Defence Science Journal, Vol. 66, No. 2, March 2016, pp.186-192, DOI : 10.14429/dsj.66.9771


# Effect of Noise on Practical Quantum Communication Systems

Vishal Sharma

*Indian Institute of Technology, Jodhpur - 342 011, India*
*E-mail: pg201383506@iitj.ac.in*

**ABSTRACT**

Entanglement is an important resource for various applications of quantum computation. Another important endeavor is to establish the role of entanglement in practical implementation where system of interest is affected by various kinds of noisy channels. Here, a single classical bit is used to send information under the influence of a noisy quantum channel. The entanglement content of quantum states is computed under noisy channels such as amplitude damping, phase damping, squeesed generalised amplitude damping, Pauli channels and various collective noise models on the protocols of quantum key distribution.

**Keywords:** Entanglement, quantum noise, markov process, optical-fiber, optical communication

## 1. INTRODUCTION

Entanglement plays a major role in quantum information theory[1]. Entangled quantum states find many applications in the fields like quantum cryptography[2], quantum computation[3,4], teleportation[5,6]. Entanglement properties are deployed in many areas as a resource to get effective results[8]. There are a number of facets of entanglement such as concurrence[7], distillable entanglement[9] and entanglement cost[9].

It is important to know the strength of entanglement in applications of quantum communication under noisy environment. We use 0 and 1 as classical information[14,35] for transmission under noisy quantum channels, for e.g., amplitude damping and Pauli channels, for the scenario where Alice and Bob act as transmitter (sender) and receiver following the postulates of quantum physics to encrypt and decrypt the information being sent. The simulation results show the amount of average error probability to judge the effect of entanglement under noisy channels for the quality of quantum communication being done. The aim is to achieve error free communication between Alice and Bob.

Cryptography based on the laws of quantum mechanics takes advantage of, say a photon as an information carrier that provides unconditional security against eavesdroppers for practical long distance communication with the help of optical fibers. This can only be success full when very efficient quantum repeaters are deployed to maintain the strength of the quantum signals at the end of the receiver side.

Quantum key distribution (QKD) is one of the important techniques in the area of secure communication network. It is based on key exchange phenomenon that is opposite to classical cryptography where key distribution is used for security. For symmetric key cryptosystems, the same secret key is required for both the users to perform encryption and decryption. This drawback is solved in public key cryptography but it is unsecure because of various attacks[27]. Diffie-Hellman key exchange is a classical key exchange protocol but more complex to perform in polynomial time for some selected problems[27,28]. All these methods are not unconditionally secure and data can be altered and duplicated by an eavesdropper, say Eve, in between the communication link at any point even without notice of the communicating parties. QKD is based on the No-Cloning theorem that is quantum mechanically and unconditionally secure and any changes in original data alerts the transmitter and receiver,hence providing high security from eavesdroppers[29,30,31,37].

Quantum key distribution simulation and error reconciliation is implemented by OptiSystem and other related softwares installed on a PC to obtain a high key rate for transmission of the quantum information. Field programmable gate array (FPGA) is one of the efficient hardwares used to perform practical QKD protocols. Features of FPGA include its simplicity for bit-wise operation, fast and parallel computing and large integrated RAM[32].

## 2. PRELIMINARIES

We start our discussion from the fundamentals of quantum computing that is required to understand the further theory used in quantum communication under noisy conditions. The transmission of any quantum state under noisy conditions can be represented with the help of a trace preserving completely positive map. This mapping occurs due to the interaction between environment and the system of interest. Mathematically, in quantum prospect this can be written as

$$\rho \rightarrow \phi(\rho) = tr_{env}\left(U(\rho \otimes \rho_{env})U^{\dagger}\right) \tag{1}$$

where U as well as ρ are written for the unitary interaction between system and environment and density operators on a Hilbert space $H_d$ of dimension-d respectively. Partial trace

Received 16 December 2015, revised 28 January 2016, online published 22 March 2016

over environment's Hilbert space is denoted by $tr_{env}$. The Kraus representation is used to represent all noisy models[10]. Alternatively, we can write Eqn. (1) as follows:

$$\phi(\rho) = \sum_i A_i \rho A_i^{\dagger} \tag{2}$$

where the $A_i$'s must satisfy the completeness condition

$$\sum_i A_i A_i^{\dagger} = I \tag{3}$$

The operators which fulfill the criteria from Eqn. (1) to (3) is essentially considered under noisy channel condition. Similarly, for two transmissions through the channel the Kraus operator representation is as follows

$$R \to \phi(R) = \sum_{i,j} (A_i \otimes A_j) R (A_i \otimes A_j)^{\dagger} \tag{4}$$

here $R$ represents density operator for $H_d \otimes H_d$ Hilbert space that is on the $d^2$ dimension.

