Article
Chinese Science Bulletin
Quantum Information
March 2011 Vol.56 No.7: 618–625
doi: 10.1007/s11434-010-4336-4

An error-free protocol for quantum entanglement distribution in long-distance quantum communication

SALEMIAN Shamsolah* & MOHAMMADNEJAD Shahram

Nanoptronics Research Center, Department of Electronics and Electrical Engineering, Iran University of Science and Technology, Tehran 1684613114, Iran

Received July 19, 2010; accepted September 2, 2010

Quantum entanglement distribution is an essential part of quantum communication and computation protocols. Here, linear optic elements are employed for the distribution of quantum entanglement over a long distance. Polarization beam splitters and wave plates are used to realize an error-free protocol for broadcasting quantum entanglement in optical quantum communication. This protocol can determine the maximum distance of quantum communication without decoherence. Error detection and error correction are performed in the proposed scheme. In other words, if there is a bit flip along the quantum channel, the end stations (Alice and Bob) can detect this state change and obtain the correct state (entangled photon) at another port. Existing general error detection protocols are based on the quantum controlled-NOT (CNOT) or similar quantum logic operations, which are very difficult to implement experimentally. Here we present a feasible scheme for the implementation of entanglement distribution based on a linear optics element that does not need a quantum CNOT gate.

quantum entanglement, quantum communication, quantum error detection, decoherence, error correction

Citation: Salemian S, Mohammadnejad S. An error-free protocol for quantum entanglement distribution in long-distance quantum communication. Chinese Sci Bull, 2011, 56: 618–625, doi: 10.1007/s11434-010-4336-4

Quantum information and communication has the potential to revolutionize many areas of science and technology. It employs fundamentally new modes of computation and communication because it is based on the physical laws of quantum mechanics instead of classical physics. The goal of quantum computing is to develop a general-purpose quantum processor including error correction, as a model system to demonstrate quantum algorithms and various quantum computing architectures, and with emphasis on potential scalability. In quantum communication, the short-term goal is to develop quantum cryptography towards establishing the technology and commercial products. A scientific goal is to demonstrate long-distance quantum communication both in an optical fiber and in free space. On a time scale of 5–10 years, goals are to gain several orders of magnitude on the secret bit rate and to demonstrate quantum repeaters. The latter will require the implementation of error correction, entanglement purification, quantum interfaces and quantum memories.

Quantum key distribution (QKD) is an important branch of quantum information and communication. The aim of QKD is transmission of confidential information between parties by sharing a secret key. The standard QKD protocol (BB84) was proposed by Bennett and Brassard in 1984 [1]. Since then, many theoretical QKD schemes have been proposed [1–18]. The QKD protocols have been exhibited over limited distances, both in optical fibers and in free space. Because of some limitations, it has not yet been used for universal practical applications. The progress in QKD has been strongly influenced by the need to overcome a variety of practical challenges. Wang et al. [19] used an inspection and power insertion (IPI) technique to prolong the distance in QKD. The IPI is a general technique for extending the transmission distance. Its performance depends entirely on

*Corresponding author (email: salemian@iust.ac.ir)

the security of the intermediate stations. The IPI is a useful choice to extend the distance in quantum communication protocols based on non-entangled sources. Early QKD systems used a single photon as an information carrier. However, it is difficult to prepare reliable single-photon sources and high efficiency photon detectors at present. In contrast, QKD based on a continuous variable (CVQKD) eliminates the requirement for single-photon technology [20].

Beside QKD, another protocol—so-called quantum secure direct communication (QSDC)—has been proposed [13,21]. QDSC communicates important messages directly without first establishing a random key to encrypt them. By considering a lossy quantum channel, Deng et al. [22] introduced a QSDC scheme with Einstein-Podolsky-Rosen (EPR) pairs. They explained that it is provably secure and has a high capacity. It is possible to increase the source capacity of QSDC using super-dense coding [23].

Two QDSC protocols over the collective amplitude damping channel [24] and collective-noise channel [25] were proposed. These two protocols have disadvantages in implementation. To encode the noiseless states and secret information, both Alice and Bob need to perform complex encoding operations, which will increase the difficulty of implementation.

Quantum networking using the Internet and commercial fiber is an important challenge in the globalization of quantum communication [26]. Elliott [27] showed how QKD techniques can be employed within realistic, highly secure communications systems, using the Internet architecture. In May 2009, the first hierarchical metropolitan quantum cryptography network was realized with seven nodes on inner-city commercial telecom fibers [28].

