Investigation of System Performance of Quantum Cryptography Key Distribution in Network Security

Mehrdad Sepehri Sharbaf
Senior IEEE Member
California State University Dominguez Hills
Computer Science Department
msharbaf@csudh.edu

Abstract

For the past decade progress in quantum cryptography changed the status of quantum key distribution (QKD) from laboratory to the practical innovation technology. Quantum cryptography is an emerging technology in which two parties can secure network communications by applying the phenomena of quantum physics. Quantum cryptography applies the uncertainty principle and the no-cloning theorem of quantum mechanics to provide ultra-secure encryption key distribution between two parties. Conventional secret-key cryptography techniques require the communication of a secret key prior to message exchange, and does not detect eavesdropping, and quantum principles can be used to detect eavesdropping probabilistically when it occurs. But there are challenges, and limitations to implement practical quantum cryptography such as detector performance for measuring photons, or optical sources which, enforce by the state-of-the-art components crucial for the system performance of quantum cryptography, and fiber optical distance range affect the system performance of quantum cryptography For that reason, the goal of this research is to investigate the system performance of quantum cryptography key distribution in network security, and this investigation develops a theoretical integrated research model or conceptual model framework concerning (figure 4) parameters which affect QKD system performance, and generates a key that affects by those variables.

To support the research the experimental data are performed, collected, and analyzed at MagiQ Technology in the Research & Development Lab. The rate of cryptography key or sifted key rate and the quantum bit error rate (QBER) are used to gauge the performance. The research presents a guideline to improve the system performance of the quantum cryptography.

Keywords-component; Quantum Crytography, QKD System Performance; System Conceptual Model; Quantun Bit Error

1.Introduction

Quantum cryptography concept developed by Charles H. Bennett and Gilles Brassard in 1984 (BB84) as part of research study between physics and information at IBM lab [9].This is the first known quantum distribution scheme. The quantum system is based on the distribution of single particles or photons, and the value of a classical bit encodes by the polarization of a photon [1]. According to [16] the key element of quantum communications is based on a quantum system which cannot only be in two states but also in a superposition of states, known as quantum bit ("qubit"). This 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 connected with the logic value "0" and "1", which mathematically are presented as:

|0> = |↓> |0> = |↗ >
|1> = |↑> |1> = |↖ >

To illustrate the concept behind the quantum cryptography, let's define the photon.

A photon is an elementary particle of light, carrying a fixed amount of energy. Based on physical law, light may be polarized; polarization is a physical property that emerges when light is regarded as an electromagnetic wave (refer to figure 1).

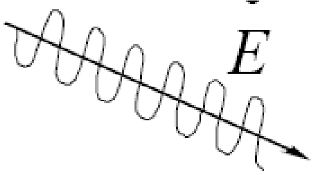


Figure 1. Light as an electromagnetic

According to [1] the direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter), and can be measured using a calcite crystal (refer to Table 1).

Table 1. Polarization state pairs.

Basis	State bit logic value	State bit logic value	Representation
rectilinear	Horizontal (0º) →	Vertical (90º) ↑	+
Diagonal	45º ↗	135º ↖	X

According to [10, 1] the protocol BB84 uses 4 quantum states that constitute 2 bases. This encoding scheme is public knowledge. If Alice wants to transmit the conventional bit 0 or 1, she may choose to use + and consequently send out over the quantum channel →, ↑, or choose to use x and consequently send out ↗ , ↖ , If Alice is sending only ↑ and → to Bob, the coding system shall identify that Alice is using the base +. For example, if Alice sends sequence of photons: ↑, ↑, →, →, the binary number represented with these states is 1100. Now, if Bob wants to obtain a binary number sent by Alice, he needs to receive each photon in the same basis. In this case, this is + basis. For each conventional bit to be transmitted in the QKD protocol Alice will set differently oriented polarizes + or x uniformly random. If Alice sends random sequence of photons: ++xx++xxx++xx+, the binary number represented with these states is 10110011001110 Now, if Bob wants to obtain a binary number sent by Alice, He needs to receive each photon in the same basis. [19, 20] explain the procedure of BB84 protocol as follows (also shown in figure 2. Excerpted from http://www.idquantique.com).

