IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Quantum Cryptography: An Improved Technique for Information Security

Vimal Kumar Awasthi[1],,Mr. Rahul Singh[2]

[1]Asistant Professor, Axis Institute of Technology and Management, Kanpur, India

[2]Asistant Professor, Kanpur Institute of Technology, Kanpur, india

Department of Computer Science and Engineering

***Abstract*—** Quantum cryptography is an advance technology in which two parties can secure network Communications by applying the concept of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics The quantum cryptography based on two important elements of quantum mechanics-the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle states that, the quantum state of any system is not measured without distributing that system. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits t that is unknown quantum states, due to no-cloning Theorem which was first presented by wootters andzurek in 1982.

This research paper includes on the theory of quantum cryptography, and how this technology contributes to the network security. This research paper presents the current state of Quantum cryptography, and the real world application implementation of this technology and finally the future direction in which quantum cryptography is forwards

Keywords:
Cryptography, Quantum Cryptography systems,
Quantum physics, Quantum key Distribution (QKD).

1. INTRODUCTION

Cryptography operates by a sender encrypting the original message or plaintext in a systematic way that obscures its meaning. The encrypted message or crypto-text is transmitted, and the receiver recovers the message by decrypting the transmission Existing cryptographic techniques are usually identified as "traditional" or "modern."

The main practical problem with secret key encryption is exchanging a secret key. In principle any two users who wished to communicate could first meet to agree on a key
in advance, but in practice this could be inconvenient.

By quantum theory , light waves are operated as discrete particles known as photons. A photon is a mass-less particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum. Entangled pairs" are pairs of photons generated by certain particle reactions. Each pair contains two photons of different but related polarization. Entanglement affects the randomness of measurements.

2. QUANTUM CRYPOGRAPHY

The foundation of quantum cryptography based in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from The advantage of quantum cryptography over traditional key exchange methods is that the exchange of information is secure. Quantum cryptography uses quantum mechanics that enables the two communicating parties to produce a shared random bit string called as a key to encrypt and decrypt messages for secure communication and it uses photons to transmit a key securely. Once the

key is transmitted, encryption and decryption using the usual secret-key method can take place.

Experimental implementations of quantum cryptography have existed since 1990, and today quantum cryptography is performed over distances of 30-40 kilometers using optical fibers. Essentially, two technologies make quantum key distribution possible: the equipment for creating single photons and that for detecting them. The ideal source is a so-called photon gun that fires a single photon on demand.

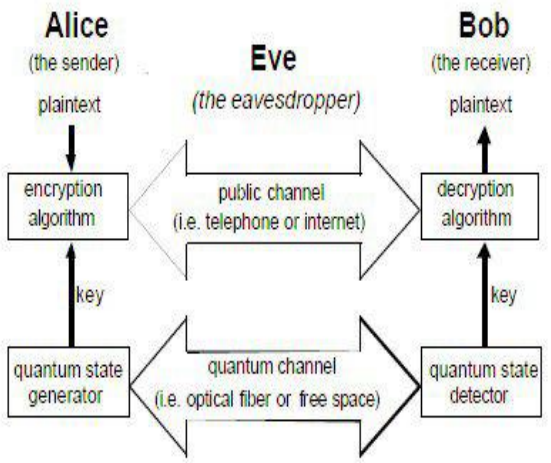


Fig. A Quantum Cryptographic Communication system for surely Transmitting random key

3. QUANTUM PHYSICS

3.1 Polarization of Photon Particles

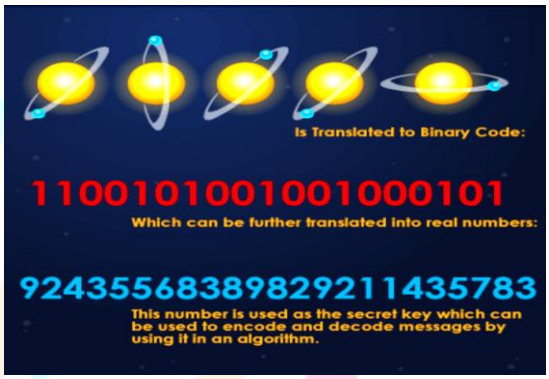
Photons are some amazing particles. They have no mass, the smallest measure of light, and they can exist in all of possible states at once, called the wave function. This means that whatever direction a photon can spin i.e either diagonally, vertically and horizontally, it does all at once. Light in this state is called unpolarized. The foundation of quantum physics is the unpredictability factor defined by Heisenberg's Uncertainty Principle. This principle says that it is impossible to know both an object's position and velocity at the same time.