Quantum entanglement is an important concept in quantum physics and is the basis of most quantum communication and computation protocols [29–39]. Each of these protocols allows efficient communication and computation beyond the capabilities of classical communication, which makes it attractive as a new emerging quantum information technology. This might result in the construction of a worldwide quantum communication network, and the distribution of quantum entanglement on a global scale is a central task of this network. Until now, only the photon has been a suitable system for long-distance quantum communication. Other systems such as atoms or ions have been studied, but their applicability for quantum communication schemes is not feasible in the near future. Therefore, photons are the only choice for long-distance quantum communication. One of the problems in photon-based schemes is the loss of photons in the quantum channel. This limits the maximum distance of single photon transmission to about 100 km in present silica fibers [40,41]. The most important challenge in quantum communication is quantum decoherence. The polarization states of photons are used as quantum states. However, the polarization state of photons is changed and destroyed by environmental effects such as thermal fluctuation, vibration, and the imperfection of the fiber. These environmental effects are considered as noise in the quantum channel. The decoherence phenomenon limits the application of quantum computation and communication in practice. Therefore, several methods have been developed to protect quantum computations from decoherence. Various error correction and error rejection methods have been proposed to overcome quantum channel noise [42,43]. There are several degrees of freedom for photons, which can be used in quantum communication protocols, such as the polarization degree of freedom, the spatial degree of freedom and the frequency degree of freedom of photons. Li et al. [44] proposed a single-photon error rejection scheme to handle collective noise with linear optics. In this scheme, additional qubits and fast polarization modulators are not required, qubits are encoded in time bins and the uncorrupted state arrives in definite time slots. Later, an efficient quantum entanglement distribution over an arbitrary collective-noise channel was presented by Sheng et al. in 2010 [45]. Their protocol was based on the frequency degree of freedom of photons and it used frequency entanglement. In this paper, we present a different scheme for the distribution of entangled states based on the polarization degree of freedom, which is a vital ingredient in the realization of long-distance quantum communication in the future.

Quantum repeaters have been proposed to extend the distance between Alice and Bob in quantum communication. Quantum repeaters are needed to achieve long-distance quantum communication. This is possible by subdividing the larger distance into smaller segments over which entanglement can be teleported. Quantum repeaters perform two tasks: quantum entanglement purification and swapping. Entanglement purification is employed to improve the entanglement of the quantum systems and then achieve the goal of quantum communication with maximally entangled states. The original quantum entanglement purification was proposed by Bennett et al. in 1996 [46]. They used controlled-NOT gates in their protocol. At present, there is no implementation of CNOT gates that can realistically be used for purification in the context of long-distance quantum communication. An entanglement purification protocol with linear optical elements such as polarizing beam splitters and quarter wave plates was proposed by Pan in 2001 [47]. This protocol required a single entangled photon pair generated by an ideal source. The currently available source of entangled photons is not an ideal entangled source. Sheng et al. [48,49] proposed new protocols that required neither CNOT gates based on linear optical elements nor sophisticated single-photon detectors, which makes their use more convenient in practical applications. Eventually, entanglement swapping [50] was used for the transporting of entanglement over long distances.

In this paper, an error-free protocol is proposed to extend the bridgeable distance of single photons and subsequently reduce the number of quantum repeaters in the quantum

communication network. Error detection and correction are performed in the proposed scheme. If there are qubit changes ($|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$) along the quantum channel, the state evolution can be detected by Alice and Bob and corrected states are obtained at another port. Here the linear polarization states of photons, $|H\rangle$ for 'horizontal' and $|V\rangle$ for 'vertical', serve as the physical representation of logical bit values, with $|H\rangle \equiv |0\rangle$ and $|V\rangle \equiv |1\rangle$.

1 Error model for quantum Information

Understanding the nature of errors is the first step in protecting information against errors. In the error models for classical communication and computation, errors may not influence bits independently, and so the error models have to consider any correlation between errors of different bits. The same is true for errors of quantum bits, but we must consider that the quantum alteration is a continuous process as opposed to the classical discrete case; the encoding operation cannot make multiple copies of arbitrary quantum states, and the corruption of an encoded quantum state cannot be detected through the complete measurement of all the qubits.

A qubit contains errors when its alteration differs from the desired one. This difference can be due to the inexact control of the qubits or interaction of the qubits with the environment. A 'quantum channel' is a formal description of how qubits in a given setting are affected by their environment. The general change of a qubit in the state $|0\rangle$ interacting with an environment in the state $|E\rangle$ yields a superposition state of the form

$$|0\rangle|E\rangle \to \beta_1|0\rangle|E_1\rangle + \beta_2|1\rangle|E_2\rangle. \quad (1)$$

That is, with amplitude β_1, the qubit remains in the basis state $|0\rangle$ and the environment evolves to some state $|E_1\rangle$. With amplitude β_2, the qubit evolves to the basis state $|1\rangle$ and the environment evolves to some state $|E_2\rangle$. Similarly, when the qubit is initially in state $|1\rangle$ with the environment in state $|E\rangle$, we have

$$|1\rangle|E\rangle \to \beta_3|1\rangle|E_3\rangle + \beta_4|0\rangle|E_4\rangle. \quad (2)$$

More generally, when a qubit in a general pure state interacts with the environment in state $|E\rangle$, we have

$$\begin{aligned}(\alpha_0|0\rangle + \alpha_1|1\rangle)|E\rangle \to{}& \alpha_0\beta_1|0\rangle|E_1\rangle + \alpha_0\beta_2|1\rangle|E_2\rangle \\ &+ \alpha_1\beta_3|1\rangle|E_3\rangle + \alpha_1\beta_4|0\rangle|E_4\rangle. \end{aligned} \quad (3)$$

