An Error-Free Protocol for Quantum Entanglement Distribution in Long Distance Quantum Communication

Shamsolah Salemian Shahram Mohammadnejad
Nanoptronics Research Center
Electronics and Electrical Engineering Department
Iran University of Science and Technology
salemian@iust.ac.ir shahramm@iust.ac.ir

***Abstract*- Quantum entanglement distribution is an essential part of quantum communication and computation protocols. Here, linear optic elements are employed for distribution of quantum entanglement over long distance. Polarization beam splitters and wave plates are used for realization of an error-free protocol for broadcasting quantum entanglement in optical quantum communication. This protocol can determine maximum distance of quantum communication to transmit quantum information without decoherence. Error detection and error correction are performed in the proposed scheme. In other words, if bit-flip occurs along the quantum channel, the end stations (Alice and Bob) can detect this state changing and obtain the correct state (entangled photon) on the 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 linear optics element that does not need quantum CNOT gate.**

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

I. INTRODUCTION

Quantum entanglement is an important concept of quantum physics and is the basis of most quantum communication and computation protocols [1-11]. 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 to construct a worldwide quantum communication network, that the distribution of quantum entanglement on a global scale is a central task of this network. Up to now, only photon is suitable system for long distance quantum communication. Other systems such as atoms or ions are studied, but their applicability for quantum communication schemes is presently not feasible within the near future. Therefore photons are the only choice for long-distance quantum communication. One of the problems of photon-based schemes is the loss of photons in the quantum channel. This limits the maximum distance of single photon transmission to about 10 km in present silica fibers [12-13]. This problem can be solved by subdividing the larger distance into smaller segment over which entanglement can be teleported. Eventually, entanglement swapping [14] is used for transporting of entanglement over long distances.

In this paper, an error-free protocol will be proposed to extend the bridgeable distance of single photons and subsequently reduce the number of quantum repeater along the quantum communication network. Error detection and error correction are performed in the proposed scheme. If qubit changes ($|0\rangle \rightarrow |1\rangle$ and $|1\rangle \rightarrow |0\rangle$) along the quantum channel, the state evolution can be detected by Alice and Bob and corrected states are obtained on another port. Here the linear polarization states of photons, $|H\rangle$ for 'horizontal' and $|V\rangle$ for 'vertical', will serve as the physical representation of logical bit values, with $|H\rangle \equiv |0\rangle$ and $|V\rangle \equiv |1\rangle$.

II. ERROR MODEL FOR QUANTUM INFORMATION

Understanding the nature of the errors is 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 would have to consider any correlation between errors on different bits. The same is true for errors on 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 encoded quantum state cannot be detected through the complete measurement of all the qubits.

Errors occur on a qubit when its alteration differs from the desired one. This difference can happen because of inexact control over the qubits or by interaction of the qubits with an 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 $|E\rangle$ will yield a superposition state of the form:

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

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

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

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

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

We can rewrite the state after the interaction as

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

Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$. Then we have

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

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

The interesting point is that a generic continuous evolution has been rewritten in terms of a finite number 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 on a Hilbert space of a single qubit.

Specific errors can be described as special cases of the right side of equation (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 $\beta_2|E_2\rangle = \beta_4|E_4\rangle$. Equation (5) for the general evolution thus simplifies to

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

Single qubit errors resulting from an uncontrolled situation leading to an inexact rotation of the qubit about the x-axis of the Bloch sphere and will have $\beta_1|E_1\rangle = c\beta_2|E_2\rangle$ for some constant c, so that the environment's state factors from the qubit's state and the operator $c\beta_2 I + \beta_2 X$ is unitary. In other words,

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

Therefore the error is called 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. Then the state of the joint system after the interaction is $U_{err}|\psi\rangle|E\rangle$. Its density matrix is

$$\rho = U_{err}|\psi\rangle|E\rangle\langle E|\langle\psi|U_{err}^{\dagger} \quad (8)$$

By applying trace operator on both sides of equation (8), the following relation is obtained,

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

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

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

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

So the A_i describing this error model are

$$\begin{aligned}A_0 &= \sqrt{1-p}\ I \\ A_1 &= \sqrt{p}\ X\end{aligned} \quad (11)$$

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

III. ERROR-FREE PROTOCOL FOR QUANTUM ENTANGLEMENT DISTRIBUTION

In quantum communication, entangled photon pairs are created and sent to Alice and Bob over the free space or fiber link. These pairs need to be detected in the Alice and Bob's 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 photons state, and the wave plates used to correct single photons state.

