On the Power and Usability of Quantum Cryptography

Hesham A. El Zouka
Computer Eng. Dept, College of Engineering and Technology
Arab Academy for Science, Technology, and Maritime Transport,
Alexandria, Egypt
helzouka@aast.edu, helzouka@gmail.com

Mustafa M. Hosni
Electrical Engineering Dept., Faculty of Engineering,
Managing Director of OMIKRON Technologies,
Alexandria, Egypt
mustafa.hosni@omikrontechnologies.com

***Abstract* — Threats and attacks to information on the digital network environment are growing rapidly; this puts extra pressure on individuals and business, as they will have to protect their privacy and intellectual property, then. Therefore, cryptographic security protocols have been developed to maintain privacy between communicating parties and to reduce the risk of malicious attacks. However, most of the cryptographic algorithms which have been developed are based on mathematical models and possess some security defects. Therefore, most of these cryptographic protocols aren't secure enough against the main threats of modern networking technologies and computing systems. In this paper, the limitations of quantum cryptography are analyzed and a security framework model which is based on quantum entanglement is used to perform an efficient data encryption of short messages. Ultimately, the proposed method is demonstrated and validated by a series of experiments and analytical results.**

Keywords- Cryptography; Cryptanalysis; Quantum Key Distribution, Confidentiality, Physical Properties, Light Particles.

I. Introduction

Cryptography is the science of securing data and communication between two communicating parties in the presence of the adversaries [1]. In other words, it is the use of techniques, policies, controls, and awareness to help in protecting the data transferred between a sender and a recipient in an attempt to avoid detection by a third party intercepting the communication traffic. As for now, modern cryptography involves many related protocols including data integrity, data confidentiality, authentication, and non-repudiation. Moreover, cryptography is used in many applications, such as computer passwords, ATM cards, e-commerce, and many others which bring together scientists from the disciplines of mathematics, electrical engineering, and computer science. Cryptography has only been concerned with encryption; the process of transferring plaintext data that can be read by anyone, to cipher text data that is scrambled and unreadable [2]. Only the secret key that is being shared between the designated sender and the receiver can be used to encrypt/ decrypt a message. Therefore, the keys used between parties involved remain a secret [3].

The methods used to carry out cryptology have become increasingly complex and its application more widespread during the past few decades. However, modern cryptography today is heavily based on mathematical theories and computational mechanisms in which cryptographic primitives are implemented as actual computational algorithms, making such algorithms hard to break in practice by unauthorized users. Eventually, it is theoretically possible to break such a system, but practically it is not an easy task as the computer would have to try about half of possible keys on average before finding the correct one. For example, it would take 1013 years to search the entire key space of 128-bit key length before achieving the correct key. To stand against brute force attacks, for example, one would need to search half of this key space to find the required key, but it is assumed to be infeasible to search through all these possible keys. Cryptography algorithms are divided into Symmetric and Asymmetric key cryptography. Symmetric Cryptography is further divided into Block ciphers and Stream ciphers. In symmetric key cryptography, the encryption key is identical to the decryption key [4]. Symmetric key algorithms are generally much less computationally intensive than asymmetric key algorithms, which makes them more feasible to use in most communication applications [5]. The main disadvantage of most symmetric cryptography is the need for a distribute secret key for each pair of communicating parties, which, in turn, implies the existence of secure channel to exchange the secret keys. DES, Triple DES, and AES are three common cryptography standards and are broadly classified as symmetric key block ciphers [6], [7]. On the other hand, the Asymmetric cryptography, also known as PKI (Public Key Infrastructure), needs a pair of distinct and different keys: a "public key," which is released to the public, and a "private key," which is known only to its proprietor. For instance, if Bob and Alice wish to communicate securely with each other using asymmetric encryption model, Alice first asks Bob to send her his public key through the unsecured channel. Now, when Alice receives Bob's public key, she uses it to encrypt her message and then sends this encrypted message to Bob. Only Bob can then decrypt the encrypted message, because he is the only one who knows the corresponding private key [8]. Bob must, similarly, get Alice's public key in order to exchange messages with her. The main advantage of using asymmetric cryptography model is that with the support of public key infrastructure (PKI) no special key management operation is needed. Therefore, the private keys are never exchanged between them and only their public keys that are distributed. RSA and ECC are examples of asymmetric algorithms. RSA is based on the factorization problem which makes it computationally infeasible to calculate the private key from knowledge of the public one [9]. If the attacker attempts to compute the user's private key, he has to compromise the secret prime numbers ***p*** and ***q*** first. Even though he has the knowledge of the public key (***e***), he will still need to factorize the two prime numbers ***p*** and ***q***. Therefore, it will not be easy for an attacker to compute ***d*** since it is not practically possible to find $\emptyset(\mathrm{n})$ without knowing the private key (***d***) and/or the factors of ***n***.