We can rewrite the state after the interaction as

$$\begin{aligned}&\alpha_0\beta_1|0\rangle|E_1\rangle + \alpha_0\beta_2|1\rangle|E_2\rangle + \alpha_1\beta_3|1\rangle|E_3\rangle + \alpha_1\beta_4|0\rangle|E_4\rangle \\ &= \frac{1}{2}(\alpha_0|0\rangle + \alpha_1|1\rangle)(\beta_1|E_1\rangle + \beta_3|E_3\rangle) \\ &\quad + \frac{1}{2}(\alpha_0|0\rangle - \alpha_1|1\rangle)(\beta_1|E_1\rangle - \beta_3|E_3\rangle) \\ &\quad + \frac{1}{2}(\alpha_0|1\rangle + \alpha_1|0\rangle)(\beta_2|E_2\rangle + \beta_4|E_4\rangle) \\ &\quad + \frac{1}{2}(\alpha_0|1\rangle - \alpha_1|0\rangle)(\beta_2|E_2\rangle - \beta_4|E_4\rangle). \end{aligned} \quad (4)$$

Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. We then have

$$\begin{aligned}|\psi\rangle|E\rangle \to{}& \frac{1}{2}|\psi\rangle(\beta_1|E_1\rangle + \beta_3|E_3\rangle) \\ &+ \frac{1}{2}(Z|\psi\rangle)(\beta_1|E_1\rangle - \beta_3|E_3\rangle) \\ &+ \frac{1}{2}(X|\psi\rangle)(\beta_2|E_2\rangle + \beta_4|E_4\rangle) \\ &+ \frac{1}{2}(XZ|\psi\rangle)(\beta_2|E_2\rangle - \beta_4|E_4\rangle). \end{aligned} \quad (5)$$

This represents the most general evolution that can happen for a single qubit, whether or not it interacts with the environment.

The interesting point is that a generic continuous evolution has been rewritten in terms of a finite number of discrete transformations; with various amplitudes the state is either unaffected or undergoes a phase flip *Z*, a bit flip *X* or a combination of both, *XZ*. This is possible because these operators form a basis for the linear operators in the Hilbert space of a single qubit.

Specific errors can be described as special cases of the right side of eq. (5). For example, suppose we know that the error is a 'bit flip', which has the effect of the NOT gate *X* with some amplitude and leaves the qubit unaffected (applies the identity) with possibly some other amplitude. This would correspond to states of the environment such that $\beta_1|E_1\rangle = \beta_3|E_3\rangle$ and $\beta_2|E_2\rangle = \beta_4|E_4\rangle$. Eq. (5) for the general evolution thus simplifies to

$$|\psi\rangle|E\rangle \to \beta_1|\psi\rangle|E_1\rangle + X\beta_2|\psi\rangle|E_2\rangle. \quad (6)$$

Single-qubit errors result from an uncontrolled situation leading to an inexact rotation of the qubit about the *x*-axis of the Bloch sphere; $\beta_1|E_1\rangle = c\beta_2|E_2\rangle$ for some constant *c*. Thus, the environment state factors out from the qubit state. The operator $c\beta_2 I + \beta_2 X$ is unitary. In other words,

$$|\psi\rangle|E\rangle \to ((c\beta_2 I + X\beta_2)|\psi\rangle) \otimes |E_2\rangle. \quad (7)$$

Therefore, the error is termed coherent and will be incoherent if the environment state does not factor out. When $\beta_1|E_1\rangle$ is orthogonal to $\beta_2|E_2\rangle$, in the quantum bit-flip error model,

the operator X (bit flip) is applied with probability $|\beta_2|^2 = p$ and remains unaffected with probability $|\beta_1|^2 = 1-p$. The generic evolution of this latter case is non-unitary.

The case of the generic evolution of a qubit can be generalized to the situation of a larger quantum system (e.g. a register of qubits in a quantum computer) in some logical state $|\psi\rangle$, interacting through some error process with an environment initially in state $|E\rangle$. Suppose this process is described by a unitary operator U_{err} acting on the joint state of the system and the environment. The state of the joint system after the interaction is then $U_{\text{err}}|\psi\rangle|E\rangle$. Its density matrix is

$$\rho = U_{\text{err}}|\psi\rangle|E\rangle\langle E|\langle\psi|U_{\text{err}}^{\dagger}. \tag{8}$$

Applying a trace operator on both sides of eq. (8) gives

$$TR_E(\rho) = TR_E\left(U_{\text{err}}|\psi\rangle|E\rangle\langle E|\langle\psi|U_{\text{err}}^{\dagger}\right) = \sum_i A_i\,|\psi\rangle\langle\psi|A_i^{\dagger}, \tag{9}$$

where A_i are operators acting on the system of interest (not including the environment). The error model is completely described by A_i.

For instance, the bit-flip error explained above can be described as an interaction between a qubit and the environment where the identity operator with probability $1-p$ and the X operator with probability p are applied. If the qubit is in the initial state $|\psi\rangle$, then the state after the error process is described by the density matrix

$$\rho_{\text{flip}} = (1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X. \tag{10}$$

Thus, A_i describing this error model is

$$\begin{aligned} A_0 &= \sqrt{1-p}\; I, \\ A_1 &= \sqrt{p}\; X. \end{aligned} \tag{11}$$

In the following sections, we focus on the practical protocol for distributing the entangled state and detecting the bit flip error in single photons along the quantum communication channel. On the basis of the type of error, proper selection of the linear optical element and adjustment of its position and angle in the photon transmission path can correct this error.

