To Discover Vulnerabilities of Quantum Cryptography in Secure Optical Data Transport

Sandeep Kumar
M-Tech Student, Shobhit University, Meerut, INDIA

Shomil Bansal
M-Tech Student, Jamia Hamdard University, New Delhi, INDIA

ABSTRACT

The last two decades have witnessed an exciting advanced research field that stems from non-classical atomic theory, the quantum mechanics. This research promises an interesting applicability in computation known as quantum computation, and also in secure data communications, known as quantum cryptography Quantum cryptography capitalizes on the inherent random polarization state of single photons, which are associated with binary logic values. Because the polarization state of a photon is not reproducible by an eavesdropper between the source and the destination polarized photons are used with an intelligent algorithm to disseminate the cryptographic key with high security from he source to the destination, a process known as quantum key distribution. However, although the polarization state of a photon remains intact in free- space propagation, it does not remain so in dielectric medium and thus quantum cryptography is not problem- free. In this paper we review quantum cryptography and we identify the various steps in the quantum key identification process. We then analyze and discuss issues related to quantum key distribution that rise in pragmatic fiber-optic transmission and in communication network topologies. In addition, we identify a major weakness of the method that is prone to attacking and which incapacitates quantum cryptography in fiber communications.

1. INTRODUCTION

[1] 1.1. Background

During the last two decades we witnessed an exciting advanced research field that stems from non-classical atomic theory, quantum mechanics. This research has found an interesting applicability known as quantum computation, with an offspring applicable to secure data communications, known as quantum cryptography. The key element of quantum computation is based on a quantum system that can not only be in two states but also in a superposition of states, known as "qubit". Such system may be the two spin eigenstates of a particle +1/2 and -1/2 or the polarization states of a photon. The two eigenstates are associated with the logic value "1" and "0", which mathematically are denoted as:

$$|1\rangle = |\uparrow|$$

$$|0\rangle = |\downarrow|$$

The superposition of two states in a qubit is a concept that is explained only with quantum mechanics.

Mathematically, this concept is linked with two complex coefficients a and b, such that, in a quantum mechanical notation:

$$|\Psi\rangle = a|0\rangle + b|1\rangle, \quad (|a|^2 + |b|^2 = 1)$$

In fact, it is this property that separates the quantum-mechanical qubit from the classical binary bit. In photonics, instead of the electron spin we use the polarization states or any other quantized value of photons (such as phase).

Several research papers and textbooks have been written on the topic of quantum computation [1-5] and quantum cryptography [6-9], both based on the quantum nature of photons and on its dual nature, wave-matter; Based on this, the subject of quantum cryptography has been recently appeared in popular magazines that have tried to trivialize and to popularize quantum cryptography [10, 11]. The oxymoron between the two terms is that "quantum computation" theoretically can break any code within a fraction of a second, whereas "quantum cryptography" establishes a secret key immune to eavesdropping assuring that the key is unbreakable and the cipher text or encrypted message undecipherable.

The term "quantum cryptography" does not really mean that cryptography is quantized, or that quantized quantities are cryptographic; they are merely a combination of two key words "quantum" and "Cryptography" to describe that this is a technology that uses polarized photon explained by quantum mechanics and hence "quantum", and also a sophisticated scheme to transmit a secret code using a sequence of randomly polarized photons (to an external viewer) from which an encryption/decryption key is constructed, hence "cryptography". The method that a secret key is generated and distributed between the two ends of a communications link is known as quantum key distribution (QKD). With this secret quantum key, messages are encrypted and decrypted.

Quantum cryptography, and particularly QKD, uses the polarization states of photons and a binary system. According to it, a subset of photon polarization states correspond to logic "0", whereas another subset of states correspond to logic "1"; this becomes evident if one divides all polarization states on a Poincaré sphere [12, Chapter 1]. The polarization states and their logic correspondence are initially known to point A, or Alice, and through a process that is explained below, Alice defines the encryption key which she makes it known in an encrypted manner to point B, or Bob; this key is known as "quantum key". Thus, the secrecy of this method and the encryption algorithm promises a secure communications channel. However, the efficiency of the method depends on the generation of qubits and on the particular algorithm that qubits are distributed between Alice and Bob. To date, several algorithms have been developed, such as the Greenberger-Horne-Zelinger [13], Bostroem and Felbinger [14] and Cai [15], which have been examined and found to have vulnerabilities to eavesdropping [16]. Similarly, the method of generating qubits should also be examined for vulnerabilities, since the polarization of photons is neither sustainable nor well-controllable, and this is the objective of this paper.