Therefore, the sender can employ the public key ***e*** to encrypt a message m and obtain the cipher text ***c***, where $\mathrm{c} = \mathrm{m}^{\mathrm{e}} \mathrm{mod}\ \mathrm{n}$. The receiver decrypts the message and gets m from c using his private key exponent d and the equation: $\mathrm{m} = \mathrm{c}^{\mathrm{d}} \mathrm{mod}\ \mathrm{n}$. RSA and other Asymmetric cryptography algorithms are based on the difficultly of factoring large composite numbers. However, most of the developed cryptographic algorithms are based on mathematical models and suffer from many security defects, such as: a brute force attack, factorization problem, and many others. Thus, most of these proposed cryptographic systems are not completely secure against the main threats of modern networking technologies and computing systems. It’s clearly that the classical cryptography algorithms allow potential security defects related to the key expansion ratio, computing power, and key refresh rate [10]. As new computational tools are developed, classical cryptography and key computational complexity have become increasingly exposable to different types of cryptanalytic attacks.

II. QUANTUM CRYPTOGRAPY AND CRYPTANALYSIS

The only security system that was proved to be completely unbreakable is the Quantum Key Distribution (QKD) system, and which wasn’t, for obvious reasons, really implemented for encryption/decryption of long messages [11], [12], [13]. Researchers have demonstrated for the first time that quantum cryptography can be used to transmit short keys securely over a commercial transmission network [14]. A few years ago, many countries have worked on studying this quantum cryptography technology. The first quantum cryptography network has been implemented in Vienna, Austria where the network was implemented with six nodes and eight optical fiber links with distance between 6 Km and 82 km. The implementation uses optical ring architecture and a maximum of six different quantum cryptographic devices for key generation. The cryptographic key generation and distribution was demonstrated, as well as the utilization of the keys for standard commercial applications. Today, QKD is the most promising technology for securing cryptographic keys and can be used to exchange keys over fiber channels with lengths up to 250 km [15], [16].

The security of quantum cryptography relies on the foundation of quantum physics which indicates the difficulty of deducing the key from the communication channel, and in comparison with the tradition public key cryptography which relies on the computational difficulty of mathematical functions, it cannot guarantee the security of the key against an eavesdropper who is capable to deduce the key by posing different cryptanalysis algorithms. For example, if one could come up with a way to factor large numbers into their primes, then one would have a tool for breaking public key algorithms. However, an optimized and streamlined synthesis for Quantum data can greatly revolutionize in generating unbreakable codes [17]. As a matter of fact, a 7- bit-quantum computer has been built by IBM, and some quantum algorithms have run on it, but the experimental results are very far beyond the theoretical ones and modern cryptanalysis technology. [18], [19], [20]. Indeed, cryptanalysis is defined as the process of studying methods of obtaining information from encrypted data without knowing the secret key. It is usually a deep analysis and attacks an encryption method to find the secret key. Normally, the best attacks on block ciphers are the brute force attack and linear-differential cryptanalysis [21].

Brute force attack is the process of trying all possible combination. It involves systematically checking the search space of all possible keys until the correct key is found [22]. In literature, Differential and Linear cryptanalysis are the most common cryptanalysis techniques used in block cipher**.** The success rate of linear cryptanalysis depends mainly on the amount of the data being used and the bias of the approximation. This kind of analysis was first developed by Matsui [23] in 1994 to attack DES, but the analysis can be also applied to attack other block ciphers.