2 Error-free protocol for quantum entanglement distribution

In quantum communication, entangled photon pairs are created and sent to Alice and Bob over free space or a fiber link. These pairs need to be detected at the Alice and Bob stations. The detection method needs to select a basis to measure in, measure the polarization, and record enough information to match each photon Alice detects with the corresponding photon Bob detects. This section describes the linear optics components used to make the basis choice and polarization measurement, the detectors used to detect error in single-photon states, and the wave plates used to correct single-photon states.

The quantum entanglement distribution protocol, shown schematically in Figure 1, is proposed to distribute entangled photons between quantum communication stations and also to correct error along the quantum channel. Entangled photon pairs are produced by an EPR source employing a spontaneous parametric down-conversion (SPDC) [51]. The photons pass first through a polarizing beam splitter (PBS), which transmits horizontally polarized photons while reflecting vertically polarized photons. The outgoing photons are entered to separate quantum channels and are transmitted to the Alice and Bob stations. Note that the EPR source and Alice station can be one station. During photon transmission in the quantum channel, the environment can effect the photon and decoherence can occur. For this reason, preservation of the quantum channel against environmental effects such as heat and electromagnetic fields is important. In any event, if the quantum state changes in the transmission line, the proposed protocol can correct it. Arriving photons pass first through the PBS at the Alice and Bob stations. Because of the effect of PBS1 and PBS4, there are four possible output combinations: a single bit-flip error results in the output state emerging from either the (c1, d2) or (c2, d1) mode pair; a double error from (c1, c2); no error from (d1, d2). The corresponding corrections of the state are performed by HWP_1, HWP_2, or both, depending on the output mode pair. If the output state is accepted only from mode pair (d1, d2), then the scheme functions as a single-pair realization of error rejection. If the output state is accepted from all mode pairs, then a limited form of error-correction is performed.

The state of polarization-entangled photons pairs produced by SPDC may be written as

$$|\varphi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2\right), \tag{12}$$

where $|H\rangle$ $(|V\rangle)$ denotes the horizontal (vertical) linear polarization state of a photon and the ket subscripts denote the spatial propagation mode. PBSs transmit horizontally polarized photons and reflect vertically polarized photons.

The entangled state $|\phi\rangle_{12}$, after passing through four PBSs, becomes

$$\begin{aligned} |\varphi\rangle_{12} &= \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2\right) \\ &\xrightarrow{\text{PBS\_1,PBS\_2}} \frac{1}{\sqrt{2}}\left(|H\rangle_{\text{a1}}|H\rangle_{\text{a2}} + |V\rangle_{\text{b1}}|V\rangle_{\text{b2}}\right) \\ &\xrightarrow{\text{PBS\_3,PBS\_4}} \frac{1}{\sqrt{2}}\left(|H\rangle_{\text{d1}}|H\rangle_{\text{d2}} + |V\rangle_{\text{d1}}|V\rangle_{\text{d2}}\right) \\ &= |\varphi\rangle_{\text{d1d2}}. \end{aligned} \tag{13}$$

Eq. (13) indicates that the state shared by Alice and Bob via output modes d1 and d2 is equivalent to the polarization-entangled state produced at the source location. For these error-free transmissions, no photons are ever directed to modes c1 and c2. However, we know that quantum