1.1.1 POLARIZATION AND THE POINCARÉ SPHERE:

When an electromagnetic wave propagates in a linear medium (e.g., non-crystalline), the electric polarization is expressed as,

$$P = e_o \chi E$$

where e_o is the electric susceptibility of the medium. When it

propagates in non-linear medium, then is expressed by a tensor, the dielectric constant e = e (1+) is also a tensor, and thus the polarization is not the same in every direction of the Cartesian or polar coordinate system. Consequently, when a polarized photon travels in a non-linear birefringent medium, the interaction of light with matter affects the state of polarization (SoP). The SoP change is visualized if we consider a sphere and each point on its surface representing a state of polarization (SoP). Then, each point S represents a SoP defined in terms of an azimuthal a and an ellipticity e as:

| 1+cos(2a)cos(2e) |

SOP = | |

|cos(2a)sin(2e)+isin(2a)|

This sphere is known as the Poincaré sphere, Figure 1. The azimuthal and ellipticity e of the Poincaré sphere are related to Stokes parameters:

$S_1 = \cos(2\varepsilon)\cos(2a)$

$S_2 = \cos(2\varepsilon)\sin(2a)$

$S_3 = \sin(2\varepsilon)$

$S_0 = \text{sqrt}(S_1^2+S_2^2+S_3^2)$

A moving point S on the surface of the Poincaré sphere defines a trajectory; the trajectory is directly related to the retardation experienced by the field components. For example, if the sphere is defined by the three Cartesian axes x, y and z, then a linear retardation without axis rotation moves S on a circle with plane perpendicular to the x-axis; the arc traveled on the perpendicular to the x-axis; the arc traveled on the amount of linear retardation. A linear retardation with axis rotation by corresponds to a movement of S on a circle having a plane perpendicular to an axis at an angle 2 with the x-axis. Similarly, a circular retardation corresponds to a movement of S along a circle on a plane perpendicular to y-axis. In this case, the rotation angle is equal to the amount of circular retardation. Two mutually orthogonal SoP, both at equal intensity, result to a depolarized field. Now, think that the polarization states on the surface of one half of the hemisphere are associated with logic "1" and the other half with logic "0". Furthermore, how the Poincaré sphere is cut in halves and what the logic association is are kept a secret.

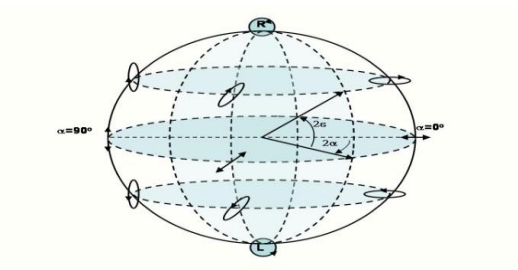

Figure 1. Poincaré sphere mapping the polarization states of a photon. Some states are used to represent a logic "1" and some others a logic "0".

[2] 1.2 Picking a reliable quantum quantity

In general, QC takes advantage of the polarization property of photons, and particularly of polarized single photons that propagate in an optical medium such as glassy fiber (or air), in conjunction with polarizing filters, the polarization state of which varies either according to a program or randomly. Thus, if polarized photons are transmitted and received through polarizing filters from one end of a fiber link to the another end, then a secret key can be defined according to an algorithm that only the two ends can know, a concept that was proven by Charles Bennett, John A. Smolin and Gilles Brassard of IBM Thomas J. Watson Research Laboratory in 1989. However, single polarized photons are not easily generated and they cannot travel far in a lossy, dispersive and birefringent medium; loss attenuates photonic power, dispersion affects the propagation characteristics of photons, and birefringence, B=k|n2- n1|, affect the polarization orientation of traveling photons.