On the other hand, Differential cryptanalysis was first introduced by E. Biham and A. Shami in 1990. In differential cryptanalysis, the attack can be successfully performed to distinguish an n-bit block cipher from a random permutation. By considering the distribution of output differences for the non-linear components of the cipher, the attacker may be able to construct differential characteristics for a number of round N that are valid with a certain probability [24]. In contrast, the main idea in differential cryptanalysis is to compare the XOR output of two plaintexts with the XOR output of the corresponding two ciphertexts. Two chosen plaintexts; P and P*, whose XOR to carefully chosen differential plaintext P'=P x P* can encipher to two ciphertexts C and C* such that C' = C x C* takes on a specific value with non negligible probability. Today, linear and differential cryptanalysis is considered to be essential in designing any new block cipher Another type of cryptanalysis involves the frequency of letters attack.

III. Quantum Cryptographic technologies

Quantum cryptography is a new process to secure data communications, since the security is guaranteed by the laws of quantum mechanical exclusion principles. This section examines the security of the Defense Advanced Research Projects Agency (DARPA) intrusion detection system [26] in attempt to clarify the necessary steps in designing and implementing secure quantum cryptography scheme for exchanging longer messages. ~~In~~ order to achieve this goal, the characteristics of the DARPA intrusion detection system are analyzed and adopted to maximize the amount of encrypted transferred data.

In order to establish a quantum cryptography network, it is essential to distribute single photon or entangled photon pairs over optical fiber. Optical channels could provide a practical way to guide high speed optical pulses with little disturbance. To ensure a secure transmission, the quantum states of the encoded data are measured using polarization encoding scheme. Photon polarization has many physical concepts and mathematical models which form the fundamental basis for understanding quantum phenomena. Polarized light is identified by electromagnetic waves that oscillate perpendicular to the direction of light's travel and with a frequency that is related to the wavelength of a light wave [27], [28].

Therefore, Establishing quantum cryptography networks needs single photon or entangled photons to be distributed over the distance. A unique solution to this problem could, hence, be provided by optical free space channels as they already allow much larger propagation distance of photons with certain wavelength ranges. In quantum cryptography, polarization is considered one of the most important features of optical waves: for encoding 1 state, a vertical polarized (“V”) wave has to be defined as one for which the electric field is restricted to lie along the plane-axis for a wave propagating along the x-axis, and similarly, to encode 0 state, a horizontal polarized (“H”) has to be defined as one in which the electric field lies along the y-axis. It is quite remarkable, then, that any other polarization state of light propagating along the x-axis can be resolved into a linear superposition of vertically polarized and horizontally polarized waves with a particular relative phase. If the light is linearly polarized, the amplitude for the two components will be determined by the projections of the polarization direction; the V or H polarization axes. For instance, light linearly polarized along the diagonal $+45^0$ direction in the y-z plane is encoded by 1 state, in-phase superposition, while light polarized along the diagonal -45^0 direction in the y-z plane is encoded by 0 state, and opposite-phase superposition. Obviously, V and H polarization states will be considered orthogonal polarizations, while another two polarizations such as (V and +450) that have a non-zero projection will be considered a non-orthogonal. However, light, of a particular linear polarization, can be produced by sending unpolarized light through a polarizing medium whose polarizing axis is oriented along the direction of the desired linear polarization. In case of sending the light through a second polarizer, only the component polarized parallel to the polarizing axis emerges, and the orthogonal component, on the other hand, is absorbed. If V light, for example, impinges on a polarizer oriented at the +450, the emerging light will be reduced in amplitude by factor $1/\sqrt{2}$ having the +450 polarization and the intensity which is 50% of the incident intensity. Moreover, if V light impinges on an H polarizer, no light will emerge and this configuration will be described as having “crossed polarizer" [29], [30].

