1
Introduction

In a broad sense, quantum information processing is based on the principals of quantum mechanics and information theory which manipulates the data, stores the outcomes and takes necessary action based on the outcomes and finally shows the capabilities and interconnects the various quantum systems. The field is multidisciplinary including ideas of cryptography, quantum mechanics, computer science and engineering, quantum optics, electrical engineering, information theory and atomic physics both theoretically and experimentally.

Theory of quantum computing has many unique and additional computing features such as quantum parallelism, quantum superposition, no cloning principle, entanglement, Heisenberg Uncertainty Principle, scalable quantum computing (exponential speed up based on quantum algorithms [Gruska et al., 2002]). All these properties provide unconditional security and enhance the computational power of quantum systems, which is absent in its classical counterpart. All these features allow quantum computing to accomplish various operations impossible classically, for example superdense coding [Bennett and Wiesner, 1992; Mattle et al., 1996], quantum teleportation [Bouwmeester et al., 1997; Boschi et al., 1998], quantum logic gates [O'Brien et al., 2003], remote state preparation [Bennett et al., 2001a; Ye et al., 2004a] and quantum key distribution [Jennewein et al., 2000], factoring large and unstructured data [Ekert and Jozsa, 1996; Shor, 1999; Grover, 1997], quantum cryptography [Jennewein et al., 2000; Naik et al., 2000; Tittel et al., 2000], entanglement distillation [Bennett et al., 1996; Pan et al., 2003], and decoherence-free subspaces [Kwiat et al., 2000; Lidar et al., 1998]. In real field applications, quantum systems interact with an external environment and result in decoherence due to noise.

Classical cryptography provides one-time-pad secret key, also known as Vernam cipher [Vernam, 1926]. This one-time pad is used only once, random and equal in length to that of message key [Shannon, 1949]. The main problem with the one-time -pad is that key length grows with the message length. At this point, quantum mechanics can solve this key distribution problem and is known as quantum key distribution (QKD) [Townsend et al., 1993; Bennett et al., 1992; Gisin et al., 2002]. QKD is the only solution which provides unconditional security and based on the laws of quantum mechanics [Wootters and Zurek, 1982]. If eavesdroppers try to steal information it leads to errors. QKD imposes a limit on the stolen information, which if it exceeds a secure threshold, the legitimate users halt the communication. Otherwise, they perform classical privacy amplification schemes to diminish the effect of eavesdropping.

Optical fibers are the first mature technology used for experimental realization of QKD [Stucki et al., 2002; Poppe et al., 2004; Yuan and Shields, 2005; Zhao et al., 2006; Yuan

et al., 2007]. However, they are limited by decoherence effects and losses present in the fibers and noise present in the single photon detectors. This limits the communication distance to the order of 100-200 km [Gobby et al., 2004; Hiskett et al., 2006; Peng et al., 2007; Rosenberg et al., 2007; Takesue et al., 2007].

There are numerous methods to overcome the problems associated with optical fibers. One such method is to divide a large distance into segments of intermediate nodes. In this approach, secret keys are first shared between the adjacent nodes and further by performing bitwise XOR- operation, a final new secret key is established between the initial and final node. For this scheme to be implemented successfully, we need trustworthy nodes and number of such nodes increases with increasing the communication distance. These nodes can be minimized by replacing classical repeater stations by quantum repeaters to avoid the conversion into classical information [Briegel et al., 1998; Duan et al., 2001]. In this process, the transfer of quantum states takes place by quantum teleportation technique and other techniques such as entanglement swapping and entanglement purification. But all these approaches face difficulties when applied to global communication.

Quantum-based satellite communication was proposed for establishing a global key exchange scenario so that the distance limitations can be overcome [Buttler et al., 1998, 2000; Nordholt et al., 2002; Rarity et al., 2002; Aspelmeyer et al., 2003]. In this process, an optical free-space link is established between a ground station and a satellite placed at earth orbit. The moving satellite exchanges separate keys with the different ground stations placed at earth, hence a single satellite link covers a large area of the earth. Opposite to optical fiber-based quantum communication, only a single trusted satellite is enough, while creating a secure key between ground station A to ground station B. Here trusted satellite store the secret key from ground station A, until it reaches to ground station B. The advantage of this scheme is that it reduces the number of trusted nodes. It was shown that there is no need for trusted satellite if entangled based quantum cryptography schemes are used in quantum-based communication [Poppe et al., 2004; Ekert, 1991; Bennett, 1992; Ekert et al., 1992; Brendel et al., 1999; Waks et al., 2002b; Weihs et al.; Naik et al., 2000; Ribordy et al., 2000; Tittel et al., 2000; Peng et al., 2005]. For its successful implementation, both the ground stations must be in the satellite reach simultaneously; also the location of the ground stations and the choice of earth orbit gives different results in terms of required links and duration to establish the communication.