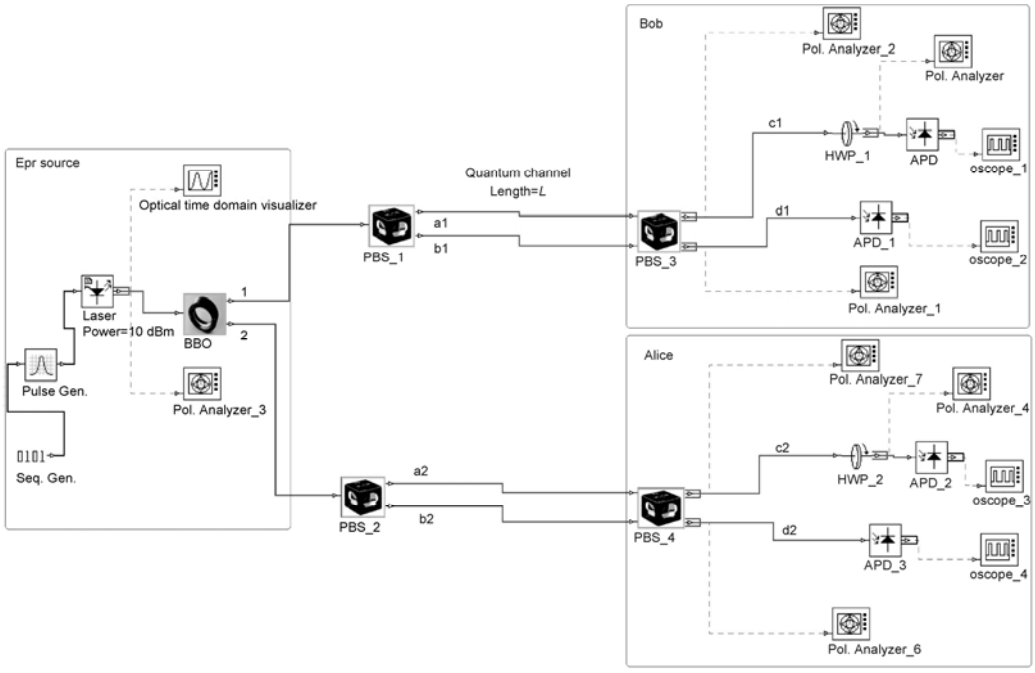


Figure 1 Entanglement distribution protocol.

channels such as fiber are not ideal and there is polarization-flip owing to the depolarizing optical fiber. Therefore, in the case of a single bit flip, the output state is obtained from either the (c1, d2) or (c2, d1) mode pair and is, respectively

$$|\varphi\rangle_{c1d2}=\frac{1}{\sqrt{2}}\left(|V\rangle_{c1}|H\rangle_{d2}+|H\rangle_{c1}|V\rangle_{d2}\right), \tag{14}$$

or

$$|\varphi\rangle_{c2d1}=\frac{1}{\sqrt{2}}\left(|H\rangle_{c2}|V\rangle_{d1}+|V\rangle_{c2}|H\rangle_{d1}\right). \tag{15}$$

In this case, the state shared by Alice and Bob differs from the initial entangled state and suffers an error. The error in the output state can be corrected very easily by placing a properly positioned (at 45° with respect to the $|H\rangle/|V\rangle$ basis) half-wave plate (HWP) in each of the two error channels c1 and c2. The HWP rotates the linear polarization state of an incoming photon into its orthogonal counterpart. As shown above, when there is a single bit flip, the flipped qubit will appear in either mode c1 or c2. The corresponding HWP in these modes then acts on the polarization state of that qubit and rotates it to the correct state. The final two-photon output state is equivalent to the initial source state with regard to the polarization entanglement and is obtained in the (c1, d2) or (c2, d1) mode pair. Supposing that there is a bit flip in quantum channel (1), we have

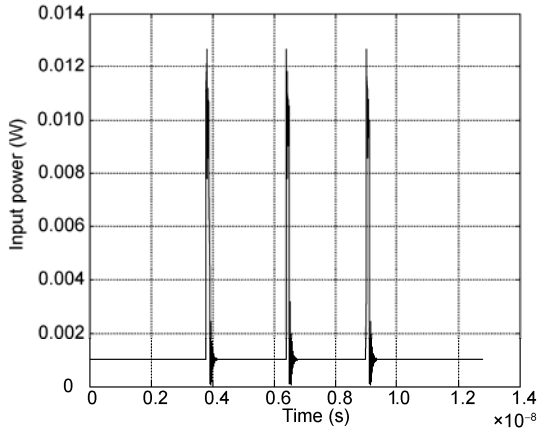
$$\begin{aligned}|\varphi\rangle_{12}&=\frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2+|V\rangle_1|V\rangle_2\right)\\&\xrightarrow{\text{PBS\_1,PBS\_2}}\frac{1}{\sqrt{2}}\left(|H\rangle_{a1}|H\rangle_{a2}+|V\rangle_{b1}|V\rangle_{b2}\right)\\&\xrightarrow{\text{bit-flip on quantum channel(1)}}\frac{1}{\sqrt{2}}\left(|V\rangle_{a1}|H\rangle_{a2}\right.\\&\quad\left.+|H\rangle_{b1}|V\rangle_{b2}\right)\\&\xrightarrow{\text{PBS\_3,PBS\_4}}\frac{1}{\sqrt{2}}\left(|V\rangle_{c1}|H\rangle_{d2}+|H\rangle_{c1}|V\rangle_{d2}\right)\\&\xrightarrow{\text{HWP\_1}}\frac{1}{\sqrt{2}}\left(|H\rangle_{c1}|H\rangle_{d2}+|V\rangle_{c1}|V\rangle_{d2}\right)\\&=|\varphi\rangle_{c1d2}.\end{aligned} \tag{16}$$

However, if there is a bit flip in quantum channel (2), the transformation is

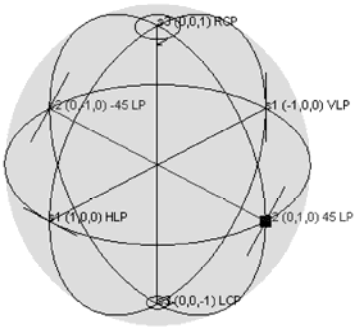
$$\begin{aligned}|\varphi\rangle_{12}&=\frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2+|V\rangle_1|V\rangle_2\right)\\&\xrightarrow{\text{PBS\_1,PBS\_2}}\frac{1}{\sqrt{2}}\left(|H\rangle_{a1}|H\rangle_{a2}+|V\rangle_{b1}|V\rangle_{b2}\right)\\&\xrightarrow{\text{bit-flip on quantum channel(2)}}\frac{1}{\sqrt{2}}\left(|H\rangle_{a1}|V\rangle_{a2}\right.\\&\quad\left.+|V\rangle_{b1}|H\rangle_{b2}\right)\\&\xrightarrow{\text{PBS\_3,PBS\_4}}\frac{1}{\sqrt{2}}\left(|H\rangle_{c2}|V\rangle_{d1}+|V\rangle_{c2}|H\rangle_{d1}\right)\\&\xrightarrow{\text{HWP\_2}}\frac{1}{\sqrt{2}}\left(|H\rangle_{c2}|H\rangle_{d1}+|V\rangle_{c2}|V\rangle_{d1}\right)\\&=|\varphi\rangle_{c2d1}.\end{aligned} \tag{17}$$