IV. Design and Analysis

When a photon is polarized in one direction, and measured in that direction, the correct count for the received photon is obtained. On the other hand, if the polarization detector measures a photon which is sent in different direction plane, the recipient gets a random result for the count. Today, many quantum key distribution systems have been proposed, such as: BB84, EPR scheme, B92, Lo-Chau scheme, and etc [31], [32], [33, [34]. All these protocols share a similar structure with some variations. The following points describe the BB84 protocol:-

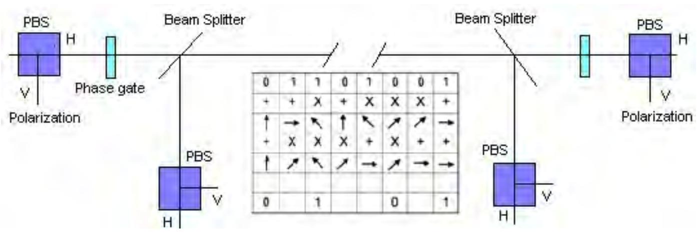
1- Alice sends Bob a stream of photons, each one is polarized with one of four direction plans, namely: Horizontal, Vertical, left-diagonal, and right diagonal. While the vertical and horizontal polarizations are denoted by rectilinear term, the left and right diagonal polarizations are denoted by diagonal term as illustrated in Figure 2.

2- Bob receives the photons and his polarization detector determines one of the two settings, diagonal or rectilinear. Thus, bob randomly chooses one setting for each received photon.

3- Later on, Bob tells Alice which of the two settings he has chosen for each photon.

4- Over an insecure channel, Alice tells Bob which polarization method she applied for each photon (diagonal or rectilinear) and which settings were correct, but she does not announce which bit was transmitted, 0 or 1 since she does not reveal which direction plane (e.g. H or V) was favored.

However, if Bob has chosen the rectilinear setting, he will measure this accurately. As shown in figure 2, the rectilinear polarization assigns 0 for H and 1 for V, and diagonal polarization assigns 0 for right diagonal and 1 for left diagonal. Obviously, Bob has correctly adjusted the polarization detector to achieve optimum polarization error correction performance. On the other hand, if an adversary tries to listen to the channel and introduce errors on the pulses in order to make Alice and Bob end up with possible different stream of bits, the errors will be detected easily due to the nature properties of polarization. Indeed, the adversary cannot measure or disturb the photon without changing its polarization settings, and hence these changes will automatically show up in Bob's measurements, where errors appear on his readings. Therefore, in quantum cryptography the adversary's measurements are bounded to affect the state of photons. That's why Quantum cryptosystem is suitable for key distribution, and used in a manner equivalent to one-time pad that is proven to be unbreakable. However, the most obvious disadvantage of this scheme is the difficulty of transmitting photons accurately over a considerable amount of distance, and without losing information. In addition, Brassard et al. [35] discovered that noticeable noises can be generated by the polarization devices itselves.



0	1	1	0	1	0	0	1
+	+	X	+	X	X	X	+
↑	→	↖	↑	↖	↗	↗	→
+	X	X	X	+	X	+	+
↑	↗	↖	↗	→	↗	→	→
0		1			0		1

Figure 2. Quantum Key Distribution Protocol

Thus, this method can be effectively used for exchanging secret keys and cannot be used as cryptosystem for encryption and decryption of long messages. Studying the properties of QKD protocols identifies some drawbacks, which have led us to search a scheme that increases the amount of data transmitted over optical communication channels. For increasing the amount of bandwidth that could be transmitted down a single fiber, several approaches can be applied to the fiber optics technology. One promising approach could be the use of wavelength division multiplexing (WDM) where a wavelength multiplexer divides the optical channels at the receiver input and transmits these wavelengths down a single fiber.

The effectiveness of this approach is that it allows the optical channel to drive multiple traffic streams simultaneously, each one carrying its own independent steam of data. As shown in Figure 3, each wavelength carries a certain amount of bandwidth – up to 10 G bit/sec - and by combining these wavelengths together to make simultaneous measurements in the receiver side, will increase the amount of data transmitted. The concept of WDM was first published in 1978 and was realized in modern technologies such as: optical add-drop multiplexer and telecommunication systems.