Alice sends Bob a sequence of photons, each independently chosen from one of the four polarizations- vertical, horizontal, 45-degree, and 135-degree. For each photon, Bob randomly chooses one of the two measurements bases (rectilinear or diagonal) to perform a measurement, and records his measurement bases and results, and later Bob publicly acknowledges his results. [16] states that because a photon is an indivisible elementary particle, the QKD communications can not be passively tapped in the conventional sense so adversaries would need to undertake far more risky active attacks. However, the Heisenberg Uncertainty Principle ensures that any active attack will not permit an attacker to faithfully read the key transmission [12, 19, 20].

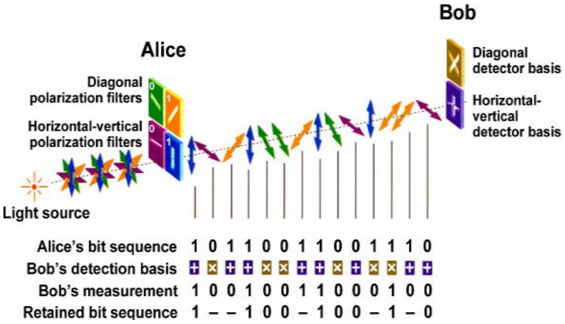

Bob
Alice
Diagonal polarization filters
0
1
Horizontal-vertical polarization filters
0
1
Diagonal detector basis
Horizontal-vertical detector basis
Light source
Alice's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
Bob's detection basis + x + + x x + + x + x x + +
Bob's measurement 1 0 0 1 0 0 1 1 0 0 0 1 0 0
Retained bit sequence 1 – – 1 0 0 – 1 0 0 – 1 – 0

Figure 2. [idquantique]Principle of the BB84 protocol Quantum Key Distribution (QKD) Protocol Implementation

Figure 2 presents in schematic form the basic steps required for QKD, reading upwards from the bottom as is typical of networking protocol stacks, along with the current techniques implemented for each step [14, 17, 18, 27, 28]. The figure 10 represents in accordance with the conventions of network engineering, in which the physical layer is depicted at the bottom of the diagram and higher layers depend on the products of those beneath them. According to [9] at the physical layer or VPN/OPC interface receive these frame of raw key symbols, and then they perform QKD protocol (sifting, error correction, privacy amplification etc.). To elaborate in detail about QKD protocol, the explanation of each stage presented.

Sifting is the process whereby Alice and Bob window away all the obvious "failed qubits" from a series of pulses. Sifting allows Alice and Bob reconcile their "raw" secret bit streams to remove the errors. According to [9] at the end of this process, i.e. after a sift and sift response transaction-Alice and Bob discard all the useless symbols, and leaving only those symbols that Bob received and for which Bob's basis matches Alice's symbols. According to [9] some of the most common errors in sifting are: (a) Alice's source did not actually emit a photon; (b) that photon was lost in transmission; (c) Eve captured the photon and did not replace it; (d) Bob's detector did not fire when the photon hit it; (e) wrong basis symbols between Alice and Bob; (f) Multiple detection symbols in which more than one Bob's detector's fired. The Shannon's theorem (1949) [25] states that in any condition, the amount of information Bob has should exceed the information possessed by Eve, i.e. Bob must have more information on Alice's bits than Eve. If this is not the case, then the bits transmitted so far discarded and the previous steps are carried on again until this condition is satisfied.

Error correction is always probabilistic-unless all bits are revealed during the process. Error detection and correction allows Alice and Bob to determine all the "error bits" among their shared, sifted bits, and correct them so that Alice and bob share the same sequence of error-corrected bits. The process of error detection allows Alice and Bob to estimate the current Quantum Bit Error Rate (QBER) on the quantum channel between them, which can then be used as input for privacy amplification. Also to eliminate errors due to incorrect choices of measurement basis, errors induced by Eve eavesdropping, and errors due to channel noise, if any exists. Privacy Amplification is the process whereby Alice and Bob reduce Eve's knowledge of their shared bits to an acceptable level. As [9] states that privacy amplification depends on having an accurate estimate of the eavesdropping-free entropy sifted and error correction secret bit sequences. According to [12] privacy amplification is the fourth step which is applied to minimize the number of bits that an eavesdropper knows in the final key. According to [9] Alice and Bob must perform a final step in order to establish a perfectly secret key: this is the process of privacy amplification. The process of reconciliation results in a bit sequence which is common to Alice and Bob, but some of its bits may be known to an eavesdropper who has tapped the classical channel. To eliminate this "leaked" information, Alice and Bob must apply, in common, a binary transformation (usually, a random permutation) to their sequences, and discard a subset of bits from the result. The precise choice of transformation and the number of bits discarded, of course, determine the amount of secrecy of the final key. The objective of this step is to minimize the quantity of correct information which the eavesdropper may have obtained about Alice and Bob's common bit sequence. Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. It's important fact that an incorrect estimate may lead to insufficient privacy amplification, and thus allow Eve to know more about the resultant "secret" bits than expected.