We see from eqs. (16) and (17) that there has been an error correction and the output states $|\varphi\rangle_{c1d2}$ and $|\varphi\rangle_{c2d1}$ are equivalent to the initial entangled state.

If there is a bit flip for both transmitted photons in the quantum channel, then the output state is obtained from modes c1 and c2 and is equivalent to the initial state $|\phi\rangle_{12}$:

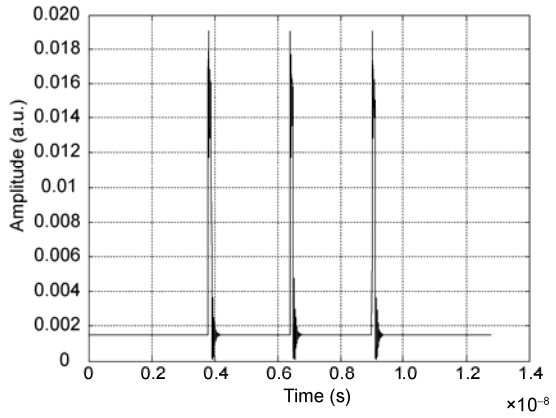


(a)

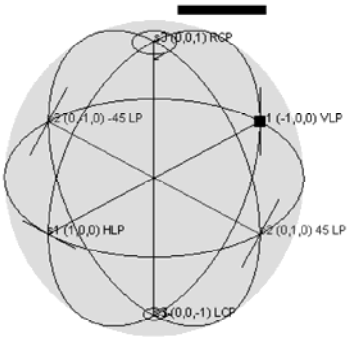


S0	s1	s2	s3	Azimuth	Ellipticity
−0.174748 dBm	1	0	0	45°	0

(d)

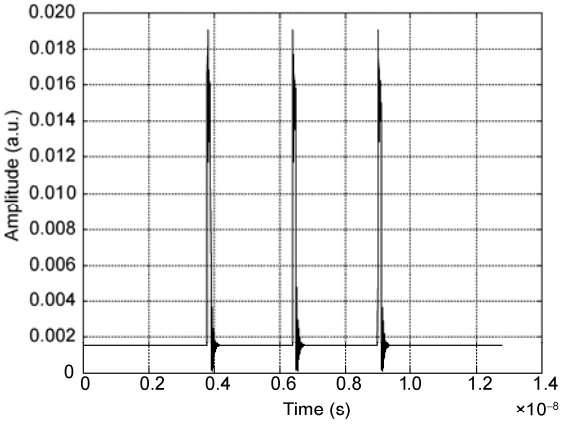


(b)

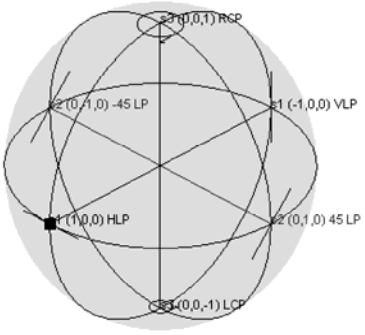


S0	s1	s2	s3	Azimuth	Ellipticity
−3.18 dBm	−1	0	0	90°	0

(e)



(c)



S0	s1	s2	s3	Azimuth	Ellipticity
−3.18 dBm	1	0	0	0	

(f)

Figure 2 Laser output power and photons detected at the Alice and Bob stations in the case of error-free transmission. (a) and (d), input power and polarization state of laser output photons; (b) and (e), APD output signal and polarization state of photons detected at the Alice station (port d2); (c) and (f), APD output signal and polarization state of photons detected at the Bob station (port d1).

$$|\varphi\rangle_{12}=\frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2+|V\rangle_1|V\rangle_2\right)$$

$$\xrightarrow{\text{PBS\_1,PBS\_2}}\frac{1}{\sqrt{2}}\left(|H\rangle_{a1}|H\rangle_{a2}+|V\rangle_{b1}|V\rangle_{b2}\right)$$

$$\xrightarrow{\text{bit-flip on quantum channel(1),(2)}}\frac{1}{\sqrt{2}}\left(|V\rangle_{a1}|V\rangle_{a2}+H_{b1}|H\rangle_{b2}\right)$$

$$\xrightarrow{\text{PBS\_3,PBS\_4}} \frac{1}{\sqrt{2}}\left(\left|V\right\rangle_{c1}\left|V\right\rangle_{c21}+\left|H\right\rangle_{c1}\left|H\right\rangle_{c2}\right)$$

$$\xrightarrow{\text{HWP\_1and HWP\_2}} \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_{c1}\left|H\right\rangle_{c21}\right.$$

$$\left.+\left|V\right\rangle_{c1}\left|V\right\rangle_{c21}\right)=\left|\varphi\right\rangle_{c1c2}. \quad (18)$$