Similarly, Wave Vector Division Multiplexing (WVDM) can be used in increasing the throughput of data in quantum technologies. In WVDM, the receiver splits the individual laser beams on the basis of unique wave vectors. WVDM can also conjunction with WDM to increase the amount of data even further. In quantum communication, the photon streams are polarized and subjected to wave vector manipulation in order to increase the data throughput in such networks. Further, WVDM can be combined with VDM to create multiple wavelength beams, where each wavelength has its own unique wave vector.

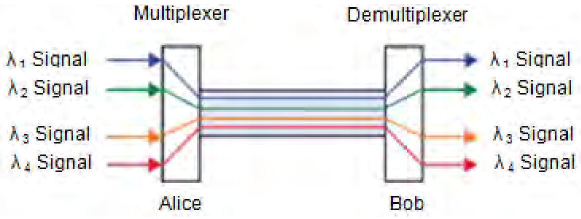


Figure 3 Wavelength Division Multiplexer

The progress in WVDM technology would allow 16 WDM channels to be effectively deployed as a part of quantum communication channels. This may provide the advantage of creating sixteen 1.5 G bit/sec channels and the initialization of 20 Km fiber optic connections, and consequently, duplicate the throughput offered by such QKD links. However, experimental design and analysis should be carried out in order to validate the theoretical results. The analysis should also consider the error correction, quantum entanglement, and multi point quantum communication.

V. LIMITATIONS AND SECURITY IMPLICATIONS

A number of key challenges still remain in quantum cryptography such as data rate, transmission distance, and bit error rate (BER). The following paragraphs will analyze the limitations of quantum cryptography and attempt to describe how quantum entanglement can be used to perform an efficient data encryption of short messages without any pre-shared key distribution. The conflict between real time encryption module and the security implications will be analyzed and presented. Photon sources and detectors: The security of quantum key protocols depends not only on the hardware and software of quantum cryptography system, but also on the physics laws and the ability to generate and encode a single photon that is protected against any side channel attacks. If that were possible, attacker could make and distribute a copy of the message without being detected. Therefore, in the quantum world, any attempt to quantum measurement would destroy the quantum state without revealing any of its secrets. Only the intended parties can view it and tell if the connection has intercepted by examining the error rates. A message is likely to be rejected if its error rates are higher than the average, which means the quantum channel is not secure. Although no successful attacks have yet been reported on quantum cryptography, the attack can be performed by careful analysis of the quantum channel and by keeping the error rates below the standard quantum limit [36].

Quantum random number generation: Random number sequences are an important resource for studies of quantum cryptography. In order to build a key sequence, the polarized states of the key are chosen and transmitted based on a random manner, either diagonal or rectilinear. At this point, the parties establish a channel of communication that can be insecure to inform each other what bases they had used for each measurement. However, if the random number is generated by a computer, then the protocol must ensure the randomness of the generated key because the complete randomness cannot be achieved by classical deterministic computers. True random numbers can only be generated if there is a truly random physical input device that provides a seed for the quantum key distribution protocol [37]. Therefore, the truly generated random number helps in reducing the amount of information that attacker can gain by sniffing on the quantum channel.

Quantum networks and quantum repeaters: In QKD protocols, the distribution of quantum states of photons are affected by losses during the signal propagation or at the detection process, which limit the distance over which the entangled photons can be properly transmitted. For example, the typical loss of 0.2 dB/Km at wavelengths around 1.5 m, would result in a minimal distance of the order of two hundreds kilometers, thus limiting the distance over which an encrypted key can be transmitted. In order to achieve a longer distance, quantum repeaters have been proposed. However, because of the fiber transmission loss and detector noise, the range of such systems is limited to some tens of kilometers. The most successful quantum repeaters combine quantum memory and entanglement swapping protocols to efficiently extend the existing distance of quantum networks. However, this approach is not feasible within current quantum technology since the quantum memory that stores the quantum states is experimentally challenging.

