Limitations of Practical Quantum Cryptography

Vibha Ojha [# 1], Anand Sharma* [2], Vishal Goar [$ 3], Prakriti Trivedi [# 4]
# Govt. Engg. College, Ajmer
[1] * MITS, Lakshmangarh
[2] $ Engineering College, Bikaner

***Abstract*- As we all know that the quantum cryptography is having lots of consideration in present time for security but it's important to note that implementation of algorithms using QC is not viable if one wants to have the security intact. It can only be used to share keys using Quantum Key Distribution (QKD). Distribution of keys is just a part of securing information. Proper encryption and decryption are equally important for preventing Eve from guessing the key. But even QKD has a lot to overcome before it's perfectly safe and practically useful. In this paper we are describing the various limitations of quantum cryptography along with its many real time implementation problems.**

Keywords- QC; QKD; BB84; limitations

I. INTRODUCTION

Quite recently, we witnessed an important advancement in data transmission that has its roots from quantum mechanics. This method, called Quantum Cryptography was first proposed in 1984.Since then there has been significant development in it and recently scientists have succeeded in transmitting data through a reasonable distance of 250 Km in free space but at a fruitless transmission speed of 16-bits per second. General purpose use of it has not yet come as on date but we have an artifact in our hand, namely the classical which can do wonders when its potentials are brought to light.

II. QUANTUM CRYPTOGRAPHY

The quantum law underlying QKD is Heisenberg principle of uncertainty: two non-commuting observables of a quantum system cannot be both accurately measured [2]. It ensures that it is not possible to clone a quantum system (no-cloning theorem) [3]. Otherwise, it would be possible to measure one observable on the original and the other observable on the clone.

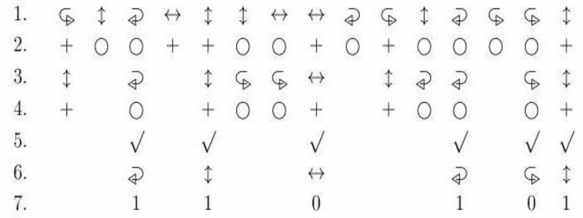
A. Quantum States

The bit is the fundamental unit in classical digital systems to express data and store information. Analogous to classical bits, the basic unit in quantum information science is a quantum bit (qubit) [4]. Two possible states for a qubit are denoted by the states 0 and 1. These states can be regarded as the states 0 and 1 for a classical bit. However, unlike a classical bit that must be in a state either 0 or 1, a qubit can be in both state O and state 1 at the same time.

B. BB84 Basics

The BB84 protocol is simple enough to be understood by a non-specialist of quantum physics [2]. Photons can have a rectangular or a circular polarization. A physical device can observe rectangular or circular polarization but not both. Rectangular polarization can be horizontal noted "↔" or vertical noted "↕". Circular polarization can be left noted "↻" or right noted "↺". Moreover, if a physical device tries to measure circular polarization on a photon that is rectangular polarized, then it gets random results: either left or right, each with a probability of 50%. And the act of measurement changes the state of the photon. The situation is symmetric if a physical device measures rectangular polarization of a photon that is circularly polarized. Session keys are made of bits, 0 or 1.

We agree that: bit 0 can be encoded either by an horizontal "↔" or a left "↻" polarization of a photon and bit 1 can be encoded either by a vertical "↕" or a right "↺" polarization of a photon. Such an encoded bit is called a quantum bit or qubit. Transmitting a key becomes transmitting a sequence of polarized photons. Alice wishes to send a secret message to Bob using a quantum encryption system. The system uses lasers to generate individual photons polarized in one of two modes: vertical/horizontal, or diagonally ± 45°. Within each mode, one orientation represents a digital value of 0, the other 1



1.	↺	↕	↻	↔	↕	↕	↔	↔	↻	↺	↕	↻	↺	↺	↕
2.	+	O	O	+	+	O	O	+	O	+	O	O	O	O	+
3.	↕		↻		↕	↺	↺	↔		↕	↻	↻		↺	↕
4.	+		O		+	O	O	+		+	O	O		O	+
5.			√		√			√				√		√	√
6.			↻		↕			↔				↻		↺	↕
7.			1		1			0				1		0	1

Figure 1 BB84 Protocol

As the sender, Alice randomly chooses both a mode and an orientation (digital value) for each photon sent over the quantum channel. As the receiver, Bob randomly chooses between the two modes when he tries to detect a photon. If he chooses the same mode that Alice used for a given photon, he will correctly measure its orientation and determine its digital value. Choosing a different mode from Alice will give him the wrong value for that photon. So Alice uses another channel to tell Bob the mode she used for each photon, but does not tell him its digital value. Bob can then ignore all the instances where he measured a photon in the wrong mode, and tells Alice which ones he measured correctly, also not telling her their digital value. Alice in turn can discard all the photons Bob didn’t measure correctly. Those measured correctly now make up the encryption key, which Bob and Alice share. If Eve attempts to eavesdrop on Bob and Alice, her attempt to read the data stream will alter it. When Eve’s receiver intercepts Alice’s transmission, the photon is converted to electrical energy as it is measured, which destroys it. Eve must generate a new quantum message to send to Bob, guessing at the digital values for many of the photons, which creates errors in the string of values used in the encryption key. Bob and Alice can find these errors by comparing small quantities of their key’s digital values. If they find a statistically significant number of differences, they will know there is an eavesdropper and can discard the key.

