Optics Communications 284 (2011) 5856–5859

Contents lists available at SciVerse ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Influence of light source linewidth in differential-phase-shift quantum key distribution systems

T. Honjo [a], T. Inoue [b], K. Inoue [b,*]

[a] NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosatowakamiya, Atsugi, Kanagawa, 243-0198, Japan
[b] Osaka University, 2-1 Yamadaoka, Suita, Osaka, 565-0871, Japan

ARTICLE INFO

Article history:
Received 25 May 2011
Received in revised form 8 August 2011
Accepted 23 August 2011
Available online 9 September 2011

Keywords:
Quantum key distribution
Differential-phase-shift QKD
Spectral linewidth

ABSTRACT

Differential-phase-shift (DPS) quantum key distribution (QKD) is one of the QKD protocols, featuring simplicity for practical implementation. It uses a coherent pulse train whose phase should be stable at least within the pulse interval. This paper quantitatively investigates the phase stability required for DPS-QKD systems. The phase stability is characterized by the spectral linewidth of the light source. A theoretical model and experiments are presented, the results of which indicate that the linewidth should be, for example, less than 0.35% of the free-spectral-range of an asymmetric Mach–Zehnder interferometer in a receiver to achieve quantum bit error rate of less than 0.5% due to linewidth broadening of the light source.

1. Introduction

Quantum key distribution (QKD) provides a secret key for secure communications, whose security is guaranteed by quantum mechanics [1]. Various QKD protocols have been proposed, such as the most famous and well studied BB84. The differential-phase-shift (DPS) QKD protocol is one of them, which features simplicity for practical implementation and robustness against photon number splitting attacks even if it uses attenuated coherent light [2,3]. Long-haul or high-speed QKD experiments have been demonstrated using the DPS-QKD protocol [4–6].

In DPS-QKD systems, the key bit information is conveyed by phase differences between adjacent pulses in a pulse train of weak coherent light. Thus, the phase of the coherent light should be stable at least within the pulse interval for the system to correctly provide a secret key. However, it has not been quantitatively clarified yet how stable the light phase should be. With this background, this paper investigates influence of phase fluctuation of the light source on DPS-QKD systems. The phase fluctuation is characterized by the spectral linewidth. Theoretical work and QKD experiments are carried out, examining influence of the light source linewidth on the quantum bit error rate in DPS-QKD systems. The results indicate that the linewidth should be, for example, less than 0.35% of the free-spectral-range of an asymmetric Mach–Zehnder interferometer used in a receiver in DPS-QKD systems, in order to achieve a quantum bit error rate of less than 0.5% due to linewidth broadening of the light source.

2. DPS-QKD protocol

First, we briefly mention the DPS-QKD protocol [2,3], whose typical setup is shown in Fig. 1. A transmitter (Alice) creates a coherent pulse train by a coherent light source and an intensity modulator, which is phase-modulated for each pulse with {0, π}, attenuated to be less than one (e. g., 0.2) photon per pulse on average, and then sent to a receiver (Bob). Bob receives it with an asymmetric Mach–Zehnder interferometer whose delay time equals to the pulse interval τ and path phase difference is 0. Adjacent pulses interfere with each other through the interferometer, and photons are counted occasionally and randomly in time by photon detectors at the interferometer's outputs, according to the phase difference of the pulses. After the photon transmission, Bob tells Alice his photon detection time. With this time information and her phase modulation data, Alice knows which detector counts photons in Bob. Then, Alice and Bob create identical bits from Bob's detection events, which can be a secret key. A feature of this protocol is that it does not have a basis selection procedure as in other QKD protocols, which leads to simplicity for practical implementation. Robustness against photon number splitting attacks even it uses attenuated coherent light is also an advantage to other QKD protocols [7].

The security of secret keys in the DPS-QKD is guaranteed by the fact that an eavesdropper cannot fully obtain the phase information of coherent pulses with a small photon number. Though the unconditional security analysis has not been completed, the system performance considering several types of eavesdropping, such as beam splitting attacks, intercept and resend attacks (including sequential attacks), and general individual attacks, have been studied [8–10]. These studies show that the transmission distance comparable to

[*] Corresponding author. Tel.: +81 6 6879 7732; fax: +81 6 6879 7735.
E-mail address: kyo@comm.eng.osaka-u.ac.jp (K. Inoue).

0030-4018/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2011.08.056

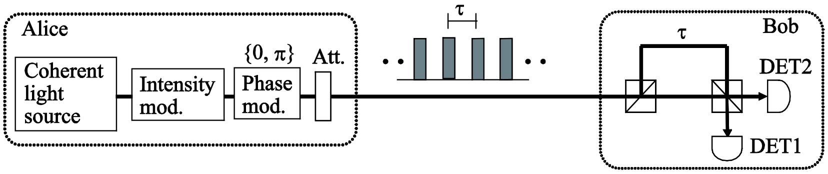

Fig. 1. Configuration of DPS-QKD. Att: optical attenuator, and DET: photon detector.

other QKD protocols is achievable, with a mean photon number of, for example, around 0.2 photon per pulse against the general individual attack.

