Optik 125 (2014) 1522–1525

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Analysis of polarization state in quantum key distribution via single-photon two-qubit states

Gu-hao Zhao [a,*], Shang-hong Zhao [a], Zhou-shi Yao [b], Chen-Lu Hao [c], Wen Meng [a], Xiang Wang [a], Zhi-hang Zhu [a], Feng Liu [b]

[a] School of Information and Navigation, Air Force Engineering University, Xian 710077, Shaanxi, China
[b] Xi'an Branch of China Academy of Space Technology, Xian 710000, Shaanxi, China
[c] School of Air and Missile Defense, Air Force Engineering University, Xian 710077, Shaanxi, China

ARTICLE INFO

Article history:
Received 2 March 2013
Accepted 3 July 2013

PACS:
03.67.Dd
84.40.Ua
77.22.Ej

Keywords:
Quantum key distribution
Mach–Zehnder interferometers
Phase coding
Polarization coding
Stability conditions of polarization

ABSTRACT

An improved quantum key distribution scheme via single-photon two-qubit states is proposed. The input–output model of the polarization state is established. And the influence of the interferometers to the polarization state is analyzed. Quantum bit error rate of polarization coding caused by birefringent and coordinate system difference between incident light and the fast and slow axes in fiber interferometer is simulated. Furthermore, maintaining conditions of polarization state are given on this basis.

1. Introduction

Since Bennett and Brassard presented the first quantum key distribution (QKD) scheme in 1984 [1], quantum cryptography is attracting researchers' attention [2–4]. A lot of schemes and theories have been proposed and improved [5–8]. These QKD schemes and theories have been implemented in a number of groups both in fiber-based systems [9–11] and in free space arrangements [12–16].

Most existing QKD systems rely on either polarization or phase of faint laser pulses as an information carrier. For long-distance free space distribution, the main difficulty of practical systems is the key generation rate. Because of the link loss, "Bob" can just capture a few photons which "Alice" sends to. It is not a significant issue for experimental demonstrations but a vital disadvantage for practical applications. Several schemes have been proposed to improve the key generation rate [17,18]. Single-photon two-qubit states possess a deterministic nature that can be exploited for direct secure communication [19]. Paper [20] proposed a scheme for quantum key distribution, in which a single photon is encoded with polarization state and phase state. But the implementation system of this scheme is a little bit complicated, and it has just analyzed the security and implementation roughly.

In this article, an improvement scheme of free-space QKD via single-photon two-qubit states is proposed. The implementation system of this scheme is concise. And the quantum bit error rate (QBER) of polarization coding caused by fiber M–Z interferometer is discussed.

2. Improvement scheme of two-qubit QKD

The implementation system in paper [21] needs four interferometers and also needs as many photon detectors and beam splitters as two polarization QKD systems. So we improve the scheme and implementation system as shown in Fig. 1.

The two-qubit QKD scheme setups are shown in Fig. 1. Only four semiconductor lasers (LD1–LD4) send out one pulse carried polarization message at a time. The laser pulse passed through Alice's interferometer and was modulated phase information and attenuated by the attenuator (A). Then, the pulse was launched into free space. The pulse was caught by Bob's antenna and passed through an interferometer. Then enters the detection unit that has eight

* Corresponding author.
E-mail address: zghlupin@163.com (G.-h. Zhao).

0030-4026/$ – see front matter © 2013 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2013.07.072

detectors (D) on the output of Bob's interferometer to distinguish what phase and polarization message the photon takes.

L, S represents, respectively, the long and short arms of Alice and Bob's interferometers. Like the original phase QKD system, here are four possible paths to reach the detectors in the two-qubit QKD scheme; they are L + S, S + S, S + L, L + L. Fig. 2 shows the output pulses of Bob's interferometer. Because the lengths of L + S and S + L are equal, so these two pulses overlap in time domain (pulse B), and the interference occurs. For the pulses of path S + S and path L + L, here is no interference. So they are kept out of the door in original phase QKD scheme. The two-qubit QKD scheme is proposed to codes the phase and polarization information in one photon. Specifically, the interference pulse (pulse B) carries both phase and polarization information, and the pulses (A and C) which are discarded in the original phase QKD scheme can be coded in polarization information.