Encoding at Alice's side is performed in one of the two states $R_0$ and on the specified Hilbert space $H_d \otimes H_d$ . This encoding is performed on the transmitted bit sent to Bob. After this, Alice sends these states via channel. Bob uses the action of the channel given in Eqn. (4) to get output in one of the two possible operators $R_0$ and $R_1$ at the receiving end. $Tr(R_s E_b)$ is the probability value in Bob's measurement, which depends on the bit value sent by Alice and the method of maximum likelihood that depends on the values of bits $b$ and $s$ to make $Tr(R_s E_b)$ maximum. The average error probability is written as

$$P_e = \frac{1}{2} \sum_b \min\{tr(R_0 E_b), tr(R_1 E_b)\} \tag{5}$$

Bob performs von Neumann measurement to get $P_e$ minimum, hence

$$P_e = \frac{1}{2} - \frac{1}{4} tr\left|R_1 - R_0\right| \tag{6}$$

Concurrence is used to measure the entanglement amount, the entanglement strength and considered as an independent entanglement measure. Concurrence for a pure state $|\psi\rangle$ with bipartite two-level systems is defined as[12, 22]

$$C(|\psi\rangle) = \langle \psi^* | \sigma_2 \otimes \sigma_2 | \psi \rangle \tag{7}$$

here $|\psi^*\rangle$ is the complex conjugate of pure state $|\psi\rangle$, $\sigma_2$ is the Pauli y-matrix defined as $\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Concurrence for a given mixed state is written as

$$C(\rho) = \inf\, p_i, \psi_i \sum_i p_i c_i(\psi) \tag{8}$$

where $p_i > 0$, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ and

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\} \tag{9}$$

here $\lambda_i$ represents decreasing eigenvalues of the Hermitian matrix $R = \sqrt{\sqrt{\rho}\,\tilde{\rho}\,\sqrt{\rho}}$ and $\tilde{\rho} = (\sigma_2 \otimes \sigma_2)\rho^*(\sigma_2 \otimes \sigma_2)$. Hence, different values of the $\lambda_i$ are the square roots corresponds to the eigenvalues of non-Hermitian matrix[22] $\rho\tilde{\rho}$ .

## 3. THE EFFECT OF VARIOUS KINDS OF NOISES ON THE QUANTUM STATES

Here we consider only some specific noise models like amplitude damping, phase-damping and two types of collective noises for the interaction with the quantum states transmitting between Alice and Bob. We follow the method used[13] for the information transfer under noisy environment. Let the quantum density state is $\rho = |\psi\rangle\langle\psi|$, here $|\psi\rangle$ is any n qubit initial pure quantum state before transmission. Under noisy conditions the transmitted pure state evolves as follows:

$$\rho_k = \Sigma_{ij} E_{i1}^k \otimes E_{i2}^k \otimes ----- \otimes E_{in}^k \rho (E_{i1}^k \otimes E_{i2}^k \otimes ------ \otimes E_{in}^k)^{\dagger} \tag{10}$$

where $E_{ij}^k$ denotes Kraus operator for specific type of noisy channel under consideration applied on desired qubit of the travelling quantum state. The evolution of density matrix undercollective noise models can be written as

$$\rho_k = U_i^{\otimes n} \rho U_i^{\dagger \otimes n} \tag{11}$$

here $k$ represents type of noisy channel used, and $U_i$ is a 2 x 2 matrix (it works on a single qubit) for collective dephasing andcollective rotation noises. After obtaining the transformed density matrix $\rho_k$, the normalization can be achieved by calculating the trace to be 1. We can make it one by dividing it by the trace of the transformed matrix $\rho_k$ .

$$\rho_{k1} = \frac{\rho_k}{Tr(\rho_k)},$$

where $\rho_{k_1}$ is the normalized transformed matrix.It is expected that the receiver gets the exact state $(\rho = |\psi\rangle\langle\psi|)$ sent by the sender in the absence of any noise andeavesdropping, hence we can compare this state with $\rho_k$ , (quantum state obtained in presence of noise). This comparisonparameter is known as fidelity and can be expressed as[21]

$$F = \langle\psi|\rho_k|\psi\rangle \tag{12}$$

The above mentioned equation of fidelity differs from conventional expression of fidelity. For two different quantum states say $\sigma$ and $\rho$ the fidelity is written as

$$F_c(\sigma, \rho) = Tr[\sqrt{\sigma^{\frac{1}{2}} \rho \sigma^{\frac{1}{2}}}].$$

The subscript $F_c$ denotes the conventional fidelity. In ideal cases the fidelity is one, but it decreases under noisy environment as shown by the simulated results in the following figures.