To overcome the shortcomings of polarization, other quantum methods have been devised. One of them uses phase shift of single photons instead of polarization. According to it, the wave nature of a photon is passed through a splitter with unequal lengths and the two halvesare recombined in a Mach-Zehnder interferometer to introduce a phase shift. However, the phase shift within a propagating photon that travels through the non-linear fiber cannot be sustained reliably for long lengths due to self modulation. Another method uses entangled states of a photon pair. According to it, a high energy single photon, such as 405nm, is passed through a strong birefringent crystal to generate two orthogonally polarized photons each at 810nm, thus preserving the total energy. The method of entangled photons capitalizes on the aforementioned property those two mutually orthogonal SoPs, both at equal intensity, result to a depolarized field. As a result, the entangled photon-pair with orthogonal polarization may n theory travel longer distances than a single polarized photon, However, this method depends on the uniformity of medium non-linear properties, and thus like the other two it also has its own ramifications.

[3] 1.3 Quantum key distribution process

In objective of this paper is to identify the technical ramifications of QKD and thus of quantum cryptography. However, in order to do so, it is pedagogical to start from the basics of the quantum key distribution method. Quantum cryptography requires that there is a secret key known only to the processing computers at the end points of a link, point A and point B, and not to anyone else including human operators and any third party (human or computer) that may have tapped the link; this key will be used by end-point A to encrypt a message and by end-point B to decrypt or decipher it. Based on this, assume a transmitter at point A (dubbed Alice), a receiver at point B (dubbed Bob), and an eavesdropper at the transmitting medium between A and B (dubbed Evan). The two points A and B are connected with an optical fiber and also with a separate public channel, such as the Internet or the public wireless network, Figure 2. The task in hand is to make known to Bob of the secret key so that Evan cannot understand it even if he has tapped the optical fiber. Although several protocols to accomplish this have been devised, we describe a straightforward one with the following logical steps, Figure 3:

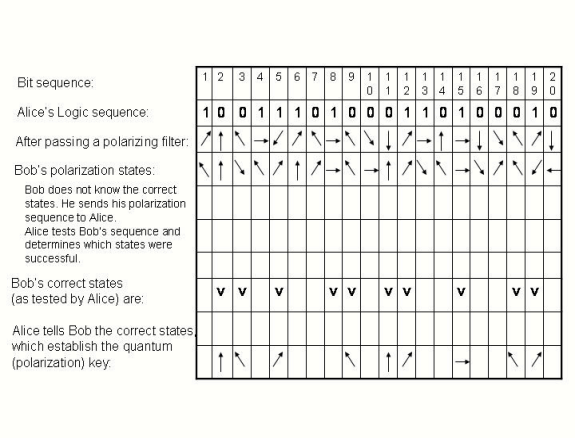

Figure 3. Quantum key generation process.

Alice sends a random association of polarization states for "1" and "0". Bob, uses a random polarization filter for the arriving polarized photons. Some pass successfully and some not. Bob, not knowing the successes and failures, tells Alice the sequence of polarization directions he used. Alice tests her original sequence of "1" and "0" with Bob's filter. She then tells Bob which polarizations were successful; the new sequence determines the quantum key

1. Alice passes a sequence of binary bits, say 100110111011, through a randomly polarization filter. This sequence is transformed in a sequence of polarization states. A subset of polarization states is associated with logic "1" and another subset with logic "0"; the two subsets may be visualized as two regions on the Poincaré sphere. The association of polarization states with logic "1" and "0" are known to Alice only and unknown to anyone else, including Bob.

2.Bob receives the sequence of polarized photons which he passes through his randomly varying polarization filter. Bob does not know the association between logic value and polarization state.

3. The random polarization states of his filter pass or reject the received randomly polarized photons; that is, a new sequence of logic "1s" and "0s" is generated in which some bits have the correct logic value that Alice sent but not all.

4. Assume that Bob's randomly varying polarization filter generates the sequence 010110101001. Although this sequence is not what the same with Alice's transmitted, the common bits between the two sequences what is important here. However, up to this step, neither Alice nor Bob know which bits are common.