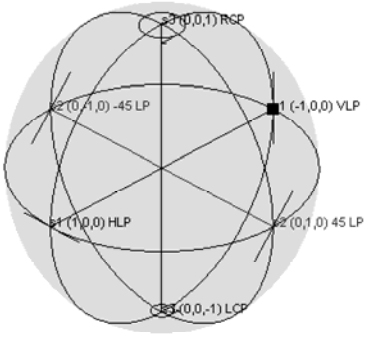
3 Simulation results and discussion

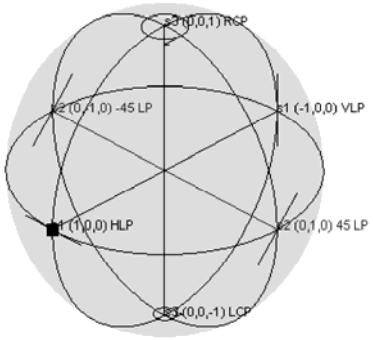
Simulations were carried out to verify the above numerical results. In the simulation, a laser produces triple optical picosecond pulses with linear polarization (+45°). The polarization-entangled photon pairs enter the two polarization beam splitters so that the polarization photon modes are spatially separated. The entangled photon pairs are then transmitted to the Alice and Bob stations via optical fiber as a quantum channel. The entangled-photon source can be near the Alice station, but for generality, it is supposed that they are far from each other. Quantum decoherence may take place in the quantum channel owing to environmental effects and fiber channel properties. The PBS is the first component in the Alice and Bob stations. Spatially separated photon modes enter these PBSs and output photons appear at output ports c1, c2, d1 and d1 depending on their polarization mode. In the first step of simulation, we suppose that there is no error in the quantum channel. Therefore, the output photon must emerge at the (d1, d2) output ports and APDs of ports c1 and c2 do not receive any photons. Figure 2 shows the profile of the input laser power and APD output signal and polarization states of photons detected at the Alice and Bob stations. As shown in the figure, the entangled photons only appear at the d1 and d2 ports.

It is now supposed that a bit-flip error occurs in quantum channel (1). This bit flip forces the photon in this channel to appear at the c1 port. However, according to eq. (14), the output entangled state is not the same as the initial state (eq. 12). The HWP at port c1 corrects this error, and eventually, the desired entangled state is obtained at the end stations of port (c1, d2). Figure (3) shows the polarization state of the photon at port c1 before and after reaching the HWP.

4 Conclusion

It has been shown that it is possible to distribute quantum entanglement to distant nodes implementing an error-free protocol. It is clear that error rejection is performed if Alice and Bob only receive the two-photon output state from the mode pair (d1, d2). Detection of both photons within modules APD_1 and APD_3 means that there was no bit flip during the distribution of the entangled state, ensuring that it is still of the initial entangled form. If Alice and Bob accept the output state from all four possible mode pairs, then an error correction can be performed on the output state using a properly oriented HWP.





S0	s1	s2	s3	Azimuth	Ellipticity
−3.18 dBm	−1	0	0	90°	0

(a)

S0	s1	s2	s3	Azimuth	Ellipticity
−3.18 dBm	1	0	0	0	0

(b)

Figure 3 Polarization state of a photon at port c1 before and after HWP_1.

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, 1984. 175–179
2 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
3 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem. Phys Rev Lett, 1992, 68: 557–559
4 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124