Quantum entanglement distribution protocol, shown schematically in Fig. 1, is proposed to distribute entangled photons between quantum communication stations and also to correct occurred error along the quantum channel. Entangled photon pairs are produced by EPR source using spontaneous parametric down conversion (SPDC) process [15]. The photons pass first through a polarizing beam splitter (PBS) which transmits horizontally polarized photons while reflecting vertically polarized photons. The outgoing photons lunch to the separate quantum channel and transmit to Alice and Bob stations. Note that the EPR source and Alice station can be in one station. During the photon transmission in the quantum channel, environmental can effect on the photon and decoherence can be happened. Because of this, preservation of quantum channel against the environmental effects such as temperature and electromagnetic field is very important. Anyway, if quantum state changes during transmission line, proposed protocol can correct it. Arrived photons pass first through PBS in Alice and Bob stations. Because of the effect of PBS1 and PBS4, there are four possible output combinations: a single bit-flip error will result 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 to the state are performed by HWP_1, or HWP_2, or both, depending on the output mode-pair. Modules Mc1, Md1, Mc2, Md2 represent the 'applications packages' and consist of unitary operations and detectors. 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 process may be written as

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

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

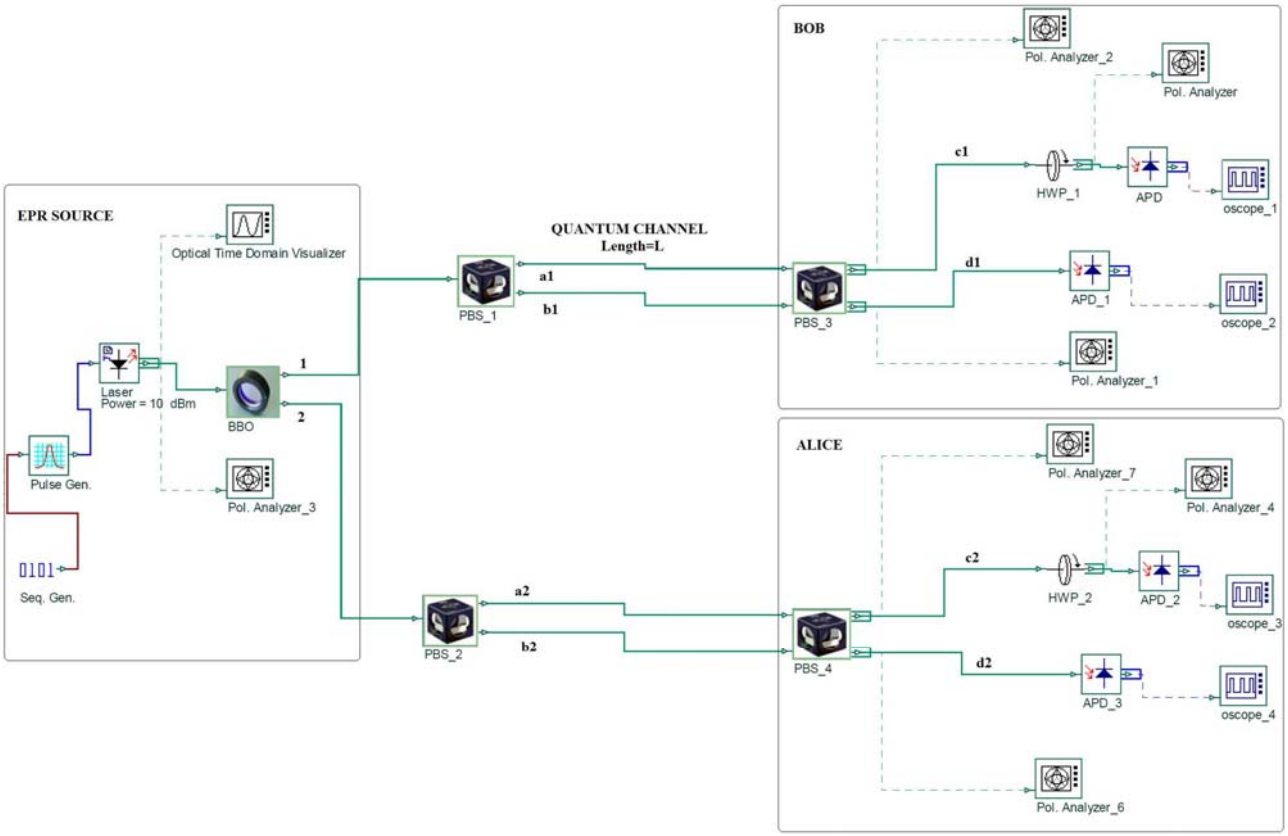

Fig.1: Entanglement distribution protocol

So that the entangled state $|\phi\rangle_{12}$, after passing through four PBSs, transfers to

$$|\phi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2\right)$$
$$\xrightarrow{PBS\_1, PBS\_2} \frac{1}{\sqrt{2}}\left(|H\rangle_{a1}|H\rangle_{a2} + |V\rangle_{b1}|V\rangle_{b2}\right) \quad (13)$$
$$\xrightarrow{PBS\_3, PBS\_4} \frac{1}{\sqrt{2}}\left(|H\rangle_{d1}|H\rangle_{d2} + |V\rangle_{d1}|V\rangle_{d2}\right) = |\phi\rangle_{d1d2}$$

As we see from equation (13), shared state between Alice and Bob via output modes d1 and d2 is equivalent to polarization-entangled state produced at the source location. For these error-free transmissions no photons are ever directed into modes c1and c2. But, we know that quantum channels such as fiber is not ideal and polarization-flip is occurred due to depolarizing optical fiber. Therefore, for the case of a single bit-flip, the output state will be obtained from either the (c1,d2) or (c2,d1) mode pair and will be of the following form respectively,