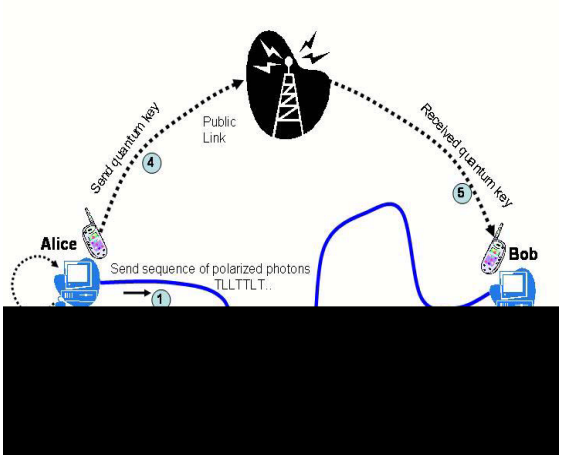

Figure 2. Quantum key distribution process. T and L represent subsets of polarization states associated with logic "1" and "0". This is known to Alice only.

Now, the next steps in quantum cryptography are unconventional and crucial.

5. Bob communicates with Alice over a public unsecured channel and he tells Alice the polarization sequence that he used while receiving Alice's polarized photons; however, Bob does not reveal the logic sequence that he generated.

6. Alice performs an experiment; she passes the logic sequence that she sent to Bob through Bob's polarization sequence and she identifies which bits in the sequence were generated which bits in the sequence were generated

7. Alice tells Bob which of his filter polarization states in the sequence were used correctly, but

without telling him their association with logic "1" and "0"; the polarization states that were used correctly constitute the quantum key.

8. When all this is done, Alice transmits the encrypted message to Bob, who deciphers it using the encryption key.

Thus, what is dubbed "quantum cryptography" (QC) is a process that consists of two major parts, the quantum key distribution (QKD), steps 1 through 7, and the message encryption/decryption process. Assuming that for a long sequence, logic "1" and "0" bits have equa probability of occurrence, statistically half of Bob's states will be correct. Because a key operates on a message bit-by-bit (using a modulo-2 operation), Alice's initial sequence to Bob must be twice as long.

The key point in both processes is the polarization state of photons and the variable polarization filter. In addition, because the polarization of single photons is not readable without altering it and because it is not reproducible, Evan the eavesdropper cannot read the polarization of single photons, reproduce it and send it to Bob. This is the key point in quantum cryptography.

2. QUANTUM CRYPTOGRAPHY TECHNICAL ISSUES

Research on QC continues in academia and industry and significant funding has been devoted to prove the viability of quantum cryptography method and particularly the quantum key distribution (QKD). Despite this, currently no off-the-self QC systems exist that are applicable to multi-wavelength (DWDM) fiber communications. As such, the networks that have been established are experimental testbeds consisting of a short single mode fiber less than 2 kilometers to establish a private single-link point-to-point topology [17]. In a general applicability of QC, there will be many issues, which deserve to be identified and examined. These issues are:

1. Single photon generation with the desired polarization state; there are no "off-the-self" sources with controllable single photon rate generation and controllable photon polarization.

2. Polarization does not remain constant but it changes as photons propagate in the fiber medium due to medium non-linearity.

3. Polarizing filters; there are no "off-the-self" fast tunable polarizing filters with zero insertion loss that can control photon polarization reliably; certain clever method based on Faraday mirrors have been developed but they seem complex and impractical in long length fibers.

4. Single photon source that is synchronized with the polarization state of an external filter; this is not known yet.

5. Point-to-point direct fiber link; the link should remain intact without splices, connectors and

other optical components that may alter the polarization state of the propagating photon.

This imposes a challenge as the fiber over time does not remain intact in its integrity and its performance.

6. Single wavelength channels; QC and particularly QKD is limited to single wavelength photons and thus to a single optical channel, thus underutilizing the full bandwidth capacity of fiber. To date, only dedicated point- to-point solutions are contemplated and no solutions have been reported in multichannel transmission.

7. Synchronized polarization filters at both ends (both Adam's and Bob's); polarization states of the filters at either end need to be synchronized and also to take into account the propagation speed of photons in the fiber medium. This is a very delicate issue as temperature drifts cause delays thus changing the synchronization between the two filters.

8. A not-perfectly coupled single photon source onto optical fiber; typical photonic power coupled onto fiber suffers from loss. There is no reason to believe that coupling a single photon source onto fiber will not suffer from similar loss which may result in photon loss and thus increased qu-bit error rate.

9. Optical fiber maintains the polarization state of photons; manufactured fiber must comply with tight physical, optical and mechanical specifications. The variability of these specifications is real and so is attenuation, birefringence, dispersion, and other non linearities that affect the properties of propagating photons in the fiber.