## 4. THE NOISE MODELS UNDER STUDY AND THE SIMULATION RESULTS

For the practical implementation of QKD protocol, there are dedicated hardwares available like XILINX based SPARTAN v3 FPGA clocked at 24 MHz. It is similar to an embedded hardware[35,36] which includes all the necessary devices and components mounted on a single chip, where clock is used for USB interfaced with PC, 1 Mbps counter value as the quantum key bits are decided by the divider circuit.

power section and phase-locked loop (PLL) is monitored by controlled commands sent by FPGA. The gated avalanche photodiode (APD) needs a pulse generation of approximately 20 ns for quantum channel, this pulse generation is generated by a digital clock manager (DCM). DCM is also responsible for the generation of 48 MHz clock to regulate the functioning of the FPGA board. Static random-access memory (SRAM) on the FPGA hardware is an important building block used to store and process the data[32,33]. Any eavesdropping attempt between the communicating parties perturbs the quantum information, hence as per no-cloning theorem Eve's presence can be detected. The DPS QKD protocol as shown in Fig. 1 is used for long distance communication between the repeater nodes and practically less complex compared to other existing quantum communication systems. The DPS QKD system is functionally compatible with optical devices and networks because of it's integrity with these devices hence it is an important component for the whole area of network security[34].

Figure 1 shown, the DPS QKD system uses optical-fiber as a quantum channel and both the sender and receiver communicates via weak coherent pulses with encoding of logical bits in terms of relative phase of these pulses. Encoding and decoding of the logical bits are performed with two signals both at transmitter and receiver side. The working principle of DPS QKD system is similar to B92 protocol, the encoding and decoding of sent pulses depends on the relative phases, if these are in phase that means encoded and decoded as 0, if relative phase is $\pi$, the logical bit is 1. Moreover some kind of security threats has to be considered because of weak coherent pulses (WCP) leave some of loop holes for eavesdroppers hence photon number splitting attack is the main concern of DPS QKD protocol[34].

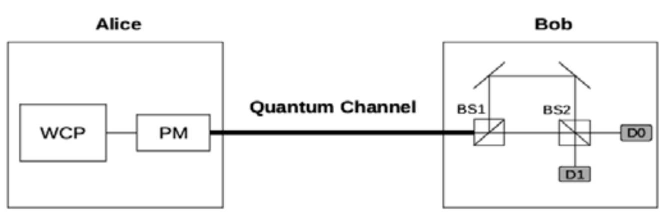


**Figure 1. Block diagram of DPS (differential phase shift) QKD protocol.**

In practical implementation of any quantum communication, system-environment interaction occur which results in decoherence. The time evolution of such open quantum systems in Markovian environment can be explained with master equation in the Lindblad form as[1, 15,16].

$$\frac{\partial\rho}{\partial t}=-\frac{i}{\hbar}[H,\rho]+\Sigma_{j,\alpha}\left(L_{j,\alpha}\rho L_{j,\alpha}^{\dagger}-\frac{1}{2}L_{j,\alpha}^{\dagger}L_{j,\alpha}\rho-\frac{1}{2}\rho L_{j,\alpha}^{\dagger}L_{j,\alpha}\right) \tag{13}$$

here $H$ is the Hamiltonian of the system and $H=0$ is considered just for the simplicity. The Lindblad operators show the coupling between system and the environment under consideration, hence in $L_{j,\alpha}=\sqrt{\lambda_{j,\alpha}}\sigma_{\alpha}^{j}$ operator, $\sigma_{\alpha}^{j}$ represents the Pauli operators of the *j-th* qubit, where $\alpha=x,y,z$ and $L_{j,\alpha}$ denotes it's action on the *j-th* qubit to represent the coupling between system-environment under consideration.

Here the Figs. 2 and 3 shows the python simulation results for master equation mentioned above and the Bloch sphere representation for qubit distribution respectively.