III. LIMITATIONS OF QC

A. Change in Polarization

While traveling through the channel, say optical fiber or through air (wireless), there is always a possibility of change in polarization of photon. The various causes of the same could be:

- *Action of Birefringence:*

The Birefringence is the process of splitting of beam of light into the ordinary and extraordinary rays when passed through certain materials. This effect can occur when the structure of the medium is anisotropic. The reason for birefringence is the fact that in anisotropic media the electric field vector and the dielectric displacement can be nonparallel (namely for the extraordinary polarisation), although being linearly related. If the n_e and n_o are the refractive indices of the material due to the ordinary and extraordinary rays respectively and F is the birefringence,

$$F= k \mid n_e – n_o \mid \qquad [7]$$

Pooling this idea with quantum, we find that the message that is transferred due to photon polarization may change its state (change in polarization) while traveling through a medium. So, one must make sure that the medium is a perfectly homologous one with respect to the refractive index. But this is practically ambitious and leads to changes in the polarization of the photon which leads to misinterpretation by Bob.

- *Paper Clip*

We need to remember that the eavesdropper may not only be a kleptomaniac but also cause cataclysm in the transfer of bits. One such example is the paper clip inkling. The fiber cable may go through rough paths such as the underground pipes, sea water, subway tunnels etc, paving way for the attacker to do his job. Just a paper clip is all that is needed. A paper clip, pinched onto the fiber is enough to cause enough change in refractive index at that point leading to change in polarization. This ultimately leads to wrong interpretation of data.[8] Imagine a city using such highly sensitive communication lines for all it’s important links and a eavesdropper who wants to shut down the city’s entire network, he will do it very easily.

B. Lack of Digital Signatures

The digital signatures are those which demonstrate the authenticity of the digital data to the receiver. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. The digital generation scheme consists of three algorithms namely key generation, signing, key verification. But we know that algorithms cannot be implemented in QC very easily. Therefore QC lacks many vital features like digital signature, certified mail and thus the ability to settle disputes before a judge.[1]

C. Predicament Due to the Source

A basic point to be taken care of while designing the source is the laser pulses' coherence in phase. It is essential that all the photons emitted should be having varying phase coherence. This requires a very sensational design of phase modulator that changes the phase of the successive photons in a rapid fashion. And the attenuated laser pulses are not single photons and the multi-photon components are important [10]

D. Need of a dedicated channel

Exchanging information using single photon needs a dedicated channel of high quality in order to achieve high speed communication. It is impossible to send keys to two or more different locations using a quantum channel as multiplexing is against quantum□s principles. Therefore it demands separate channels linking the source with the many destinations which implies high cost. This is a major disadvantage faced by quantum communication especially through optical channel.

E. Distance and Free Space Communication

The latest distance that scientists have managed to get in QKD is 250 Km at a speed of 16 bits per second and that too through guided medium [1]. However, the satellites in air are at around 36000 Km from the earth surface separated by free space, which makes it incomparable to the former data. So Quantum in wireless is far from reach. One may suggest Quantum repeaters but the number of such repeaters required makes it costlier than the actual system itself! And we need to compromise on the distance for speed and vice versa. Researchers have been trying to implement ground-Satellite communications for so many years. Proposals have already been given that one can use the weak laser pulses instead of single photon for free space communication as a single photon when sent through the turbulent atmosphere, would lead to errors even during nights.

We know that when a signal has to be transmitted to satellite it must pass through the ionosphere layer that contains many sub-layers within itself, containing several ions. The short wavelength photons are absorbed by these materials that splits up a neutral atom into an electron and a companion. Altogether the photon that is sent is lost. However the theory of background rejection and immunity to the Faraday rotation has lead to successful proposal of this theory, taking an advantage that the atmosphere is non-birefringent in optical wavelengths. Still there are many more implementation problems that are needed to be considered. Some of which are

- The background radiation rejection and the non-birefringent atmosphere work only for normal atmospheric conditions. One cannot expect such conditions throughout the year. The main challenge is that the above method does not give secure and reliable communication for all weather conditions.
- The Denial of Service (DoS): The DoS is simply an attempt to make the resource unavailable for its intended users. For a transmission to be reliable it must be resistant to the Denial of Service attacks. However till date, the extent to which the free space communication has the immunity towards DoS remains very low. Furthermore, till date the maximum possible distance that has been demonstrated is 10Km in day light and 23Km in the night (In Free Space).