10. Optical fiber has absorption or scattering centers; at about 1400nm, absorption peaks due to OH-, below 1300nm and above 1620nm increases due to absorption and Raleigh scattering. Currently, there is no zero-loss fiber in any part of the useful spectrum. In fact, to overcome this, researchers are thinking of quantum repeaters; that is, subsystems that will receive the polarized signal, restore its strength, and retransmit it. This of course may defeat the purpose of QKD because Evan can also have the same subsystem which with minor modification can receive the signal, copy the polarized key, restore the polarization state pfphotons and retransmit it to Bob.

11. A very long bit sequence is required to warranty good encryption key. Because the two filters, one at each end, are randomly and independently polarized, the number of bits from Alice's sequence that will pass through Bob's filter are fewer; it is those bits that constitute the encryption key. Thus, in order to warranty a relatively long encryption key (few hundred bits), long sequences must be used.

12. Low bit rate transmission results in significant latency in key identification and encrypted message transmission. Because the process of transmitting photons is very slow, few hundred bits per second, and the bit sequence is too long, see issue #10, the process is comparatively slow.

13. Single chance to successfully negotiate the encryption key. If after a QKD process a key is erroneously identified by Alice, or erroneously executed by Bob, neither side will know. This may create an important issue as it defeats the robustness of the encryption purpose.

14. There is no mechanism to confirm that the key has been correctly constructed and that the encrypted message has been correctly received and decrypted. This is similar to issue #12, yet it identifies a potentially serious issue with the robustness of QC and a lack of verification. What if, a malicious attacker affects one or the other polarizing filter? What is, a malicious attacker adds propagation delay on the line so that filter synchronization is shifted by a bit period? Will Bob recognize it and reconstruct the message?

15. No acknowledgment by Bob that the negotiated encryption key works reliably or correctly. Bob must know if his polarizing filter behaves as prescribed by Alice, and should also know this from the first arriving photon in the encrypted message. Deciding when the first photon arrives is a task with its own.

16. The quantum cryptographic process of key distribution must frequently repeat itself to reinstate possible de-encrypting misalignments.

17. An eavesdropper may easily attack the transmitted polarization states on purpose. The focus in QKD so far to prevent from eavesdropping. However, it is equally important to prevent or countermeasure attacking. An attacker may tap the medium and maliciously destroy the QKD process and thus hamper transmission of the encrypted message. In such case, an eavesdropper is not only a person that needs to "listen" but also one that hinders and deters successful communication between point A and point B; jamming is a well known form of communication deterrence.

18. If multiphoton bit transmission is contemplated, then a small part of the photonic pulse may be extracted from the fiber (by sophisticated tapping) and thus break the encrypted message (assuming that the sophisticated eavesdropper can also "listen" to the conversation between Adam and Bob in steps 4 through 6).

3. OPTICAL COMMUNICATIONS

To substantiate the aforementioned issues, we briefly describe certain key components in optical communication paths; a more rigorous description of their functionality and of their

impairments may be found in [12, 18].

[4] 3.1 Photon sources

Solid state laser devices do not generate single photons but a multiplicity. In addition, the polarization state of photons emanating from the laser device is not easily controlled.

[5] 3.2 Polarization filters and states

Polarization states are controlled by polarization filters. However, film based filters have an insertion loss that may not be suitable for single photon transmission. Moreover, tunable polarizing filters are not mainstream components yet.

[6] 3.3 Absorption and Scattering

The fiber medium cannot be entirely free from absorption and scattering centers and thus attenuation.

To overcome this, some researchers have tried transmitting a laser beam from one mountain top to another, a method known as free-space optical transmission (FSO). The FSO method is known to be more secure than fiber-optic transmission because it is not easy to intercept a thin beam in space without severely attenuating it or interrupting it. In fact, the notion of using the FSO method in deep space in optically interconnected satellite networks [19, 20] has been recognized and gained momentum for inter- satellite communications.