2. System Performance of Quantum Cryptography

The system performance of quantum cryptography or the over system range performance and throughput, are limited by detection efficiency, optical source efficiency, and fiber link loss [30, 31]. Also [13] argue about the limitation of detector efficiency on the system performance of quantum cryptography. Other scholars such as [27] discuss about backscattering limitation to the system performance of QKD, and [34] elaborate more about source efficiency, detector efficiency, and link loss related to the performance of QKD.

Also the scholars argue that the secure key generation rate of a quantum cryptography system is highly sensitive to the error rate due to eavesdropper [2, 4, 10, 12, 13, 32]. In the process of QKD BB84 Protocol implementation of the raw key creation is one of the important parameters to characterize the performance of QKD system [9, 11, 22]. The raw rate in the protocol is defined as:

$$\mathrm{Rate}_{\mathrm{raw}}=q\mu f\eta_d\eta_l \qquad (1)$$

where q is a setup dependent coefficient, or where is the systematic factor, which is .5 for four state of BB84 protocol, μ is the mean number photons per pulse, f is the laser pulsing frequency, η_d is the photon's detection probability or the detector efficiency, and η_l is the transfer efficiency of the link or the transmission coefficient of the link between the active receiving station and Alice's detector. As it stated in this paper, sifting is the process whereby Alice and Bob window away all the obvious "failed qubits" from a series of pulses. Sifting allows Alice and Bob reconcile their "raw" secret bit streams to remove the errors. The sifted key rate is used to gauge the performance of the QKD [9, 13, 30]. The equation for sifted key rated can be expressed as:

$$\mathrm{Rate}_{\mathrm{sift}}=1/2\mu f\eta_d\eta_l \qquad (2)$$

Where the sifted key corresponds to the cases in which Alice and Bob made compatible choices of bases, hence its rate is half that of the raw key. For that reason [11] express that the raw rate is essentially the product of the pulse rate f_{rep}, the mean number of photons per pulse μ, the probability t_{link} of a photon to arrive at the analyzer and the probability η of the photon being detected:

$$R_{\mathrm{sift}} = ½\, R_{\mathrm{raw}} = ½\, q\, t_{\mathrm{link}}\, f_{rep}\, \mu \qquad (3)$$

The quantum bit error rate (QBER) which is also an important parameter to characterize the QKD system. It is used to gauge the performance of quantum cryptography [11, 12, 32, 33]. The QBER equation can be expressed as:

$$\mathrm{QBER}=\frac{Fasle-Counts}{Total-Counts}=\frac{Fasle-Counts}{False-Counts+Correct-\ Counts}=\frac{N\ wrong}{N\ right+N\ wrong}=\frac{Rerror}{Rsift+Rerror}\approx\frac{Rerror}{Rsift} \quad (4)$$

The QBER is defined as the number of wrong bits to the total number of received bits.

According to [7] the QBER for the faint laser pulse QKD can be written as a sum of two main contributing factors:

$$\mathrm{QBER} = \mathrm{QBERopt} + \mathrm{QBERdet} = P_{\mathrm{opt}} + P_{\mathrm{noise}}/P_{\mathrm{photon}} = P_{\mathrm{opt}} + P_{\mathrm{noise}}/\mu\eta_d\eta_l, \qquad (5)$$

where P_{opt} is the probability of a photon going to the wrong detector, and P_{nois} is the probability of getting a noise-count (mainly dark counts) per gating pulse window. For the phase-based

$$\mathrm{QKD}: = P_{\mathrm{opt}} = (1\text{-}V)/2 \qquad (6)$$

where V is the interference visibility. Also [10, 11] present the QBER in different way as follows:

$$QBER = \frac{p_{\mathrm{opt}}p_{\mathrm{phot}} + p_{\mathrm{dark}}}{p_{\mathrm{phot}} + 2p_{\mathrm{dark}}} \cong p_{\mathrm{opt}} + \frac{p_{\mathrm{dark}}}{p_{\mathrm{phot}}} \equiv QBER_{\mathrm{opt}} + QBER_{\mathrm{det}} \qquad (7)$$

where p_{dark} and p_{phot} are, respectively, the probabilities of getting a dark count and a photon count and p_{opt} is the probability that a photon is detected by the wrong detector, due to the limited interference fringe visibility or due to poor polarization alignment. Equation (6) holds for a system implementing the BB84 protocol.