The principle of key distribution in the improvement scheme is as follows.

(1) The polarization coding unit of Alice randomly activates for each photon pulse to rotate the state of polarization to one of the four states, which are -45° $((1/\sqrt{2})|H\rangle - (1/\sqrt{2})|V\rangle)$, $+45^\circ$ $(1/\sqrt{2}|H\rangle + 1/\sqrt{2}|V\rangle)$, 0° $(|H\rangle)$, 90° $(|V\rangle)$, then sends them into the M–Z interferometer.
(2) The phase modulator randomly encodes $0, \pi, \pi/2$ or $3\pi/2$ states to pulse in the long arm. Then the photon carries two different quantum key information which are sent to Bob.
(3) In much the same way that phase QKD scheme decode does, the Bob's phase modulator selects 0 or $\pi/2$ phase to measuring what phase the pulse B takes.
(4) All the pulses of A, B and C carry the polarization information. The polarization decoding units decoding the polarization information in the same way as polarization QKD scheme, both in out1 and out2.

Bob told Alice what measurement matrix he used in the phase and polarization detection. But Bob did not publish the result he had obtained. Then Alice tells Bob which results are correct.

3. Polarization QBER caused by M–Z interferometers

From the standpoint of interference, the difference of transmission matrix between long arm and short arm must be very small. And in some mobile platforms, the polarization state will change with the change of mirror's position drastically. Typically, the encapsulated fiber interferometer is used in the phase QKD scheme quantum distribution experiment. But the polarization state of photon also changes slowly in the fiber system, largely because of the birefringence. The bit error rate of polarization coding increases. We will discuss the variation regularity of polarization state and QBER under the influence of fiber interferometer in detail below.

Take the case of S + S path, suppose Jones vector of incident light is $E_{\text{Ain}} = \begin{bmatrix} E_{x1} \\ E_{y1} \end{bmatrix}$, and the output light is $E_{\text{out1}} = \begin{bmatrix} E_{x2} \\ E_{y2} \end{bmatrix}$. The coordinate system of fast and slow axes in the fiber interferometer is (u, v). The coordinate system of incident light is (x, y), and the angle between these two coordinate systems is θ. Matrix for coordinate transform is $R(\theta) = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$. Jones matrix of fiber is $J = \begin{bmatrix} e^{i\eta_{\text{SX}}} & 0 \\ 0 & e^{i\mu_{\text{SX}}} \end{bmatrix} = e^{i(\eta_{\text{SX}}+\mu_{\text{SX}})/2} \begin{bmatrix} e^{i\psi_{\text{SX}}/2} & 0 \\ 0 & e^{i\psi_{\text{SX}}/2} \end{bmatrix}$, $\psi_{\text{SX}} = \eta_{\text{SX}} - \mu_{\text{SX}}$ is the phase difference between v-phase component and u-phase component, and SX = {SA, SB} represent the short arm fibers of interferometer both on Alice's side and Bob's side. Considering the difference between coordinate systems of two fiber-based interferometers, J_C is the rotation matrix.