[7] 3.4 Fiber medium

The typical fiber medium cannot be polarization free. There is a residual birefringence that is measured as the difference of refractive indices in the x and y direction of the fiber (z is the transmission direction). Even small pressure and temperature points and tensile stress will vary the fiber birefringence significantly to distort the polarization state of propagating photons, and thus the quantum cryptographic process. In addition, the fiber medium must be continuous without splices and without connectors, which may change the polarization state as photons travel from one fiber segment to another. Finally, the fiber medium cannot be of very long lengths as optical amplification will be required every 60-100 km. However, amplification cannot warranty that the polarization state will be maintained, and opaque repeaters that may restore polarization defeat the purpose as themselves become vulnerable to eavesdropping.

[8] 3.5 The receiver

The receiver in quantum cryptography consists of a random polarizing filter, which exhibits the same symptoms of polarizing filters described above, an ultra-sensitive photo detector, and of a synchronizing clock. The sensitivity of the detector must be such that it detects single photons; such receivers are not trivial to cost-efficiently construct. Similarly, because the clock is not in synchronism with the source (but it relies on the accuracy of a free running clock) the bit rate cannot be too fast. Indeed, bit rates are in the order of few kilobits per second, which is a million times slower than typical optical transmission rates at gigabits per second.

[9] 3.6 Network topologies

Typical network topologies are the ring with several optical add-drop multiplexing nodes, the mesh topology with several interconnected nodes, and the point-to-point with optical add-drop multiplexing nodes. As such, any of the three topologies assumes that the optical signal will travel through a node, which even if it is all-optical or optically transparent, it does not warranty that the polarization of the transmitted photons will be maintained. Consequently, end-to-end quantum cryptography, as currently defined cannot be used in any of these topologies if one or more nodes are on the path between Adam and Bob.

4. WDM FIBER COMMUNICATIONS

Currently, the typical optical communications technology is dense wavelength division multiplexing (DWDM). This is a technology with a well defined standard grid of optical channels and has successfully transmitted several Terabits per second of aggregate traffic in a single fiber. However, the success of the DWDM technology is not the result of single photons or the polarization states of photons but in its ability to transport high speed data over many optical channels that are multiplexed in the fiber. As a consequence, any new cryptographic technology should stay in step with DWDM and solve the data security issue for each channel and on the aggregate. Moreover, a more complex and pragmatic network topology should be considered, as well as that photons travel in a not so perfect fiber for hundreds of kilometers through optical components that may affect the properties of the optical signal. Finally, it should also be considered that the photonic signal will suffer from linear and non-linear phenomena that are typical in fiber communication. Such phenomena that emanate from the photon-matter interaction are four wave mixing, polarization mode dispersion, cross-phase modulation, instability modulations, polarization state rotation, phase shift, and so on, have an effect on photons and the photonic signal [18]. Therefore, if single photons of different wavelength would be transmitted to comply with DWDM technology, their interactions would affect their polarization state, their logic value (1 or 0), and even more, their existence.

5. PAPERCLIP: A WEAPON OF MASS CONFUSION

Photonic quantum cryptography in its current state is so vulnerable that may be eventually proven disastrous, if widely used. For example, imagine that by the year 2010 the quantum cryptography, as we know to date, has become the preferred technology to transmit data securely over fiber and it is deployed in every city across the country. Imagine that eavesdroppers have been discouraged tapping the fiber to "listen" data. Thus, this technology has accomplished its objective and dependence has been established, as it has been done to day with personal computers.

However, imagine that a malicious attacker wants to bring havoc and confusion in communications and to incapacitate the information dissemination process in communications by destroying the ability to encrypt messages. In such case, the many kilometers of fiber, on poles, underground pipes and subway tunnels present endless opportunities to access.

Now, what does this have to do with paperclips? A small box of paperclips in the hands of a sophisticated attacker becomes a powerful anti-QKD weapon that potentially can cause mass confusion. Imagine that the malevolent attacker accesses the secret-key bearing fibers and he/she clamps paperclips on it; then, the pinching pressure exerted on the fiber by the paperclips:

- changes the propagation and polarization properties of photons in fiber such that the polarization states transmitted by Alice arrive Bob altered, Figure 4,

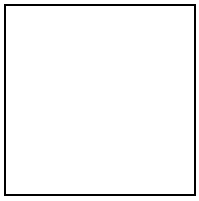

Figure 4. Attacking the quantum key generation process.

Evan has changed the correct delivery of states so that when Bob tells Alice the sequence of polarization directions he used, Alice determines a which turns out to be wrong as it will not decrypt correctly the encrypted messages.