Low transmission and error rate: The transmission rate is naturally defined as the average information obtained by the output side (i.e. the number of corrected secret bits that can be transmitted. In quantum technology, the sender transmits a particles of light, or stream of photons, to encode zeros and ones to the recipient, which if correctly measures will construct the secret key that is used to encrypt and decrypt the subsequent messages. The modern quantum hardware connections allow the communicating parties to transmit photons at a rate much faster than before. However, when the speed is increased, the recipient detector will not be able to sense the photons due to the limitations of the detectors they use. Commercially, each photon needs about 40-80 nanoseconds to recover before the detectors can sense another photon, which in turn will slow down the transmission rate and decrease the key production rate. The following examples show how we can generate short secret messages that avoid the dead time period of the detectors. For each generated message, the dead time is computed and given. If the algorithm failed to avoid the dead time period, then we remove one letter from the back end of the message and try again. Running the program on different input messages each with a length k and hold-off time following each detection event is around 40 nanoseconds, the program produces the output according to the following equation:

$$K = \ * P_{TRX} \qquad (1)$$

$$P_{TRX} = \mu * \varphi \qquad (2)$$

Where µ is the efficiency of the recipient's detector and P_{TRX} is the probability of correctly transmitting and receiving a bit with a quantum state opposite to its preceding measured quantum state. For a range of values of the normalized dead time, the overall performance of the detection system is assessed.

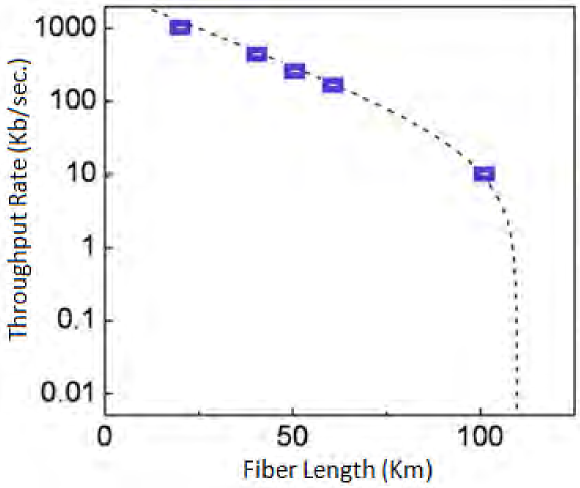


Figure 4 Performance Analysis

The experimental results showed that the proposed system is able to achieve the highest detection rate with minimum error by using the differential time multiplexed scheme as illustrated in section four of this paper. The correlations between the P_{TRX} and the sender's free error messages K is illustrated in figure 5.

In addition the quality of the quantum channel (φ) as well as the distance between the sender and the receiver is also analyzed and the results show that the fiber length after the modeling is almost the same for each standard speed power level (blue squares) as shown in figure 4

The experiment shows that the throughput rate is 20 K bit/s at 80 Km. By employing wavelength division multiplexer we can increase the throughput rate of the quantum cryptography system up to nearly 1 GHz, which is approaching the value used in classical quantum key distribution channels.