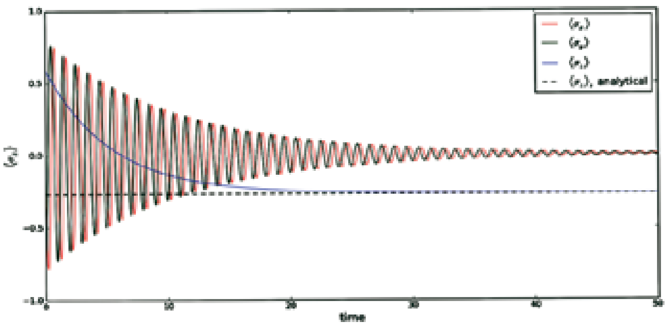


**Figure 2. Simulation result of master equation indicates that the dissipation is faster in squeezed vacuum compared to vacuum (blue and red lines shows the squeezed vacuum and vacuum, respectively).**

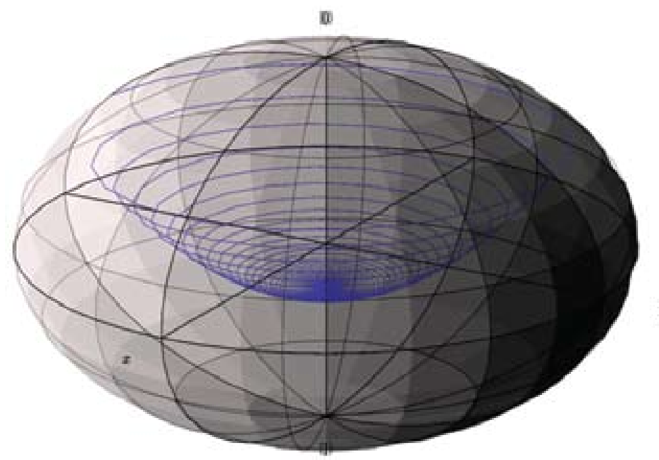

**Figure 3. Bloch sphere representation for qubit distribution.**

### 4.1 QKD Protocol under Amplitude-Damping and Phase-Damping Noise

In this section, considering noisy conditions on quantum key distribution (QKD) protocol, the travel qubits interact with the amplitude-damping noise or the phase-damping noise. The Kraus operators for Amplitude-damping noise model is written as[13]

$$E_0^A=\begin{bmatrix}1 & 0\\ 0 & \sqrt{1-\eta_A}\end{bmatrix};\ E_1^A=\begin{bmatrix}0 & \sqrt{\eta_A}\\ 0 & 0\end{bmatrix} \tag{14}$$

where $\eta_A\ (0\le\eta_A\le1)$ describes the probability of error due to Amplitude-damping noisy environment when a travel qubit pass through it. $\eta_A$ is also referred to as decoherence rate. Similarly, phase-damping noise model is characterised by the following Kraus operators

$$E_0^P=\sqrt{1-\eta_P}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \tag{15}$$

$$E_1^P=\sqrt{\eta_P}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix};E_2^P=\sqrt{\eta_P}\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix} \tag{16}$$

where $\eta_P$ $(0 \le \eta_P \le 1)$ is the decoherence rate for the phase-damping noise. The simulated results for fidelity versus $\eta$ under amplitude-damping and phase-damping noise are shown in Figs. 4 and 5, respectively. These figures show that high values of fidelity describes less effect of noise at different values of $\eta$. The Bell pair used in BBM protocol is $\left|\phi^-\right\rangle = \frac{(|01\rangle - |10\rangle)}{\sqrt{2}}$, whereas basis used in B92 protocol are $|0\rangle$ and $|+\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$. In the following simulated results, the Blue and Red lines correspond to B92 and BBM protocols, respectively.