The probability of getting a photon count is given by:

$$P_{\mathrm{shot}} = \mu\eta_t\eta_d \qquad (8)$$

And

$P_{dark} = n_{dark}\Delta t$ (9)

where n_{dark} is the single photon avalanche diode(SPAD) dark counting rate (dark counts per second) and Δt is the detection time window. Based on that:

$$QBER_{\mathrm{det}} = \frac{n_{\mathrm{dark}}}{\eta_{\mathrm{d}}} \frac{\Delta t}{\mu \eta_{\mathrm{t}}} \quad (10)$$

$QBER_{det}$ is inversely proportional to the system's transmission efficiency.

Based on a thorough review of theoretical background, this investigation establishes the following questions:

Research Questions

R1: Does the detector affect to the QKD performance?
R2: Does the optical source affect to the QKD performance?
R3: Does the fiber optical distance range affect to the QKD performance?
R4: Is there a relationship between the rate of cryptography key or sifted key rate and the quantum bit error rate (QBER) to the performance of QKD?

Research Hypotheses

The hypotheses are derived directly from the research questions, and are posed in a format so that a determination can be made as to whether the data subsequently collected at MagiQ Technology R & D Lab, provides support for them or not.

H1: The detector does affect to the QKD performance.
H2: The optical source does affect to the QKD performance.
H3: The fiber optical range does affect to the QKD performance.
H4: There is a relationship between the rate of cryptography key or sifted key rate and the quantum bit error rate (QBER) to the performance of QKD.

Based on above research questions, and research hypotheses, this investigation develops a theoretical integrated research model or conceptual model framework concerning (figure 4) parameters which affect QKD system performance. Conceptual frameworks (theoretical frameworks) are a type of intermediate theory that attempt to connect to all aspects of inquiry (e.g., problem definition, purpose, literature review, methodology, data collection and analysis). Conceptual frameworks can act like maps that give coherence to empirical inquiry.

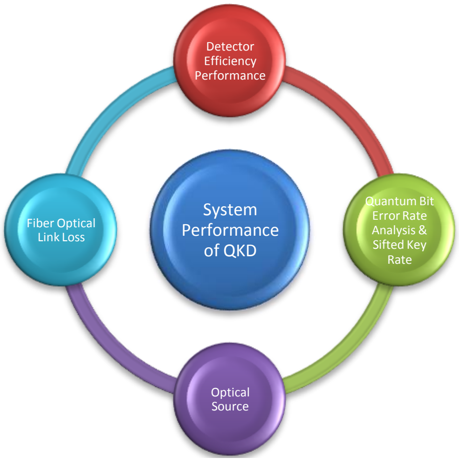

Detector Efficiency Performance
Fiber Optical Link Loss
System Performance of QKD
Quantum Bit Error Rate Analysis & Sifted Key Rate
Optical Source

Figure 4. Conceptual Model

To build a commercial QKD system there are majors challenges such as interferometry, extra photons, single-photon detection, and distance limitation. To investigate performance of QKD, the research paper examines a typical QKD system consists of two parties (Alice, and Bob) exchanging weak optical signals through the quantum channel at MagiQ Technology in the Research & Development Lab (figure 5).

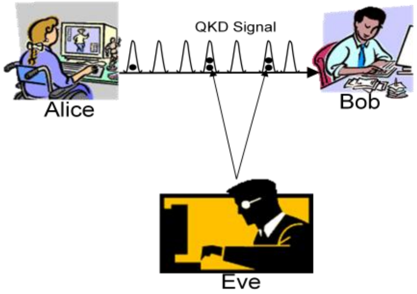


Figure 5

In real application, because of the limited availability of single photon sources, the research examines weak coherent pulses (WCP). The use of the WCP as compare to single photon source greatly simplified QKD apparatus, but WCP can contain more than one photon. If Alice uses weak coherent pulses (WCP), the probability of finding **n** photons in a pulse with the average photon number μ follows the Poisson statistics [33]:

$$P_{\mu}(n) = e^{-\mu}\,\mu^{n}/n! \quad (11)$$

Presence of multiphotons pulses creates a possibility of Eve’s photon splitting attacks [33]. Using WCP increases vulnerability of the QKD system with the loss of the channel [32, 33]. In order to keep the link secure, Alice must maximize the difference between numbers of photons successfully deliver to Bob’s detector, and the total number of the multiple-photon pulses. For that reason μ needs to stay low: (μ = η- is the channel transmittivity) to guarantee the security as the link distance (loss) increase [31, 32, 33]. In the case of zero channel loss, the optimization always takes place at μ=.5. This condition is accepted by most of the research groups [33, 34].