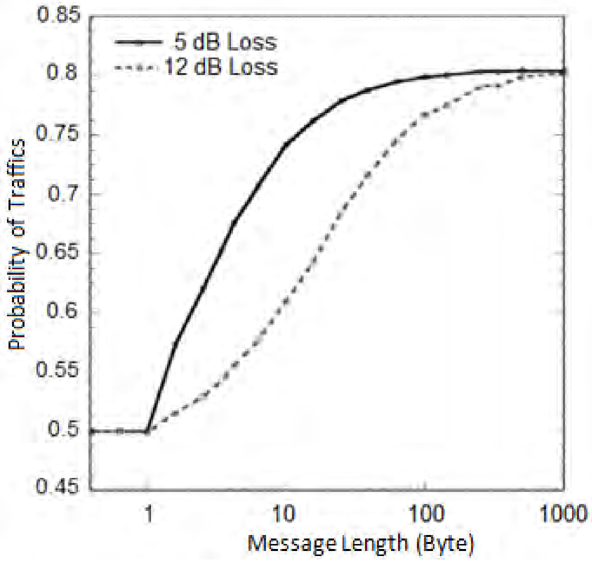


Figure 5 Correlation of Message Free Error

Security measures: Once the photons are polarized, they can't be accurately measured again, unless we use the same filter that initially produced their current states, making the quantum cryptography nearly unbreakable. Thus, the generated keys provide the perfect random sequence when the protocol is working as intended. There is no known way to break such quantum systems. However, the current implementations of quantum key distribution systems tend to be relatively slow, which prohibits their use in domains that require high security for key distribution. Despite the fact that quantum protocols are commonly used to securely produce and distribute cryptographic keys, the analysis we performed showed that the quantum system can be configured to communicate short security messages. Although the experiments are based on theoretical calculations, the proposed cryptosystem can be carried out on real quantum devices and supports different message sizes.

However, the high cost of simulating quantum circuits on classical computers makes the future of quantum cryptosystems one of real challenge.

VI. CONCLUSION AND FUTURE WORK

A number of different cryptographic techniques were analyzed in this paper to ensure the continuous security effect of these algorithms and to determine their security level. It was found, then, that many classical cryptography techniques that combine symmetric and public key encryption have potential security defects related to their key expansion and key refresh rate. Quantum cryptography was found to be a good alternative, but only useful for key distribution and exchanging session keys. Using quantum cryptographic systems for encrypting/decrypting long messages was demonstrated and the results showed that the quantum cryptosystem works well when applying wave division multiplexer on the quantum channel. This approach has proven to be quite effective, as it allows the optical channel to drive multiple traffic streams simultaneously, each one carrying its own independent stream of data. The experiment shows that the throughput rate is 20 K bit/s at 80 Km. By employing WVDM we can increase the throughput rate of the quantum cryptography system up to nearly 1 GHz. In future work, it is planned to run experiments to investigate the performance of such cryptosystem on long distance quantum communication channel.

VII. REFERENCES

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[2] Ibrahim A. Al-Kadi, "The Origins of cryptology: The Arab Contributions Cryptologia," April 1992.

[3] Mullen, Gary, Mummert, and Carl, "Finite Fields and Applications," American Mathematical Society, 2007, p. 112.

[4] Hans Delfs and Helmut Knebl, "Introductin to Cryptography: Principles and Applications," Information Security and Cryptography, Springer 2007, pp. 1-287.

[5] Ketu File white papers, “Symmetric vs. Asymmetric Encryption,” a division of Midwest Research Corporation.

[6] Tingyuan Nie and Teng Zhang, "A Study of DES and Blowfish Encryption Algorithm," IEEE, 2009.

[7] J. Daemen and V. Rijmen, "Announcing the Advanced Encryption Standard (AES)," Processing Standards, AES Proposal: Rijndael, November 2001.

[8] C. Adams and S. Lloyd, "Understanding PKI: Concepts, Standards, and Deployment Considerations," 2nd Edition, Addison Wesley, 2003.

[9] W. Stallings, "Cryptography and Netwrok Security: Principles and Practice", 5th Edition, Prentice Hall, 2011.

[10] O.P Verma, Ritu Agarwal, Dhiraj Dafouti, and Shobha Tyagi, "Peformance Analysis of Data Encryption Algorithms," IEEE, Delhi Technological University, India, 2011.

[11] 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.

[12] Alan Mink, Dbart, and S. Wiesner, “Quantum Cryptography or Unforgeable Subway Tokens Advances in Cryptology,” Proceedings of Crypto, August 1982.

[13] Ajit Singh and Nidhi Sharma, “Development of Mechanism for Enhancing Data Security in Quantum cryptography,” Advanced Computing: An International Journal (ACIJ), vol.2, no.3, May 2011.

[14] H. Kleinert, "Path Integrals in Quantum Mechanics," Statistics and Polymer Physics, World Scientific, Second extended edition, Singapore 1995, pp. 1–85.

[15] B. Schneier, "Applied Cryptorgaphy," John Wiley and Sons, Inc, 1996.