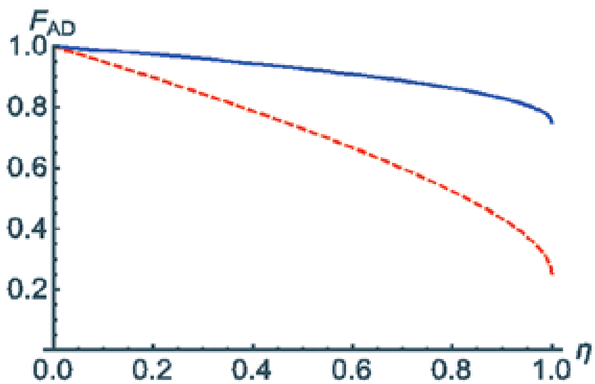


**Figure 4. Effect of amplitude damping noise on the QKD protocol.**

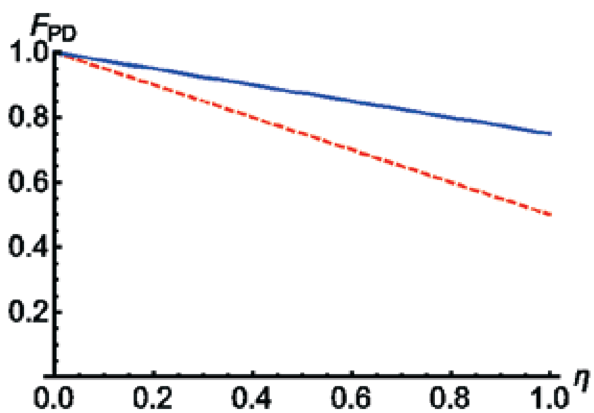


**Figure 5. Effect of phase damping noise on the QKD protocol.**

### 4.2 Effect of the Collective Noise on the QKD Protocol

For the practical implementation, it is necessary to consider the channel noise that is generated due to the interaction of photons with the environment. This process is known as collective noise [17,18], with the assumption that the time variations of the noise is greater than the photons travelling time within a particular time window. Collective noise model is described by the following two types of noises[19], $U_{dp}$ is known as the unitary operator for collective-dephasing and $U_r$ is the unitary perator for collective-rotation noise. Each of these noises can be explained by the following unitary operations. The unitary operations for collective-dephasing noise is as follows[20]

$$U_{dp}|0\rangle = |0\rangle; U_{dp}|1\rangle = e^{i\varphi}|1\rangle \qquad (17)$$

where $|0\rangle$ and $|1\rangle$ are the horizontal and vertical polarizations of photons respectively and $\varphi$ is the noise parameter varying with respect to time. Similarly, the unitary operations for collective-rotation noise are as follows[19]

$$U_r|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle; U_r|1\rangle = -\sin\theta|0\rangle + \cos \qquad (18)$$

here $\theta$ is also the noise parameter varying with respect to time[19]. These noises are characterised by the following Kraus operators

$$U_{dp} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}; U_r = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \qquad (19)$$

The fidelity-$\eta$ plots for collective noise is shown in Figs. 6 and 7. Higher values of fidelity indicates less effect of noise at particular values of $\theta$ and $\phi$ for collective rotation and collective dephasing noise respectively.

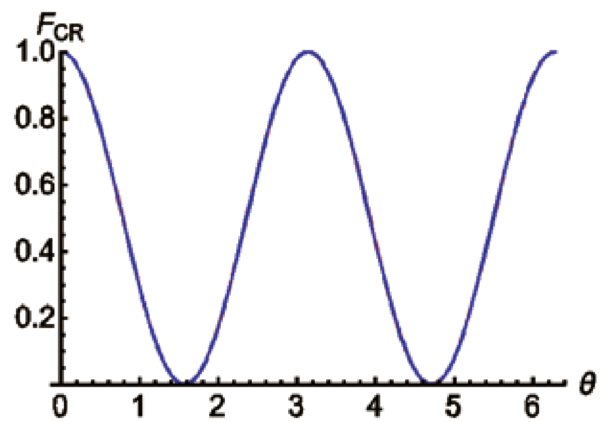


**Figure 6. Effect of the collective rotation noise (In CR noise both have same fidelity) on QKD protocol.**

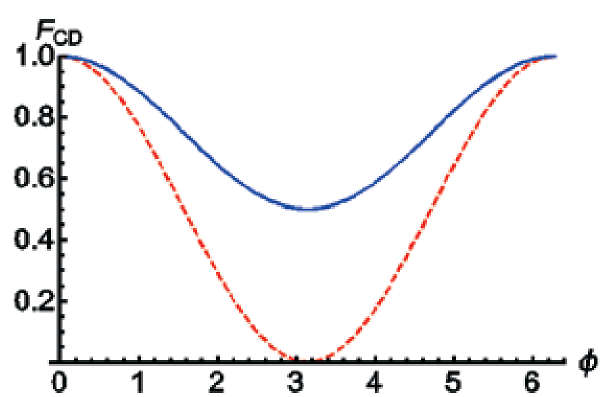


**Figure 7. Effect of the collective dephasing noise on the QKD Protocol.**

### 4.3 Effect of the Pauli Noise on the QKD Protocol

Pauli noise model is characterised by the following Kraus operators

$$W_{01} = \sqrt{P1}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; W_{11} = \sqrt{P2}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{20}$$

$$W_{10} = \sqrt{P3}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; W_{00} = \sqrt{P4}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{21}$$

where $P1 + P2 + P3 + P4 = 1$, that is sum of probabilities is equal to unity. The fidelity expressions for the BBM protocol under various types of noises are as follows

