mechanics on which its security is based. To validate these security concepts it may even be necessary to perform new experiments on the foundations of quantum mechanics. Thus, we should expect there to be considerable feedback from QKD into basic Physics. In any event, we can look forward to an exciting future for QKD with many possibilities for future theoretical, experimental and applied physics research.

REFERENCES:

1. Quantum Cryptography. Wikipedia.
2. West, Jacob. The Quantum Computer. 31 May 2000. Dept. of Comp. Sci,
3. Charles H. Bennett and F. Bessette and G. Brassard and L.Salvail and J. Smolin, "Experimental Quantum" Cryptography," Journal of Cryptology, 5, 3-28 (2010)
4. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Quantum Cryptography, Reviews of Modern Physics 74(1): pp 145 - 195.
5. David Mermin, "Lecture Notes on Quantum Computation," [Cornell University, Physics 481-681, CS 483; Spring,]