In quantum-based satellite communication, most of the communication happens in empty space where photons propagate with negligible attenuation and challenges occur in the space where high attenuation comes into picture under the effect of earth's atmosphere. On the other side, low absorption occurs in the wavelength range 600-850 nm and single photon detectors are available, particularly for this range. In this spectral range, quantum states are encoded in polarization degree of freedom without any birefringence.

The quantum-based satellite communication with single photon [Beveratos et al., 2002; Waks et al., 2002a; Alléaume et al., 2004] or entangled photons [Peng et al., 2005; Resch et al., 2005; Marcikic et al., 2006] are difficult to realize specially for spaceborne transmitter module. This is because of the specific and complex requirements associated with these modules such as power and mass. Also, these photon sources need delicate and complex setup. The photon-number-splitting (PNS) attack is the main challenge for the transmitter which generates attenuated laser pulses [Dušek et al., 1999; Brassard et al., 2000; Lütkenhaus, 2000]. The eavesdroppers steal the information by taking one or more photons from a multiphoton source; hence, it is essential to highly attenuate such sources

equal to the link efficiency.

The presence of eavesdroppers can be detected by replacing fixed average photon number by decoy states. These decoy states are of different intensity values which are generated at the transmitter end. The eavesdropping in form of PNS attack can be detected at receiver side by comparing the receiver's detection probability of each pulse [Hwang, 2003; Wang, 2005; Lo et al., 2005b]. This is the main advantage of using decoy state which makes communication systems more secure for large distances and allows the use of attenuated pulses in a secure manner with improved efficiency near about to those of single-photon QKD. The feasibility of experimental approach of decoy states have been proposed in optical fiber communication [Zhao et al., 2006; Yuan et al., 2007; Peng et al., 2007; Rosenberg et al., 2007] and also in free space communication [Schmitt-Manderbach et al., 2007].

Overview

In this thesis, we use photons for encryption and decryption of quantum bits. Here we give a short description about the organization of the thesis. In chapter 2 we describe the fundamentals of quantum information processing and quantum cryptography that is used in quantum communication. Some specific attacks like photon-number-splitting attack and intercept-resend attack are described on the quantum channel in the quantum key distribution cryptography protocols. These specific attacks deploy attenuated laser pulses which results in high channel attenuation and losses. The chapter concludes with the brief description of QKD (quantum key distribution) in the quantum-based satellite communication. Chapter 3 takes up the problem of remote state state preparation under noisy environment both for probabilistic and deterministic approach under the control of a third party, Charlie. Fidelity expressions under various noisy models such as amplitude damping (AD), phase damping (PD), collective noise and squeezed generalized amplitude damping (SGAD) are computed. This chapter concludes with the comparison of classical information needed for the particular method used and their applications and experimental realizations. Chapter 4 makes a comparative study of various QKD (Quantum key distribution), QSDC (Quantum secure direct communication), DSQC (Deterministic secure quantum communication), QDC (Quantum direct communication) and QD (Quantum dialogue) protocols under the noisy models described in chapter 3. The chapter concludes with a comparison of the performance of single qubit and entangled based protocols under the said noisy models. In chapter 5, the effect of decoherence in quantum cryptographic security under some specific noisy models for the Ping-Pong QKD protocol is studied. The channel attenuation is a serious problem in quantum based satellite communication which further degrades the performance of the quantum communication system, as described in chapter 6. It is shown that performance can be improved by using decoy states. The SARG04 protocols, with decoy states, are seen to outperform the BB84 protocol for quantum-based satellite communication. Further, various turbulence effects are analyzed both for uplink and downlink scenarios keeping in mind the eavesdropping attacks and channel attenuation in system performance. Finally, conclusions are made in chapter 7.