$$F_{AD} = \frac{1}{4}(2 + 2\sqrt{1-\eta} - \eta) \tag{22}$$

$$F_{PD} = \left(1 - \frac{\eta}{2}\right) \tag{23}$$

$$F_{CD} = \cos\left(\frac{\phi}{2}\right)^2 \tag{24}$$

$$F_{CR} = \cos\left(\theta\right)^2 \tag{25}$$

$$F_{PN} = P_4 \tag{26}$$

On the other hand, the B92 protocol has the following fidelity expressions under noisy environment

$$F_{AD} = \frac{1}{4}\left(3 + \sqrt{(1-\eta)}\right) \tag{27}$$

$$F_{PD} = \frac{1}{2}\left(2 - \frac{\eta}{2}\right) \tag{28}$$

$$F_{CD} = \frac{3}{4} + \cos\left(\frac{\phi}{4}\right) \tag{29}$$

$$F_{CR} = \cos\left(\theta\right)^2 \tag{30}$$

$$F_{PN} = \frac{P_1 + P_3 + 2P_4}{2} \tag{31}$$

here $F_{AD}$, $F_{PD}$, $F_{CD}$, $F_{CR}$ and $F_{PN}$ are the fidelities corresponds to the amplitude-damping, phase-damping, collective dephasing, collective-rotation and Pauli noise, respectively. $\eta$, $\theta$ and $\phi$ are the noise parameters mentioned in Kraus operator equations. $P_1, P_2, P_3$ and $P_4$ are the associated probabilities with Pauli noise model with the condition that

$P1 + P2 + P3 + P4 = 1$

### 4.4 QKD Protocol under Squeezed Generalized Amplitude Damping Channel

The squeezed generalised amplitude damping (SGAD) channel is derived by the master Eqn. (10). This follows the concept of completely positive map given in Eqn. (3). For more information about the effects of squeezing and corresponding Kraus operators[16].

## 5. CONCLUSIONS

Authors observed that different types of noises in the master equation form are responsible for varying nature of different quantum states under quantum communication between Alice and Bob. The simulated fidelity graph results show that, the fidelity values vary with the above mentioned noise parameters under particular type of noise. The various types of noises mentioned in quantum algorithms[25,26] are of different kind compared with the noises mentioned here. Entanglement purification[23] and quantum error correction[24] are the effective methods by which errors generated from decoherence can be corrected. The following observations are made from the above results

(i) The Bell-state of the form $\left|\phi^-\right\rangle = \frac{\left(|01\rangle - |10\rangle\right)}{\sqrt{2}}$ used in BBM protocol is highly corrupted under Amplitude-damping noise, so it is not practically reliable under AD noise as shown in Fig. 4.

(ii) From Fig. 5 it is clear that under PD noise, single qubit based B92 protocol provides high value of fidelity compared to entangled state based BBM protocol, hence while transmission under PD noise, B92 is less affected by this kind of noise compared to BBM protocol.

(iii) From Figs. 4 to 7, it can be concluded that single qubit based B92 protocol(with $|0\rangle$ and $|+\rangle$ basis) is immune to all type of noises compared to the BBM protocol.

(iv) In BBM protocol $\left|\phi^-\right\rangle = \frac{\left(|01\rangle - |10\rangle\right)}{\sqrt{2}}$ is used for quantum communication hence, any disturbance in sent sequence of $\left|\phi^-\right\rangle$ is detected as Eavesdropping.

(v) Under CR noise, the fidelity graph of the B92 protocol shows variations with $\theta$ which is not considered as an efficent approach for practical point of view, because this degrades the originality of the information being sent at long distances, hence in practical implementation the information will further decay due to device imperfections and losses in optical fibers used as a medium for data transmission, so noise consideration with the fidelity is an important point of research to be considered to avoid the loss of originality of the information sent from Alice to Bob.

Differential phase shift (DPS) QKD protocol is capable of communicating the quantum information for long distance using optical fiber as a quantum channel which is practically important between the quantum repeater nodes because of its high key rates and ease of practical implementation. But, the various attacks must be considered for DPS QKD protocol for security issues. Similar to B92 protocol, in DPS QKD protocol also Alice randomly prepares the quantum states and sends two non-orthogonal states to Bob, but opposite to B92 protocol, in DPS QKD protocol no need of a bright reference pulse but requires a weak coherent pulse (WCP) with less than 1 amount of average photon number, hence practically easy and simple to perform compared to that of B92 protocol.

The quantum noise generated due to the fiber imperfections could provide large amount of noise, so it is the main concern to deal with such noise while considering optical fibers for transmission of quantum information. Proper care should be taken when modulation speed of 40 Gb/s and above because it may severely degrades the quantum signal strength. Hence, We need a practical quantum communication system which is flexible, easily implementable and efficient with low communication complexity.

