Quantum key distribution via an optical wireless communication link for telephone networks

S. Suchat,[a,b] W. Khunnam,[a] and P. P. Yupapin,[b] MEMBER SPIE
[a]King Mongkut's Institute of Technology Ladkrabang, Advanced Research Center for Photonics, Department of Applied Physics, Faculty of Science, Ladkrabang Bangkok 10520, Thailand
[b]Thammasat University, Department of Physics, Faculty of Science and Technology, Pathumtani 12121, Thailand
E-mail: kypreech@kmitl.ac.th

Abstract. We propose a new system of quantum key distribution via optical wireless communication links, where the required information, especially telephone conversation, can be secured by using a quantum code/decode (CODEC) technique incorporated in the networks. The entangled photons can be encoded into the classical information and then the decoded signal can also be retrieved. The proposed system consists of quantum key generation and uplink and downlink parts that can be implemented in the mobile telephone handset and networks. Such a system and technique show the feasibility of use for a perfectly security telephone networks. [DOI: 10.1117/1.2786479]

Subject terms: optical wireless; quantum key; perfect security.

Paper 070252LRRR received Mar. 20, 2007; revised manuscript received Jul. 17, 2007; accepted for publication Jul. 23, 2007; published online Oct. 3, 2007.

The mobile telephone has been widely and commonly used for nearly two decades. Because many applications can be provided by a network provider, the demand for use of the mobile phone is large. Furthermore, there are some advantages including a small size, lightweight, and especially, low cost, which means these phones can be applied worldwide. However, there is a serious problem of interception, when perfect security is required by users. Up to now, no system that can secure personal data safely from an eavesdropper has been implemented in telephone networks. Recently, Yupapin and Suchat[1] reported the use of weak light to produce nonlinear behavior of light in a fiber optic ring resonator instead of using a strong light pulse in an ordinary single-mode fiber. Four-wave mixing results from the delayed pulse trains and nonlinear Kerr-type effects in a fiber ring resonator could perform the required entangled states after certain controlled polarization states. Delayed polarization modes via the ring resonator[2] were combined, and the entangled photon states were observed and registered. In practice, the simple design and arrangement of quantum key generation can result in a quantum device for mobile telephone and realistic network use, i.e., the quantum key generation device is now possible in the micrometer scale range. An optical link has shown the potential of being used for long-distance quantum communication, where the transmission of classical and quantum channels are required to transmit via an optical wireless link and where the sender and user can confirm the requested data. Zhou et al.[3] proposed an optical fiber communication system for optical downlink transmission with remote millimeter-wave local-oscillator delivery for intermediate frequency fiber uplink transmission by a wireless transmission of several kilometers. Manderbach et al.[4] have reported on the experimental implementation of Bennett-Brassard 1984 (BB84)-protocol-type quantum key distribution over a 144-km free-space link using weak coherent laser pulses.

In this communication, we propose the concept of an optical wireless communication link for telephone networks. In this concept, we assume that quantum cryptography, quantum teleportation, quantum key and quantum coding and decoding can be implemented using an optical wireless communication link, where the uplink and downlink can be performed and used by a commercial mobile telephone device, where each of the transmitted wavelengths can randomly form the entangled pairs, i.e., the quantum key. The quantum code/decode (CODEC) of the quantum keys can be performed and linked via wireless and optical transmission links. In this application, the idea of an optical encryption technique experiment can be realized to create top-security for mobile telephone uplink and downlink converters and communications. Such a design can also be used with all types of network distributions, where the qubits can be performed and used in the link distributions.

To begin our discussion of this concept, first, we introduce a technique that can be used to create the quantum CODEC. Figure 1 shows[1] a polarization coupler that separates the basic vertical and horizontal polarization states corresponding to an optical switch between short and long pulses. We assume these horizontally polarized pulses with a temporal separation of Δt. The coherence time of the consecutive pulses is larger than Δt. Then the following time-bin state including polarization dispersion is created through a Mach-Zehnder Interferometer (MZI).

$$|\Phi\rangle_p = |1,H\rangle_s|1,H\rangle_i + |2,H\rangle_s|2,H\rangle_i. \tag{1}$$

In the expression of $|k,H\rangle$, k is the number of time slots ($k=1,2$), the state of polarizations are denoted by horizontal (H) or vertical (V), and the subscripts imply the state of the signal (s) or the idler (i). In Eq. (1), for simplicity we omitted an amplitude term that is common to all product states, as done similarly in the subsequent equations in this paper. The two-photon states with H polarization, shown in Eq. (1), are the input into the orthogonal polarization-delay circuit (fiber ring resonator).