To create a photon, quantum cryptographers use LEDs (light emitting diodes), a source of unpolarized light. LEDs are capable of creating one photon at a time and using this way a string of photons can be created. By using the polarization filters, the photon can be forced to take one state or another or polarize it. If a vertical polarizing filter situated beyond a LED is used, photons that emerge can be polarized: The photons that are not absorbed will emerge on the other side with a vertical spin.

3.2 Photons becoming the keys

Here, the binary code comes into play. Each type of a photon's spin represents one piece of information usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a message F**or ex:** 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon.

For ex: a photon that has a vertical spin (|) can be assigned a 1. Suppose, Ali sends her photons through randomly chosen filters and record the polarization of each photon. When Ali sends her photons to Bob using an LED, Ali randomly polarize them through either the X or the + filters, so that each polarized photon has one of four possible states: (|), (--), (/) or ( ).



On the other side, when Bob receives these photons, Bob decides whether to measure each with either his + or X filter but could not use both the filters together. Bob has no idea about which filter to use for each photon but can guess for each one. After the entire transmission, Bob and Ali have a non-encrypted discussion about the transmission. Bob calls Ali and informs which filter he used for each photon, and Alice confirms whether it was the correct or incorrect filter to use. The conversation sounds like this:

*Bob:Plus Ali:Correct *Bob:Plus Ali:Incorrect *Bob:X Ali:Correct Since Bob does not reveal the measurements but only the type of filter used, a third party listening the conversation cannot find out the actual photon sequence.

For ex: Ali sent one photon as a (/) and Bob says he used a + filter to measure it. Ali will say "incorrect" to Bob. But if Bob says he used an X filter to measure that particular photon, Ali will say "correct." A person listening will only know that the photon could be either a (/) or a ( ). Bob knows that his measurements are correct, because a (--) photon travelling through a + filter will remain polarized as a (--) photon after it passes through the filter.

Ali and Bob with identical strings of polarized photons look like this: -- / | | | / -- -- | | | -- / | Â¦ so on. Once binary code is applied, the photons become a message. Bob and Ali can agree on binary assignments, say 1 for photons polarized as ( ) and (--) and 0 for photons polarized like (/) and (|). String of photons looks like this: 11110000011110001010.

They are translated into English, prime numbers or others. So, Bob and Ali use them as codes for the keys in their encryption process.

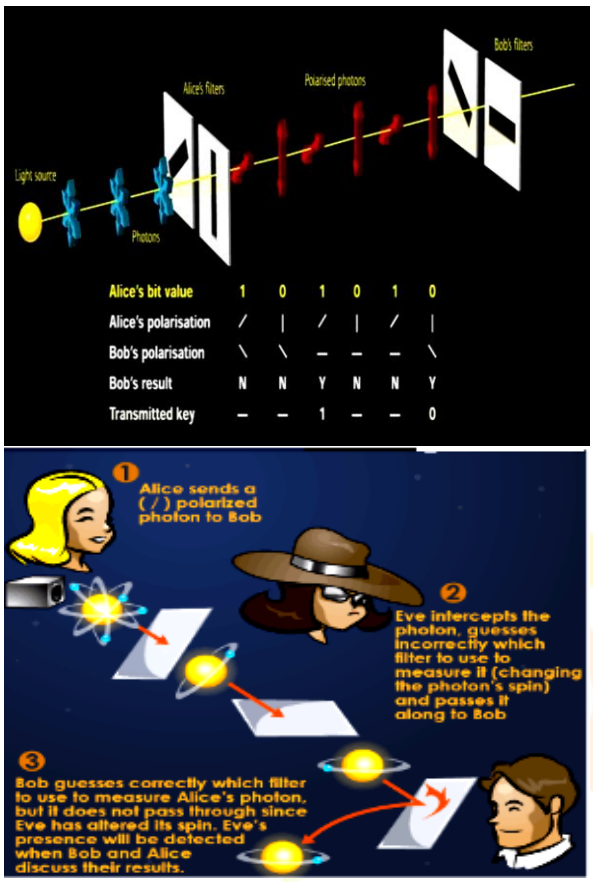


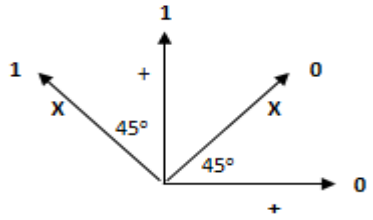
Fig. Use of photons as Keys using polarization filter

4. QUANTUM KEY DISTRIBUTION (QKD)

Quantum key distribution is a method used in the framework of quantum cryptography in order to reduce a perfectly random key which is shared by a sender and a receiver while making sure that nobody else has a chance to learn about the key, e.g. by capturing the communication channel used during the process. The best known and popular scheme of quantum key distribution is based on the Bennet–Brassard protocol(i.e. BB84), which was invented in 1984. It depends on the no-cloning theorem for non-orthogonal quantum states.