## REFERENCES


1. Nielsen, M.A. &Chuang, I.L. Quantum computation and quantum information. Cambridge University Press, 2000, pp. 1-710.
2. Bennet, C.H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *In* Proceedings of IEEE International Conference on Computers, Systems and Single Proceeding, 1984, pp. 175-179.
3. Bennett, Charles H.; Fuchs, Christopher A. & Smolin, John A. Entanglement-enhanced classical communication over a noisy classical channel. Springer Book, 1997, pp. 79-88.
doi:10.1007/978-1-4615-5923-8_9.
4. Deutsch, D. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. Res. Soc. Lond.* A 400, 1985, 97-117.
5. Leung, Debbie; Mancinska, Laura; Matthews, William; Ozols, Maris & Roy, Aidan. Entanglement can increase asymptotic rates of zero-error classical communicationover classical channels. *Commun. Math. Phys.,* 2012, **311**, 97-111.
doi: 10.1007/s00220-012-1451-x
6. Bennet, C.H.; Brassard, G.; Crépeau, C. Jozsa, R.; Peres, A. & Wootters, W.K. Teleporting an unkonuwn quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett*., 1993, **70,** 1895-1899.
doi:10.1103/PhysRevLett.70.1895
7. Mintert, F.; Carvalho, A.R.R.; Kus, M. & Buchleitner, A. Measures and dynamics of entangled states. *Physics Reports*, 2005, **415(4)**, 207-260.
doi: 10.1016/j.physrep.2005.04.006
8. Bennett, C.H.; Fuchs, C.A. & Smolin, J.A. Entanglement-enhanced classical communication on a noisy quantum channel. 1996. http://arxiv.org/abs/quant-ph/9611006.
9. Horodecki, R.; Horodecki, P.; Horodecki, M. & Horodeck-I, K. Quantum entanglement. *Rev. Modern Phys.*, 2009, **81**, 865-942.
doi:10.1103/RevModPhys.81.865
10. Kraus, K. States, effects, and operations: Fundamental notions of quantum theroy. Springer-Verlag Berlin Heidelberg, 1983.
doi: 10.1007/3-540-12732-1
11. Bostroem, K. & Felbinger, T. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.*, 2002, **89**, 187902-1 – 187902-8.
doi:10.1103/PhysRevLett.89.187902.
12. Wootters, W.K. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett*., 1998, **80**(10), 2245 - 2248.
doi: 10.1103/PhysRevLett.80.2245.
13. Sharma, V.; Shukla, C.; Banerjee, S. & Pathak, A. Controlled bidirectional remote state preparation in noisy environment: A generalized view. *Quantum Info. Process.* 2015, **14**, 3441–3464.
doi: 10.1007/s11128-015-1038-5
14. Sharma, V. & Sharma, R. Analysis of spread spectrum in MATLAB. *Int. J. Sci. Eng. Res.*, 2014, **5**(1), 1899-1902.
15. Chen, A.X.; Li, J.H. & Jin, L.X. Trace distance of remote state preparation through noisy channels. *Commun. Theor. Phys.*, 2005, **43**(4), 631-636.
doi: 10.1088/0253-6102/43/4/014
16. Srikanth, R. & Banerjee, S. The squeezed generalized amplitude damping channel. *Am. Phy. Society Phys. Rev***.** A, 2008, **77,** 1-10.
doi: 10.1103/PhysRevA.77.012318.
17. Chen, Xiuliang; Zhou, Chunyuan; Wu, Guang; Zeng, Heping. Efficient quantum key distribution with stable and expansible differential phase shift schemes. *Appl. Phy. Lett.,* 2004, **85**(9), 1648-1650.
doi: 10.1063/1.1786658
18. Tseng, Hsin-Yi; Lin, Jason & Hwang, Tzonelih New quantum private comparison protocol using EPR pairs. *Quant. Inf. Proc*., 2012, **11**(2), 373 – 384.
doi: 10.1007/s11128-011-0251-0.
19. Tian-Yu Ye: Fault-Tolerant authenticated quantum dialogue using logical Bell states. *Quant. Inf. Proc*., 2015, **14**(9), 3499-3514. doi: 10.1007/s11128-015-1040-y.
20. Walton, Z.D.; Abouraddy, A.F. & Sergienko, A.V. Decoherence-free subspaces in quantum key distribution. *Phys. Rev. Lett.,*2003, **91**(8), 1-4.
doi:10.1103/PhysRevLett.91.087901
21. Guan, X.-W.; Chen, X.-B.; Wang, L.-C.& Yang, Y.-X. Joint remote preparation of an arbitrary two-qubit state in noisy environments. *Int. J. Theor. Phys.*, 2014, **53**, 2236-2245.
doi 10.1007/s10773-014-2024-x.
22. Song, Hong-Ting & Xi, Zai-Rong. More entanglement, less reliability. *In* Proceedings of the 30th Chinese Control Conference, 2011, pp. 5328-5331, Yantai, China.
23. Horodecki, Pawal. On entanglement distillation and quantum error correction for unknown states and channels. *Open Phy.*, 2003, 1(4), 695–707.
doi: 10.2478/BF02475911.
24. Preskill, J. Reliable quantum computers. *Proc. R. Soc. London, A*, 1998, **454**, 385-410.
doi: 10.1098/rspa.1998.0167
25. Zhang, Yu-Chao; Bao, Wan-Su; Wang, Xiang; Fu, Xiang-Qun. Effects of systematic phase errors on optimized quantum random-walk search algorithm. *Chin. Phys. B,* 2015, **24**(6), 1-9.
doi:10.1088/1674-1056/24/6/060304.
26. Guo, H.; Long, G.L. & Sun, Y. Effects of imperfect gate operations in shor's prime factorization algorithm. *J. Chin. Chem. Soc*., 2001, **48**, 449 - 454.
27. Scheiner, B. Applied cryptgraphy. Edn. 2nd. John Wiley and Sons, 2000, pp.1-1027.
28. Diffie,W. & Hellmann, M.E. New directions in cryptography. *IEEE Trans. Info. Theory*, 1976, **22**, 644-654.
29. Wootters, W. & Zurek, W. A single quantum cannot be cloned. *Nature,* 1982, **299**, 802-803.
doi: 10.1038/299802a0.