[16] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. Muñoz, and J. Capmany, "Simultaneous Transmission of 20x2 WDM/SCM-QKD and four Bidirectional Classical Channels Over a PON, " Opt. Express 20, 16358-16365, July 2012.

[17] N. Lutkenhaus, “Security Against Eavesdropping Attacks in Quantum Cryptography,” Phys. Rev. A, vol. 54, no. 1, 1996, pp. 97–111.

[18] V. Burenkov, B. Qi, B. Fortescue, and H.-K. Lo, “Security of High Speed Quantum Key Distribution with Finite Detector Dead Time”, arXiv.org:arXiv:1005.0272, May 2010.

[19] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Continuous Operation of High Bit Rate Quantum Key Distribution,” Appl. Phys. Ltr. 96, 161102, April, 2010.

[20] A. Mink and A. Nakassis,"LDPC for QKD Reconciliation," The Computing Science and Technology International Journal, vol. 2, no. 2, June 2012.

[21] P. Sebastian, N. Benjamin, T. Jakobsen, and M. Abyar, "Linear and Differential Cryptanalysis," University of Aarhus, Denmark, December 2006.

[22] Brute force attack. Wikipedia. http://en.wikipedia.org/wiki/ Bruteforceattack, [Accessed on April, 2014].

[23] M. Matsui, "Linear cryptanalysis method for DES cipher," Advances in Cryptology, EUROCRYPT’93, LNCS 765, Springer-Verlag, 1994, pp. 386–397.

[24] Eli Biham and Adi Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Advances in Cryptology, CRYPTO 1990, vol. 537 of Lecture Notes in Computer Science, Berlin, Heidelberg, New York, Springer Verlag, 1991, pp. 3-72.

[25] F.L. Bauer, "Decrypted Secrets: Methods and Maxims of Cryptology," 3rd Edition, Munich: Springer, 2002, pp. 271-300.

[26] DARPA-BAA-12-42, “Quiness: Macroscopic Quantum Communications," May 2012. https://www.fbo.gov/index?s=opportunity&mode=form&id=6a3a61d577305f71d9be268925c4b201&tab=core&_cview=0, [Accessed on April, 2014].

[27] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, “Experimental quantum cryptography” Jouranl of Cryptology 5 (1), Springer, 1992, pp. 3-28.

[28] S. J. van Enk, J. I. Cirac, and P. Zoller, "Photonic Channels for Quantum Communication," Science, vol. 279, no. 5348, 1998, pp. 205–208.

[29] D. Bouwmeester, A. Ekert, and A. Zeilinger, "The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation," 3rd Edition, Springer, 2001.

[30] Sheila Kinsella, "Online Measurement of Entanglement of a Quantum State," National University of Ireland, Galway, Ireland, March 2006.

[31] Lo, H.K., Chau, H.F., Ardehali, M: Efficient Quantum Key Distribution Scheme and Proof of its Unconditional Security," Journal of Cryptology 18, 133, 2005. http://www.citebase.org/abstract? id=oai:arXiv.org:quant-ph/0011056, [Accessed on April, 2014].

[32] Michael A. Nielsen and Isaac L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, 2000.

[33] P. Shor and J. Priskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Physical Review Letters, vol. 85, 2000, pp. 441 - 444.

[34] Mart Haitjema, A Survey of the Prominent Quantum Key Distribution Protocols, http://www.cs.wustl.edu/~jain/cse571-07/ftp/quantum/ index.html #b92 , [Accessed on April, 2014].

[35] C. H. Bennett and et al, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen (EPR) Channels," Physical Review Letters, vol. 70, no. 13, 1993, pp. 1895–1899.

[36] Rahul Aggarwal, Heeren Sharma and Deepak Gupta, "Analysis of Various Attacks over BB84 Qunantum Key Distribution Protocolss", International Journal of Computer Applications (0975-8887), vol. 20, no.8, pp.28-31, 2011.

[37] Bransao, F. et al, "Robust device-independent randomness amplification with few devices," Preprint at http://arxiv.org/abs/1310.4544, [Accessed on May, 2014]