The main parameters such as the quantum physics implementation maturity, classical protocol implementation maturity, key transfer readiness, practical security, network readiness has not yet been fully satisfied even for short distance communication and none of the above has been satisfied for long distance transmission (>70Km).

F. Trojan Horse Attack

While considering the plug and play systems, Alice's device is open to receive photons So Eve in the middle may send in a light pulse towards Alice’s polarizer, this light gets reflected from the polarizer and leaks vital information to Eve[13]. Other attacks such as the time-shift attack, has been successfully used to crack commercially used quantum key distribution system. This is the first successful demonstration of hacking in a quantum channel[19]. Presently hackers are not having much to gain by spending their resource in hacking the sparsely used a quantum channel. But as QC users increase one can expect more such unexpected innovative attacks which are unthought-of till date.

G. Tolerable error

For channels such as an optic fiber, the probability for both absorption and depolarization of the photon stretches exponentially with the length of the fiber. This may cause the following problems:

- The number of trials required to transmit a photon without absorption or depolarization grows exponentially with length of channel.
- Even when a photon arrives, the fidelity of the transmitted state decreases exponentially with length of channel. The tolerable error probabilities for transmission are less than 10−2, and for local operations they are less than 5 × 10−5. This seems to be far away from any practical implementation in the near future [14]

IV. CONCLUSION

By our discussion we can conclude that QC has a very high weakness of the implementation and lack of algorithms. In future one can expect most of the implementation problems in QC to be overcome. Even that being is the case; QC□s application will be restricted to Quantum Key Distribution (QKD) which plays an important but rather a small part in the protection of data. This restriction is basically due to the fact that algorithms cannot be implemented in QC without sacrificing on security. Our paper will help in pointing out the short comings in QC which needs to be overcome in order to ensure it a future.

REFERENCES

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bangalore, India, 1984, pp. 175–179.

[2] Patrick Bellot , Toan-Linh-Tam Nguyen, Minh-Dung Dang, Quoc-Cuong Le, Thanh-Mai Nguyen “Usages of Secure Networks built using Quantum Technology”, *Intl. Conf. in Computer Science, Can Tho, Vietnam* – RIVF’05, February 21–24, 2005.

[3] W. K.Wooters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, pp. 802–803, 1982.

[4] J. F. Clauser, “Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect,” *Phys. Rev. D, Part. Fields*, vol. 9, pp. 853–860, 1974.

[5] 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.

[6] I. B. Damg˚ard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. Research Series RS-05-20, BRICS, Department of Computer Science, University of Aarhus (www.brics.dk), 2005.

[7] Eric Weisstein's World of Science on Birefringence http://scienceworld.wolfram.com/physics/Birefringence.html

[8] Kartalopoulos, S. V. “Identifying vulnerabilities of quantum cryptography in secure optical data transport” milcom 2005, vol 5, pp. 2788-2796

[9] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” *Phys. Rev. Lett.*, vol. 85, pp.1330–1333, 2000.

[11] R. Perlner and D. Cooper, “Quantum Resistant Public Key Cryptography: A Survey”, Proc of IDtrust 2009, Gaithersburg, MD, Apr. 14-19, 2009.

[12] W.F. Ehrsam, C.H.W. Meyer, and W.L. Tuchman, “A Cryptographic Key Management Scheme for Implementing the Data Encryption Standard,” *IBM Systems Journal*, v. 17, n. 2, 1978, pp. 106–125.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[14] Holger F Hofmann , Toshiki Ide “Optimal cloning of single-photon polarization by coherent feedback of beam splitter losses” *New Journal of Physics* vol **.8** , pp. 130.1-130.9, Aug 2006

[15] Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth) Author(s): Bruce Schneier

[16] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” *IEEE Transactions on Information Theory*, v. IT–22, n. 6, Nov 1976, pp. 644–654.

[17] R.L. Rivest, “Dr. Ron Rivest on the Difficulty of Factoring,” *Ciphertext: The RSA Newsletter*, v. 1, n. 1, Fall 1993, pp. 6, 8.

[18] Information Security Management Handbook By Harold F. Tipton, Micki Kraus

[19] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo: Experimental demonstration of time-shift attack against practical quantum key distribution systems ", *Physical Review A*, vol. 78, Issue 4,2008 arXiv:0704.3253

[20] Raymond Y. Q. Cai and Valerio Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, **11**:045024, April 2009. DOI:10.1088/1367-2630/11/4/045024. EPRINT arXiv:0811.2628.