30. Dieks, D. Communication by EPR devices. *Phys. Lett. A*, 1982, **92**(6), 271-272. doi: 10.1016/0375-9601(82)90084-6.
31. Peres, A. Quantum theory: Concepts and methods. Kluwer Academic Publishers, Springer, 1995, pp. 1-464.
32. Cui, Ke; Wang, Jian; Zhang, Hong-Fei; Luo, Chun-Li; Jin, Ge & Chen, Teng-Yun. A real-time design based on FPGA for expeditious error reconciliation in QKD system. *IEEE Trans. Info. Forensics Sec.*, 2013, **8**(1), 184-190. doi:10.1109/tifs.2012.222885
33. Kumar P. & Prabhakar, A. Designing practical quantum communication systems. *In* the National Conferences on Communication, IIT-Bombay, 2008, pp. 1-5.
34. Gyongyosi, Laszlo & Imre, Sandor. Secure long-distance quantum communication over optical fiber quantum channels.optical fiber communications and devices. Tech Book, 2012, pp. 163-202. doi: 10.5772/26976.
35. Sharma, V. Feasibility of temperature sensors in railway coaches. *Int. J. Sci. Eng. Res.*, 2014, **5**(2), 881-884.
36. Sharma, V. Experimental use of electronic nose for odour detection. *Int. J. Eng. Sys.Model. Simulation*, 2015, **7**(2), 238-243. doi: 10.1504/IJESMS.2015.072509
37. Sharma, V.; Thapliyal, K.; Pathak, A. & Banerjee, S. A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. 2016. http://arxiv.org/abs/1603.00178 (Accessed on 1 March 2016).

## ACKNOWLEDGEMENTS

I would like to thank the Ministry of Human Resource Development, Govt. of India, for offering a doctoral fellowship as a PhD research scholar at Indian Institute of Technology Jodhpur, Rajasthan, India. Author also thanked Dr Subhashish Banerjee and Dr Anil Prabhakar for there valuable discussions.

## CONTRIBUTORS

**Mr Vishal Sharma** received his BE (ECE) from University of Rajasthan, in 2006 and ME (Embedded Systems) from BITS, Pilani, Rajasthan, in 2010. Currently pursuing his PhD at Indian Institute of Technology, Jodhpur, Rajasthan. He served as a Senior Project Fellow for Electronic Nose project in CEERI, Pilani and also worked as a Project Engineer in Robotics lab at IIT, Jodhpur. His research interest includes: Quantum computation and quantum information, electronics and communication, image and signal processing, sensors, embedded systems, robotics and computer vision, machine learning and pattern recognition.

In the current study, he studied the effect of noise in quantum communication both theoretically and practically and implemented some of the part on FPGA