Also performance of a WCP QKD depends on the detector efficiency to detect the pulse, and dark current noise as well as the interferometer insertion loss, and the security model used through the choice of the mean photon numbers [30]. For that reason certain amount of errors can be accomplished by procedures known as error correction and privacy amplification. In this investigation the goal is to maximize the secure key rate under the theoretical conditions to reduce the probability of information leakage below predefined value. In this research it defines secure bit gain by G which is the probability of secure bit out of single initial pulse. The gain of the secure bits is dependent on the losses in the fibre link αL (where α denotes losses [dB/km], and L is the fibre length[km], quantum efficiency of the detector, visibility of interferometer V, and probability of the dark count of the detector P_{DC}. The first protocol Alice and Bob run is sifting. The sifted key contains errors. Alice and Bob have to run some error corrections protocol to estimate secure bits lost due to error correction. The protocol to define the requirement is Cascade [3, 21]. Based on numerical simulation cascade the raw bits are needed for the error correction, this can be done by work published by [3, 21, 33], where equation (12):

$$H = - f (e \log_2 e - (1 - e) \log_2 (1 - e))$$

The corrected sifted key is not completely secure due to privacy amplification. Alice and Bob have to run a privacy amplification protocol to establish the final secure key. This can be done by work published by [33] equation (13).

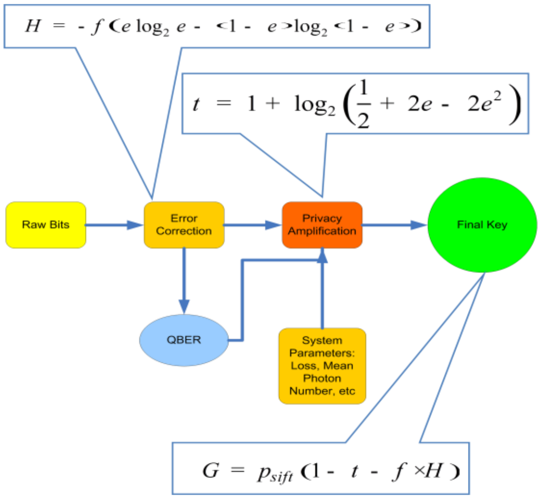
$$t = 1 + \log_2 \left(\frac{1}{2} + 2e - 2e^2 \right)$$

Based on additionally, quantum cryptography requires the use of privacy amplification to reduce, or eliminate, any potential information an adversary could have gained by interacting with the quantum transmission, privacy amplification increases security by combining several bits in the initial key to form each bit of the final key, reducing the length of the key in the process. This process becomes very inefficient as the error rate increases because the privacy amplification algorithm must essentially sacrifice exponentially many initial key bits in order to extract a single secure key bit.

Finally, the secure bit gain can be written as equation (14): $G = p_{sift} (1 - t - f \times H)$

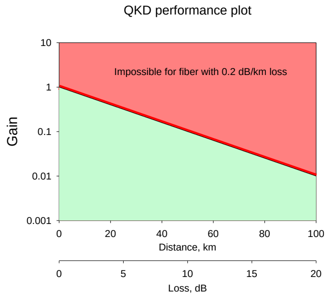
And Key Rate=Gain X Rep Pulse Rate

Figure 8. illustrates the procedures for the final secure key.


$H = - f (e \log_2 e - (1 - e) \log_2 (1 - e))$
$t = 1 + \log_2 \left(\frac{1}{2} + 2e - 2e^2 \right)$
Raw Bits
Error Correction
Privacy Amplification
Final Key
QBER
System Parameters: Loss, Mean Photon Number, etc
$G = p_{sift} (1 - t - f \times H)$

The final secure key depends to the system parameters such as mean photon number, loss ,detector efficiency, etc. The optimal mean number of photons can be found by maximizing G.