4.1 Quantum Coding Scheme

Polarization and measurement of polarization of photons can be done with the use of Polaroid. For the purpose of evolving a simple coding scheme, let us consider only the rectilinear and diagonal polarization schemes. This gives us 4 directions of polarization of a photon. See figure below.



Mapping of quantum digits to binary digits

The 4 possible quantum states (shown in the figure) give us 4 quantum bits or 'qubits'. With the 4 qubits we can represent the classical bits 1 and 0 as follows.

Bit 0 = photon with horizontal polarization or by a photon with polarization at 45 degrees to the horizontal direction.

Bit 1 = photon with vertical polarization or by a photon with polarization at 135 degrees to the horizontal direction.

The above scheme, by Charles H. Bennett and Gilles Brassard, was the first proposed quantum encoding of classical bits and is referred to as the BB84 coding scheme.

We shall use the following notations:

'+' to represent the rectilinear scheme

'X' to represent the diagonal scheme

'-' to represent 0 (Horizontal polarization quantum state)

'/' to represent 0 (45 degrees to horizontal polarization state)

'|' to represent 1 (Vertical polarization quantum state)

'\' to represent 1 (45 degrees to vertical polarization state)

So, using the above qubit representations, a BB84 transmission for the binary 11010011 could look like this:

Alice : Bits	1	1	0	1	0	0	1	1
Alice : Qubit	↕	↕	↔	↕	/	/	\	↕
Bob : Scheme	+	X	X	+	+	X	X	+
Bob : Qubit	↕	\	\	↕	↔	/	\	↕
Bob : Bits	1	1	1	1	0	0	1	1
Key Selection	√			√		√	√	√

Quantum cryptology also has a few fundamental flaws one is the length under which the system will

work is too short is because of interference. A photon's spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be. This means that a 1 may come through as a 0. As the distance a photon must travel is increased, so, too, is the chance that it will meet other particles and be influenced by them.

CONCLUSIONS

As of today, most of the transactions are protected using encryption unproven to be secure against a computational attack. The basic notion of quantum cryptography is to employ single photon transmissions to distribute the random key material, while removing the threat of an undetected eaves dropper.

Quantum cryptography obtains its fundamental security from the fact that each qubit is carried by a single photon, and each photon will be altered as soon as it is read. This makes impossible to intercept message without being detected. It is based on quantum theory which ensures that presence of Eve can be detected when Alice and Bob are exchanging the onetime key pad (which is an unbreakable key).

However for quantum cryptography to become practically viable a lot more progress has to be made to overcome the issue of single photon production, achieving long distances of transmission, understanding all possible attacks. Current key generation rate using quantum cryptography is in the order of 1000 bits/second.

REFERENCES

[1] A review on Quantum cryptography Technology by "Piya Techateerawat" International transaction journal of Engineering and Management & Applied Sciences & Technology.

[2] C.H. Bennett, E. Bernstein, G. Brassard and U.V. Vazirani, "Strengths andweaknesses of quantum computing",SIAM Journal on Computing 26(5),pp. 1510–1523, 1997.

[3] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J.Smolin, "Experi-mental quantum cryptography",Journal of Cryptology5(1), pp. 3–28, 1992.

[4] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. A vol. 73, 2006.

[5] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications 2003.

[6] A review on Quantum cryptography Technology by "Piya Techateerawat" International transaction journal of Engineering and Management & Applied Sciences & Technology

[7] C.H. Bennett, E. Bernstein, G. Brassard and U.V. Vazirani, "Strengths andweaknesses of quantum computing",SIAM Journal on Computing26(5),pp. 1510–1523, 1997.[3] C.H. Bennett, F. Bessette,G. Brassard, L. Salvail and J.Smolin, "Experi-mental quantum cryptography",Journal of Cryptology5(1), pp. 3–28, 1992.

[8] C.H. Bennett and G. Brassard, "Quantum cryptography andits application to provably secure key expansion, public -key distribution, and cointossing",Proceedings of IEEE International Symposium on InformationTheory, St-Jovite, Canada, page 91, September 1983.

[9] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing",Proceedings of IEEE InternationalConferenceon Computers, Systems & Signal Processing, Bangalore, India, pp. 175–179,December 1984.

.