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

or

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

In this case, the shared state between Alice and Bob is different to initial entangled state and suffer an error. Error correction can be done on the output state 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 a single bit-flip happens, it means that the flipped qubit will appear in either mode c1or c2. Then the corresponding HWP in these modes act on the polarization state of that qubit and rotate it to correct state. The final two-photon output state will be equivalent to the initial source state with regard to the polarization entanglement and will be obtained in the (c1,d2) or (c2,d1) mode pair. Suppose bit flip happens in quantum channel (1), we have

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

But if bit flip happens in quantum channel (2), transformation is as following,

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

We can see from equation (16) and (17) that error correction has been done and output states $|\phi\rangle_{c1d2}$ and $|\phi\rangle_{c2d1}$ are equivalent to initial entangled state.

If bit-flip occurs in both transmitted photons in quantum channel, then the output state will be obtained from modes c1 and c2 and will be equivalent to the initial state $|\phi\rangle_{12}$ |,

$$|\phi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2\right)$$
$$\xrightarrow{PBS\_1, PBS\_2} \frac{1}{\sqrt{2}}\left(|H\rangle_{a1}|H\rangle_{a2} + |V\rangle_{b1}|V\rangle_{b2}\right)$$
$$\xrightarrow{bit-flip\ on\ quantum\ channel(1),(2)} \frac{1}{\sqrt{2}}\left(|V\rangle_{a1}|V\rangle_{a2} + H_{b1}|H\rangle_{b2}\right) \quad (18)$$
$$\xrightarrow{PBS\_3, PBS\_4} \frac{1}{\sqrt{2}}\left(|V\rangle_{c1}|V\rangle_{c21} + |H\rangle_{c1}|H\rangle_{c2}\right)$$
$$\xrightarrow{HWP\_1\ and\ HWP\_2} \frac{1}{\sqrt{2}}\left(|H\rangle_{c1}|H\rangle_{c21} + |V\rangle_{c1}|V\rangle_{c21}\right) = |\phi\rangle_{c1c2}$$

IV. CONCLUSION

Thus, it has been proved that it is possible to distribute quantum entanglement on distant node by an error-free protocol. It is clear that error rejection is performed if Alice and Bob only received the two photon output state from mode pair (d1,d2). Detection of both photons within modules APD_1 and APD_3 means that no bit-flip occurred 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 by using properly oriented HWP.