For the fixed detector temperature and transmission distance, optimization for the QKD can be achieved by increasing the strength of the optical signal sent by Alice. As μ is increased, Bob’s detector’s receives more photons, increasing the gain per pulse. But based on equation (14), the number of bits applied by error correction and privacy increases up as well which resulting in a decrease in gain. Figure 9 shows secure bit gain as a function of QKD transmission distance. As you see secure bit gain decreases as distance increase. It also suggests, an optimal value of μ does not depend on the detector operational parameters , but it is function of the link loss only Figure 9. [31, 15]



After μ optimization is performed, it needs to optimize the detector operational point in order to extract maximum performance from the system. For that reason it is essential to specify characteristic of the detector, such as quantum efficiency of the detector (QE), dark current probability (DC), and afterpulsing probability. Quantum efficiency of the detector (QE) is the probability of detector detects a true click from a single photon in given time slot. In another word , the quantum efficiency is the number of photons that can be detected as a photocurrent divided by the number of the incident photons. Based on definition, it's true click. Dark current probability is the probability of detector detects a false click containing no photon in a time slot. In another word, the dark current is a small current which flows when a reverse voltage is applied to a photodiode even in dark state. This is a major source of noise for applications in which a reverse voltage is applied to photodiodes. Based on definition, noise creates false click. Afterpulsing probability is the probability of getting a false click condition on the probability of getting click from previous time slot. The detector characteristics are effect to the system performance of QKD. For the system to detect reliable bit is a challenge. The quantum bit error is proportional to the ratio of the erroneous clicks in Bob's detector to the total number of photons registered. In real application QKD system, three main factors to the error count are: dark current in the detector (dark current probability, is the probability of detector detects a false click containing no photon in a time slot), and finite visibility of interferometer (probability of a detector misguided to a wrong detector), and afterpulsing probability which can be reduced by cooling down the detector. Also as link loss increases with distance, less photon arrive to Bob's detector. For that reason detector noise stays constant which that reflects to increase of QBER. As a guideline to improve the QKD system performance, a system designer could first to choose μ based on the known fibre loss, and then concentrates to optimize the system performance by adjusting detector parameters.

3. Conclusion:

It is possible to apply quantum cryptography key distribution to secure the bit communication at the current level of technology development. BB84 protocol can provide a secure communication link between Alice and Bob. The investigation of this research demonstrates that the system performance of QKD in network security affects by those variables which we discussed in our research questions. The research also provides guidelines for the optimization of QKD. There is a definite space for further improvement in photon collection efficiency, detector performance, and interferometer loss. By optimizing the system variables, a WCP QKD link can provide a stable secure communication against eavesdroppers.

4. Acknowledgement:

The author is grateful to Dr. Anton Zavriyev, Director of R & D in MagiQ Technology company for his technical advise, support, and help in this research paper.

5. References:

[1] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J., "Experimental quantum cryptography". *Journal of Cryptology, 5(*1), 1992 p. 3-28.

[2] Bogdanski, J., Rafiei, N., & Bourennane, M. (2008). Five-user QKD over switched fiber networks. *Proceeding of SPIE Vol. 7092,* P. 70920k-1-8.

[3]BRASSARD, G. and SALVAIL, L., 1994, in Advances in Cryptology- *EUROCRYPT '93,* Vol. 765, edited by T. Helleseth (Berlin: Springer), p. 410.

[4] Bruss, D., Erdelyi, G., Meyer, T., Riege, T., & Rothe, J., " Quantum cryptography: A survey". *ACM Computing Surveys, 39(*2), 2007, p. 1-27.

[5] Buchmann, J., May, A., & Vollmer U., "Perspective for cryptographic long-term security". *Communications of ACM. 49(*9), 2006, p. 50-56.

[6] Coron, J. S., " What is cryptography?", *IEEE Security & Privacy Journal, 12(8), 2006, p. 70-73.*

[7] Curcic, T., Filipkowski, M. E., Chtchelkanova, A., D'Ambrosio, P. A., Wolf, S. A., Foster, M., & Cochran, D., "Quantum Networks: From Quantum Cryptography to Quantum Architecture", *ACM SIGCOMM Computer Communication Review,* Vol.34, No.5, 2004, pp. 3-8.

[8] Davis, J., "Information Systems Security Engineering: A critical Components of the Systems Engineering Lifecycle", *ACM SIGAda,* 2004, pp.13-17.