$$
\begin{aligned}
E_{\text{out1}} &= \begin{bmatrix} E_{x2} \\ E_{y2} \end{bmatrix} = R(-\theta) J_{\text{SB}} R(\varphi) C e^{i\phi} J_{\text{SA}} R(\theta) \begin{bmatrix} E_{x1} \\ E_{y1} \end{bmatrix} \\
&= R(-\theta) e^{\frac{i(\eta_{\text{SB}}+\mu_{\text{SB}})}{2}} \begin{bmatrix} e^{\frac{i\psi_{\text{SB}}}{2}} & 0 \\ 0 & e^{\frac{-i\psi_{\text{SB}}}{2}} \end{bmatrix} \\
&\quad R(\varphi) C e^{i\phi} e^{\frac{i(\eta_{\text{SA}}+\mu_{\text{SA}})}{2}} \begin{bmatrix} e^{\frac{i\psi_{\text{SA}}}{2}} & 0 \\ 0 & e^{\frac{-i\psi_{\text{SA}}}{2}} \end{bmatrix} R(\theta) \begin{bmatrix} E_{x1} \\ E_{y1} \end{bmatrix} \\
&= R(-\theta) \begin{bmatrix} e^{\frac{i\psi_{\text{SB}}}{2}} & 0 \\ 0 & e^{\frac{-i\psi_{\text{SB}}}{2}} \end{bmatrix} R(\varphi) \begin{bmatrix} e^{\frac{i\psi_{\text{SA}}}{2}} & 0 \\ 0 & e^{\frac{-i\psi_{\text{SA}}}{2}} \end{bmatrix} \\
&\quad R(\theta) \begin{bmatrix} E_{x1} \\ E_{y1} \end{bmatrix} e^{\frac{i(\eta_{\text{SB}}+\mu_{\text{SB}})}{2}} e^{i\phi} e^{\frac{i(\eta_{\text{SA}}+\mu_{\text{SA}})}{2}} \\
&= R(-\theta) \begin{bmatrix} e^{\frac{i(\psi_{\text{SB}}+\psi_{\text{SA}})}{2}} \cos\varphi & e^{\frac{i(\psi_{\text{SB}}-\psi_{\text{SA}})}{2}} \sin\varphi \\ -e^{\frac{i(\psi_{\text{SA}}-\psi_{\text{SB}})}{2}} \sin\varphi & e^{\frac{-i(\psi_{\text{SB}}+\psi_{\text{SA}})}{2}} \cos\varphi \end{bmatrix} \\
&\quad R(\theta) \begin{bmatrix} E_{x1} \\ E_{y1} \end{bmatrix} e^{\frac{i(\eta_{\text{SB}}+\mu_{\text{SB}})}{2}} e^{i\phi} e^{\frac{i(\eta_{\text{SA}}+\mu_{\text{SA}})}{2}}
\end{aligned}
$$

where the Φ represents common phase of the atmospheric channel, C is considered as unitary. Let $M = R(-\theta) \begin{bmatrix} e^{i\rho} & 0 \\ 0 & e^{-i\rho} \end{bmatrix} R(\theta)$, $\rho = (\psi_{\text{SB}} + \psi_{\text{SA}})/2$ represent the birefeingent phase difference between fast and slow axes in the path.

$$
\begin{aligned}
M &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} e^{i\rho} & 0 \\ 0 & e^{-i\rho} \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \\
&= \begin{bmatrix} \cos^2\theta e^{i\rho} + \sin^2\theta e^{-i\rho} & \sin\theta\cos\theta(e^{i\rho} - e^{-i\rho}) \\ \sin\theta\cos\theta(e^{i\rho} - e^{-i\rho}) & \sin^2\theta e^{i\rho} + \cos^2\theta e^{-i\rho} \end{bmatrix} \\
&= \begin{bmatrix} \cos\rho + i\sin\rho\cos 2\theta & i\sin\rho\sin 2\theta \\ i\sin\rho\sin 2\theta & \cos s\rho - i\sin\rho\cos 2\theta \end{bmatrix}
\end{aligned}
$$

The polarization measurement is little affected by the public phase. And the output of these four polarizations in polarization coding could be:

$$
\begin{aligned}
E_{\text{out0}} &= ME_0 = \begin{bmatrix} \cos\rho + i\sin\rho\cos 2\theta \\ i\sin^2\rho\sin 2\theta \end{bmatrix} \\
&= \sqrt{\cos^2\rho + \sin^2\rho\cos^2 2\theta}|0\rangle + \sqrt{\sin^2\rho + \sin^2 2\theta}|1\rangle
\end{aligned}
$$

$$
\begin{aligned}
E_{\text{out90}} &= ME_{90} = \begin{bmatrix} i\sin\rho\sin 2\theta \\ \cos\rho - i\sin\rho\cos 2\theta \end{bmatrix} \\
&= \sqrt{\sin^2\rho\sin^2 2\theta}|0\rangle + \sqrt{\cos^2\rho + \sin^2\rho\cos^2 2\theta}|1\rangle
\end{aligned}
$$