The delay circuit consists of a coupler and the difference between the round-trip times of the fiber ring resonator, which is equal to Δt. The polarization controller (PC) is tilted to changing the round trip of the fiber ring, and then converted to V at the delay circuit output. This causes the term $|k,H\rangle$ in Eq. (1) to be converted to the term $r|k,H\rangle + t_2 \exp(i\phi)|k+1,V\rangle + rt_2 \exp(i_2\phi)|k+2,H\rangle + r_2t_2 \exp(i_3\phi)|k+3,V\rangle$. Here t and r are the amplitude transmission coefficients for the throughput and crosspaths of a coupler. Equation (1) is then converted into the polarized state by the circuit of Fig. 1 as

$$|\Phi\rangle = [|1,H\rangle_s|1,H\rangle_i + \exp(i\phi_i)|1,H\rangle_s|2,V\rangle_i] + \exp(i\phi_s) \times|2,V\rangle_s|1,H\rangle_i + \exp[i(\phi_s+\phi_i)]|2,V\rangle_s|2,V\rangle_i + |2,H\rangle_s|2,H\rangle_i + \exp(i\phi_i)|2,H\rangle_s|3,V\rangle_i + \exp(i\phi_s) \times|3,V\rangle_s|2,H\rangle_i + \exp[i(\phi_s+\phi_i)]|3,V\rangle_s|3,V\rangle_i. \quad (2)$$

By the coincidence of the counts in the second time slot, we can extract the fourth and fifth terms. As a result, we can obtain the following polarization entangled state as

$$|\Phi\rangle = |2,H\rangle_s|2,H\rangle_i + \exp[i(\phi_s+\phi_i)]|2,V\rangle_s|2,V\rangle_i. \quad (3)$$

In the case of a system using weak light input (i.e., without pumping part and component), the fiber acts as a nonlinear medium because of the optical Kerr effect and four-wave mixing in the fiber ring resonator. The use of a long fiber with small core and ring radius is attractive for achieving a high optical intensity and long interaction length. The nonlinear effect that implements this setup is of the four-wave mixing type. In Fig. 1, we proposed a system configuration that the remote access point (RAP) can be required to perform the optical-to-electrical (O/E) and/or electrical-to-optical (E/O) conversion as well as radio frequency (rf) radiating/receiving. The downlink/uplink rf carriers can be feasibly delivered between Alice and Bob. The polarization state from Alice can be maintained by a state registration of polarization state by Bob and consequently he receives the correct polarization state.

Let us first consider the case where the reference photon passes through the path L and the signal photon through the path S, as shown in Fig. 1. In this case, these photons reach the PBC at the same time. As in the parity checking

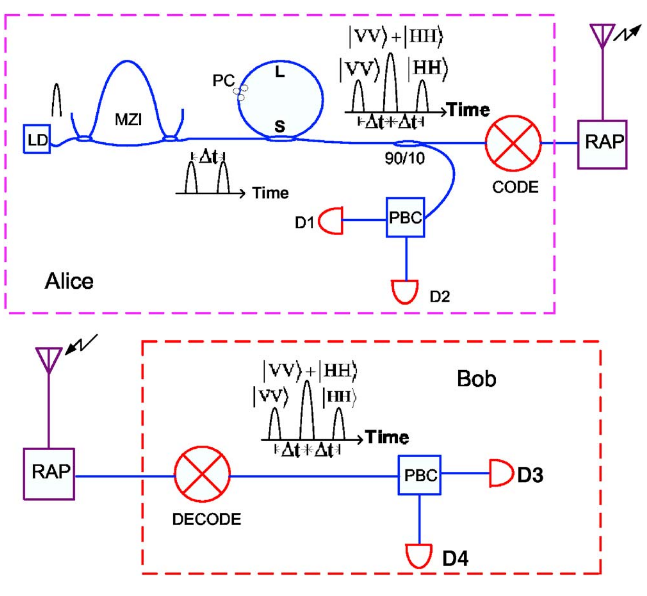

Fig. 1 Schematic diagram of an optical wireless communication link for telephone networks system: PO; polarization control: LD; laser diode; RAP, remote access point; PBC, polarization beam combiner; and D, avalanche photodetector.