In the above DPS-QKD protocol, key bits are created from interference between adjacent pulses. Thus, the phase differences between pulses should be assigned values, i. e., 0 and π, for correct operation. For this requirement to be satisfied, the phase of the coherent light source should be stable at least within the pulse interval. When the light phase fluctuates, bit errors occur.

3. Spectral linewidth and quantum bit error rate (QBER)

The phase stability of coherent light is characterized by the spectral linewidth. Thus, influence of the phase fluctuation on DPS-QKD systems can be discussed in terms of the spectral linewidth, which is presented in this section.

An asymmetric Mach–Zehnder interferometer is regarded as an optical filter having sinusoidal transmittance as a function of frequency, as illustrated in Fig. 2. When CW light with its carrier frequency exactly, for example, at a bottom of the transmittance passes through the interferometer, photons always go to either one of the two detectors, e. g., DET2 [Fig. 2(a)]. However, the phase fluctuation broadens the frequency spectrum, and components of the spectrum tails leak to the other detector, DET1. On the other hand, when lightwave of the same carrier frequency whose phase is alternatively modulated by 0 and π at a modulation rate equal to the free spectral range of the interferometer is input to the interferometer, its spectrum has modulation sidebands at peak frequencies of the transmittance with no carrier frequency component, and photons always go to DET1, as illustrated in Fig. 2(b). However, spectral broadening due to phase fluctuation can cause photon counts at DET2, similar to the cw case.

In terms of DPS signal, the cw light corresponds to signal of consecutive "0" bits, and the 0–π modulated light corresponds to signal of consecutive "1" bits. A DPS signal of random bits is regarded as a mixture of these two extreme signals, whose spectrum is spread due to random modulation. Note that this spectrum broadened from the signal modulation is filtered via the interferometer in the frequency domain and, as a result, the phase-modulated signal is converted to the intensity-modulated signal in the time domain. This consideration concludes that the signal modulation induced spectral broadening causes no bit errors, but additional spectral broadening due to the phase fluctuation induces bit errors.

The above discussion indicates that the bit error rate can be evaluated by considering the ratio of spectral components leaked to a wrong detector for cw light, which is illustrated in Fig. 3. The leaking ratio R is evaluated by

$$R = \int_{-\infty}^{\infty} T(\delta f)F(\delta f)d(\delta f) \tag{1}$$

with

$$T(\delta f) = \sin^2\left(\pi\frac{\delta f}{f_{\mathrm{FSR}}}\right)$$

and

$$F(\delta f) = \frac{\Delta f}{2\pi}\frac{1}{(\delta f)^2 + (\Delta f/2)^2},$$

where δf: frequency deviation from the center frequency, $T(\delta f)$: the transmittance of a Mach–Zehnder interferometer, f_{FSR}: the free-spectral-range (FSR) of the interferometer determined by the path length difference, $F(\delta f)$: the spectral density of the input light, Δf: the spectral linewidth (full width of half maximum), the center frequency of the input light is at the bottom of the transmittance, and the spectrum shape is assumed to be Lorentzian. Note that the above leaking ratio is the ratio of the leaked power to the total power, since the spectral density $F(\delta f)$ is normalized so that its integral over the whole frequency is unity.

The above discussion is based on a classical model of lightwave. In case of a photon, the spectral line shape is equivalent to the photon probability distribution in the frequency domain. A detector clicks according to this photon probability. Note here that, when a photon is counted, Bob has no way to judge whether that count comes from the leaked probability or from the desired signal

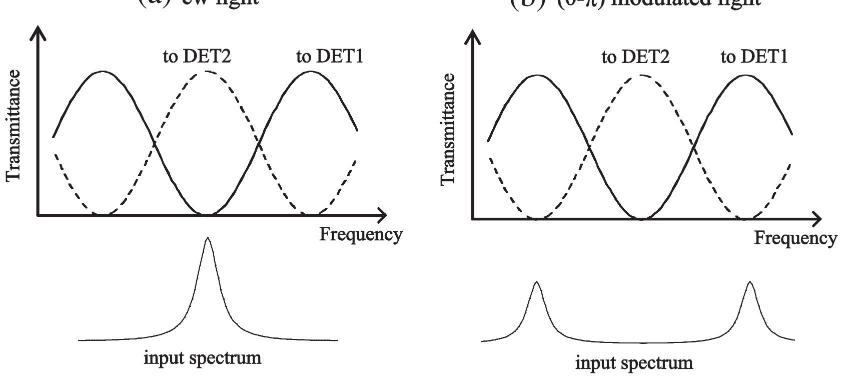

Fig. 2. Transmittance of asymmetric Mach–Zehnder interferometer.