[9] Elliot, C., "Quantum Cryptography", *IEEE Security & Privacy Journal*, 2004, pp. 57-61.

[10] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2008). Quantum Cryptography. *Review Moderns Physics, arXiv: quantum-ph/0101098v2*, p. 1-57.

[11] Gisin, N., & Thew, R. (2008). Quantum Communication. *Physics Review, arXiv:quant-ph/0703255v1*.

[12] Gumus E., Aydin, G., & Aydin M. (2007). Quantum cryptograhpu and comparison of quantum distribution protocols, *Journal of Electrical & Electronics Engineering, 8(*1), 2008.

[13] Jacobs, B., Hendrickson, S., Dennis M., & Franson, J. (2006). Quantum cryptography at 830nm in standard telecommunications fiber. *Poceeding of SPIE* Vol. 6244, p. 62440H-1-11.

[14] Khan M. M., Hyder, S., Pathan, M., & Sheikh, K. H. (2006). A quantum key distribution network through single mode optical fiber. *Proceeding of International Symposium on Collaborative Technologies and Systems.* p.13-19.

[15] Internet Resources:
http://www.magiqtech.com
www.idquantique.com

[16]Kartalopoulos, S. V. (2007). Quantum cryptography for secure optical networks, *Proceedings of IEEE ICC Conference*, p. 1311-1316.

[17] Li, X., & Zhang, D., "Quantum information authentication using entangled states", *IEEE Computer Society, International Conference on Digital Telecommunications*, 2006, pp. 64.

[18] Liu, S., Sullivan, J., & Ormaner, J. "A practical approach to enterprise IT security". *IEEE IT Professional Journal*, *9(*3), 2001, p. 35-42.

[19]Lo , H. K., & Lutkenhaus, N. (2007). Quantum cryptography: from theory to practice. *arXiv:quant-ph/0702202v3*

[20]Lo H. K., & Zhao, Y. (2008) Quantum Cryptography. *Physics Review, arXiv:quant-ph/0803.2507v4*

[21]LUTKENHAUS, N., 2000, Phys. Rev. A, 61, 052304.

[22]Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM, 48(*3), p. 351-406.

[23]Mollin, R. A. (2005), RSA and public key cryptography. *ACM SIGACT News, 36(*2), p. 14-20.

[24] Rothe, J. (2002). Some facets of complexity theory and cryptography: A five-lecture tutorial. *ACM Computing Surveys, 34(*4), p. 504-549.

[25] Shannon, E. C., "Communication theory of secrecy system", *Bell System Technical Journal,* Vol.28, No.4, 1949, pp.656-715.

[26] Steane, M. A., & Rieffel, G. W., "Beyond bits: The future of quantum information processing", *IEEE Computer*, 2000, pp. 38-45.

[27] Subacius, D., Zavriyev A., & Trifonov, A. (2005). Backscattering limitation for fiber-optic quantum key distribution systems. *Applied Physcis Letter, 82*(1), p. 1-3.

[30] Teja, V., Banerjee, P., Sharma N. N., & Mittal, R. K. (2007). Quantum Cryptography: State-of-art , challenges, and future perspective, *Proceeding of the 7th IEEE International Conference on Nanotechnology*, p. 1296-1301.

[31] Trifonov, A., Subacius, D., Berzanskis, A., & Zavriyev, A. (2004). Single photon counting at telecom wavelength and quantum key distribution. *Journal of Modern Optics, Vol. 15*(9), p.1399-1415.

[32] Trifonov, A., Zavriyev, A., Subacius, D., Alleaume, R., & Roch J. F. (2005). Practical quantum cryptography. *Journal of Optical Society of America,* p. 13-21.

[33] Trifonov, A., Zavriyev, A.,(2004). Practical single photon source for quantum communications. *Journal of Optics B: Quantum and Semiclassical Optics. P. 25-29.*

[34] Trifonov, A., Zavriyev, A.,(2005).Secure communication with a heralded single-photon source. *Journal of Optics B: Quantum and Semiclassical Optics. P. 772-777.*

[35] Wang B. C., Kumavor, P., Yelin S. F., & Beal A. C. (20005). Multi-user quantum cryptography. *Proceeding of SPIE Vol. 6014*, p. 601416-1-12.

[36] Wootters, W. K., & Zurek, W. H., "A single quantum cannot be cloned". *Nature*, 299, 1982, p. 802.