REFERENCE

[1] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, “Quantum cryptography using entangled photons in energy-time bell states,” Phys. Rev. Lett., vol. 84, p. 4737, 2000.

[2] P.P. Yupapin, " Generalized quantum key distribution via micro ring resonator for mobile telephone networks," Optik - International Journal for Light and Electron Optics, vol. 121, Issue 5, pp. 422-425, 2010

[3] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” Phys. Rev. Lett., vol. 67, pp. 661–663, 1991.

[4] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger,“Dense coding in experimental quantum communica-tion,” Phys. Rev. Lett., vol. 76, no. 25, pp. 4656–4659,1996.

[5] S. Adhikari, A.S. Majumdar, S. Roy, B. Ghosh, and N. Nayak, "Teleportation via maximally and non-maximally entangled mixed states," QIC, vol.10 No.5&6, pp. 0398-0419, 2010.

[6] G. Brassard, “Quantum communication complexity (asurvey),” quant-ph/0101005, 2001.

[7] H. Buhrman, W. V. Dam, P. Høyer, and A. Tapp, “Multiparty quantum communication complexity,” Phys. Rev.A, vol. 60, pp. 2737–2741, 1999.

[8] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, andA. Zeilinger, “Quantum cryptography with entangledphotons,” Phys. Rev. Lett., vol. 84, p. 4729, 2000.

[9] C. H. Bennett, G. Brassard, C. Cr´epeau, R. Jozsa,A. Peres, and W. K.Wootters, “Teleporting an unknownquantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett., vol. 70, no. 13, pp.1895–1899, 1993.

[10] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund,and P. G. Kwiat, “Entangled state quantum cryptography: Eavesdropping on the ekert protocol,” Phys. Rev.Lett., vol. 84, p. 4733, 2000.

[11] C. Brukner, M. Zukowski, and A. Zeilinger, “Quantum communication complexity protocol with two entangledqutrits,” Phys. Rev. Lett., vol. 89, p. 197901, 2002.

[12] E. Waks, A. Zeevi, and Y. Yamamoto, “Security of quantum key distribution with entangled photons against in-dividual attacks,” Phys. Rev. A, vol. 65, p. 52310, 2002.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys., vol. 74, pp. 145–195, 2002.

[14] M. ˙ Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ek-ert, ““Event ready detectors” Bell experiment via entan-glement swapping,” Phys. Rev. Lett., vol. 71, no. 26.

[15] P.G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V.Sergienko, Y.H. Shih, Phys. Rev. Lett. 75 (1995) 4337.

Shamsolah Salemian was born in 1976. He received the B.Sc. degree from Shiraz University and the M.Sc. degree from Iran University of Science and Technology (IUST). He is currently working toward the Ph.D. degree at IUST where his research interests include quantum communication and computation and optical integrated circuits.

Shahram Mohammadnejad received the B.Sc. degree in electrical engineering from the University of Houston, Houston, TX, in 1981 and the M.Sc. and Ph.D. degrees in semiconductor material growth and lasers from Shizuoka University, Shizuoka, Japan, in 1990 and 1993, respectively.

He invented the PdSrS laser for the first time in 1992. He has published more than 80 scientific papers and books. His research interests include semiconductor material growth, quantum electronics, semiconductor devices, optoelectronics, and lasers. Dr. Mohammadnejad is a scientific committee member of the Iranian Conference of Electrical Engineering (ICEE), a member of Institute of Engineering and Technology (IET), and a member of IET- CEng.