described, the incoming photons in the states $|H\rangle_i|H\rangle_s$ and $|V\rangle_i|V\rangle_s$ (the two photons have different polarizations just before the PBC) result in a two-photon state and a vacuum in the mode X, respectively. On the other hand, the photons in the state $\alpha|V\rangle_i|H\rangle_s+\beta|H\rangle_i|V\rangle_s$ (the two photons have the same polarization just before the PBC) result in one photon in the mode X and one photon in Y, in the state $\alpha|H\rangle_X|H\rangle_Y+\beta|V\rangle_X|V\rangle_Y$. Hence, by counting the number of photons in the mode X, we can discard the cases $|H\rangle_i|H\rangle_s$ and $|V\rangle_i|V\rangle_s$. If Bob detects a photon in $|D\rangle_X$, the two photons are projected onto the state $|D\rangle_X(\alpha|H\rangle_Y+\beta|V\rangle_Y)$. Then Bob obtains the photon in the signal state $\alpha|H\rangle_Y+\beta|V\rangle_Y$.

In a practical communication tasks such as quantum key distribution (QKD), photons in mode Y can be measured on a polarization basis. In this case, one can postselect the event where at least one photon is emitted in each mode X and Y by the twofold coincidence detection. Therefore, the conventional threshold photon detectors, which do not discriminate two or more photons from a single photon, can be used. In the other cases, where the reference photon passes through the path S and/or the signal photon passes through the path L, at least one of the photons should have a different arrival time at detector $|D\rangle_X$ or $|D\rangle_Y$. Hence, we can eliminate the contributions from such cases by discriminating the arrival times of the photons at the detectors $|D\rangle_X$ and $|D\rangle_Y$ by postselection. Any losses in the channels and inefficiencies of the detectors are also discarded by the postselection. A single photon is formed in an MZI that incorporates a fiber optic ring resonator. Each of the entangled pair, which can be clarified by a quantum key between Alice and Bob, where the required memory and speed are realized, can form the correct code, forms the signal. In this application, the idea of the proposed optical encryption technique can be realized to create top security for a mobile telephone uplink converter and communication. The down stream link can be similarly implemented.

We proposed the idea of a new system of the quantum key distribution via an optical wireless communication link for telephone network applications. In practice, a set of all possible states sent by Alice to Bob is a set of two states corresponding to the identical bits, where the two states are horizontal (H) and vertical (V) polarization photons instead of a photon, which is observed as a random orientation. In this application, the idea of the proposed optical encryption technique can be realized to create top security for a mobile telephone uplink converter and communications.

In conclusion, the quantum CODEC can be formed by a fiber optic device, which consists of an MZI incorporated with a fiber optic ring resonator. Then the quantum keys could be distributed in the networks via the optical wireless link, where perfect security can be formed between Alice and Bob without any cheating from Eave. Finally, the classical channel signals can be recovered using the quantum CODEC. The top security information, using a CODEC technique based on quantum cryptography by light, i.e., entangled photons, was discussed and a simple setup demonstrated.

Acknowledgments

The authors would like to acknowledge to the Department of Applied Physics, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand, for supporting the laboratory facilities. S. Suchat (PhD candidate) would like to acknowledge to the Department of Physics, Faculty of Science and Technology, Thammasat University (TU), Thailand, for some financial support of his study.

References

1. P. P. Yupapin and S. Suchat, "Entangled photon generation using fiber optic Mach-Zehnder interferometer incorporating the nonlinear effect in a fiber ring resonator," *J. Nanophoton.* **1**, 013504 (2007).
2. P. P. Yupapin, P. Saeung, and C. Li, "Characteristics of complementary ring-resonator add/drop filters modeling by using graphical approach," *Opt. Commun.* **272**, 81–86 (2007).
3. M. T. Zhou, J. G. Zhang, A. B. Sharma, Y. Zhang, S. Xiao, and M. Fijise, "Design of millimeter-wave fiber-wireless downlink with remote local-oscillator delivery by using dual-electrode Mach-Zehnder modulators configured for optical single-sideband modulations," *Opt. Commun.* **269**, 69–75 (2007).
4. T. S. Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free space decoy-state quantum key distribution over 144 mm," *Phys. Rev. Lett.* **98**, 010504 (2007).