5 Bennett C H, Wiesner S J. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett, 1992, 69: 2881–2884
6 Goldenberg L, Vaidman L. Quantum cryptography based on orthogonal states. Phys Rev Lett, 1995, 75: 1239–1243
7 Huttner B, Imoto N, Gisin N, et al. Quantum cryptography with coherent states. Phys Rev A, 1995, 51: 1863–1869
8 Koashi M, Imoto N. Quantum cryptography based on split transmission of one-bit information in two steps. Phys Rev Lett, 1997, 79: 2383–2386
9 Bruß D. Optimal eavesdropping in quantum cryptography with six states. Phys Rev Lett, 1998, 81: 3018–3021
10 Hwang W Y, Koh I G, Han Y D. Quantum cryptography without public announcement of bases. Phys Lett A, 1998, 244: 489–494
11 Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85: 5635–5638
12 Cabello A. Quantum key distribution without alternative measurements. Phys Rev A, 2000, 61: 052312–052315
13 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302–032304
14 Shi B S, Jiang Y K, Guo G C. Quantum key distribution using different-frequency photons. Appl Phys B: Laser Opt, 2000, 70: 415–417
15 Xue P, Li C F, Guo G C. Conditional efficient multiuser quantum cryptography network. Phys Rev A, 2002, 65: 022317–022323
16 Deng F G, Liu X S, Ma Y J, et al. A theoretical scheme for multi-user quantum key distribution with *N* Einstein-Podolsky-Rosen pairs on a passive optical network. Chin Phys Lett, 2002, 19: 893–896
17 Phoenix S J D, Barnett S M, Townsend P D, et al. Multi-user quantum cryptography on optical networks. J Mod Opt, 1995, 42: 1155–1163.
18 Lo H K, Chan H F, Ardehali M. Efficient quantum key distribution scheme and proof of its unconditional security. J Cryptology, 2005, 18: 133–165
19 Wang W Y, Wang C, Zhang G Y, et al. Arbitrarily long distance quantum communication using inspection and power insertion. Chinese Sci Bull, 2009, 54: 158–162
20 Lu Z X, Yu L, Li K, et al. Reverse reconciliation for continuous variable quantum key distribution. Sci China-Phys Mech Astron, 2010, 53: 100–105
21 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. Acta Phys Pol A, 2002, 101: 357–368
22 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319–052322
23 Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305–044308
24 Juan Q S, Yan W Q, Ming M L, et al. Quantum secure direct communication over the collective amplitude damping channel. Sci China Ser G-Phys Mech Astron, 2009, 52: 1208–1212
25 Gu B, Pei S X, Song B, et al. Deterministic secure quantum communication over a collective-noise channel. Sci China Ser G-Phys Mech Astron, 2009, 52: 1913–1918
26 Li C Z. Real applications of quantum communications in China. Chinese Sci Bull, 2009, 54: 2976–2977
27 Elliott C. Building the quantum network. New J Phys, 2002, 4: 46.1–46.12
28 Xu F X, Chen W, Wang S, et al. Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Sci Bull, 2009, 54: 2991–2997
29 Tittel W, Brendel J, Zbinden H, et al. Quantum cryptography using entangled photons in energy-time bell states. Phys Rev Lett, 2000, 84: 4737–4740
30 Yupapin P P. Generalized quantum key distribution via micro ring resonator for mobile telephone networks. Optik-Int J Light Electron Optics, 2010, 121: 422–425
31 Ekert A K. Quantum cryptography based on bell's theorem. Phys Rev Lett, 1991, 67: 661–663
32 Mattle K, Weinfurter H, Kwiat P G, et al. Dense coding in experimental quantum communication. Phys Rev Lett, 1996, 76: 4656–4659
33 Adhikari S, Majumdar A S, Roy S, et al. Teleportation via maximally and non-maximally entangled mixed states. QIC, 2010, 10: 0398–0419
34 Brassard G. Quantum communication complexity (a survey). arXiv: quant-ph/0101005, 2001
35 Buhrman H, Dam W V, Høyer P, et al. Multiparty quantum communication complexity. Phys Rev A, 1999, 60: 2737–2741
36 Jennewein T, Simon C, Weihs G, et al. Quantum cryptography with entangledphotons. Phys Rev Lett, 2000, 84: 4729–4732
37 Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70: 1895–1899
38 Naik D S, Peterson C G, White A G, et al. Entangled state quantum cryptography: Eavesdropping on the ekert protocol. Phys RevLett, 2000, 84: 4733–4736
39 Brukner C, Zukowski M, Zeilinger A. Quantum communication complexity protocol with two entangledqutrits. Phys Rev Lett, 2002, 89: 197901–197904
40 Waks E, Zeevi A, Yamamoto Y. Security of quantum key distribution with entangled photons against individual attacks. Phys Rev A, 2002. 65: 52310–52325
41 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
42 Walton Z D, Abouraddy A F, Sergienko A V, et al. Decoherence-free subspaces in quantum key distribution. Phys Rev Lett, 2003, 91: 087901–087904
43 Yamamoto T, Shimamura J, Zdemir K, et al. Faithful qubit distribution assisted by one additional qubit against collective noise. Phys Rev Lett, 2005, 95: 040503–040506
44 Li X H, Deng F U, Zhou H U. Faithful qubit transmission against collective noise without ancillary qubits. App Phys Lett, 2007, 91: 144101–144103
45 Sheng Y B, Deng F G. Efficient quantum entanglement distribution over an arbitrary collective-noise channel. Phys Rev A, 2010, 81: 042332–042336
46 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement, and faithful teleportation via noisy channels. Phys Rev Lett, 1996, 76: 722–725
47 Pan J W, Simon C, Brukner C, et al. Feasible entanglement purification for quantum communication. Nature, 2001, 410: 1067–1070
48 Sheng Y B, Deng F G, Zhou H Y. Efficient polarization-entanglement purification based on parametric down conversion sources with cross-Kerr nonlinearity. Phys Rev A, 2008, 77: 042308–042315
49 Sheng Y B, Deng F G. Deterministic entanglement purification and complete nonlocal Bell-state analysis with hyperentanglement. Phys Rev A, 2010, 81: 032307–032313
50 Zukowski M, Zeilinger A, Horne M A, et al. Event ready detectors: Bell experiment via entanglement swapping. Phys Rev Lett, 1993, 71: 4287–4290
51 Kwiat P G, Mattle K, Weinfurter H, et al. New high-intensity source of polarization-entangled photon pairs. Phys Rev Lett, 1995, 75: 4337–4341