- Bob sends back to Alice an entirely inconsistent polarization pattern to Alice, which is also altered.
- Alice, not knowing what is going on with the paperclips, tests the received pattern that Bob sent to her, finds the (erroneous) commonality, and she sends to Bob a quantum-key which is wrong.
- Bob receives a message that cannot be decipher.
- Eventually, Alice and Bob will realize that the security of the quantum channel has been compromised. To continue communication securily, Alice and Bob must now try another fiber, which also may have been compromised. Thus, some paperclips make the quantum key distribution process useless, secret documents and sensitive information cannot be transported over fiber successfully, and there is mass confusion in communications.

Although the aforementioned may seem hypothetical, however it is a reasonable scenario, it is simple and it is inexpensive. In a trivial experiment, we have verified how easily the polarization of light changes by about 90 degrees with very small amounts of tensile of bending forces exerted on fiber.

6. CONCLUSION

We presented a critical view of the workings of quantum cryptography and quantum key distribution.

This technology is based on the polarization of photons, which is not a well controlled quantity over long distances and in multi-channel networks. We identified the merits of the technology and we emphasized its vulnerabilities. Quantum cryptography is still on the learning curve. Therefore, in its current state quantum cryptography does not provide an as expected robust technology but a technology useful in well-manicured applications. As the momentum in quantum computation research continues, it is expected that new technology will be created that will spawn useful applications, such as single photon generation and detection, which can provide interchip fast optical interfaces that will be wireless and immune to electromagnetic interference.

7. REFERENCES

[1] Yu. Kitaev, A.H. Shen, and M.N. Vyalyi, Classical Quantum Computation, American Mathematical Society, Providence, RI, 2

[2] G. Benenti, and G. Casatti, Principles of Quantum Computation, vol I: Basic Concepts World Scientific Publishing, New Jersey, 2004

[3] S.J. Lomonaco, Jr., editor, Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millenium American Mathematical Society, Providence, RI, 2002

[4] D. Deutch, "Quantum computational networks", Proceedings of the Royal Society of London vol. 425, pp. 73-90, 1989.

[5] Tombesi and O. Hirota, editors, "Quantum Communication, Computing and Measurement3",Kluwer Academic/Plenum Publishers, New York, 2001.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Rev. Mod Phys. vol. 74, pp. 145-195, 2002.

[7] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the Ekert protocol", Phys. Rev. Lett., vol. 84, pp. 4733-4736, 2000.

[8] P. Trojek, C. Schmid, M. Bourennane, H. Weinfurter, and C. Kurtsiefer, "Compact sources of polarization-entangled photon", Opt. Express, vol. 12, pp. 276-281, 2004.

[9] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system", New J. Phys, vol. 4, 41.1-41.8, 2002.

[10] G. Stix, "Best-Kept Secrets", Scientific American, January 2005, pp. 79-83.

[11] J. Ouellette, "Quantum Key Distribution", The Industrial Physicist , December 2004/January 2005, pp.

[12] S.V. Kartalopoulos, DWDM: Networks, Devices and Technology Chapter 1, Wiley/IEEE Press, 2003.

[13] X. Li, "A quantum key distribution protocol without classical communication", quant- ph/020950, September 6, 2002.

[14] K. Bostroem and T. Felbinger, "Ping-pong coding", quant-ph/020940, September 5, 2002.

[15] Q-Y. Cai, "Deterministic Secure Direct Communication Using Ping-pong Protocol without Public Channel", quant-ph/0301048, January 13, 2003.

[16] D. R. Kuhn, "Vulnerabilities in Quantum Key Distribution Protocols", quant-ph/0305076, May 12, 2003.

[17] Poppe, et al., "Practical Quantum Key Distribution with Polarization Entangled Photons", quant-ph/0404115, April 23, 2004.

[18] S.V. Kartalopoulos, " Fault Detectability in DWDM ", Wiley/IEEE Press, 2000.

[19] S.V. Kartalopoulos, "A Global Multi Satellite Network", US patent 5,602,838, 2/11/1997.

[20] S.V. Kartalopoulos, "A Global Multi-satellite Network", Proceedings of the ICC'97 Conference, Montreal, Canada, 1997, pp. 699-698.