Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization

Cailang Xie [a], Ying Guo [a], Qin Liao [a], Wei Zhao [a], Duan Huang [a], Ling Zhang [a,*], Guihua Zeng [b]

[a] School of Information Science and Engineering, Central South University, Changsha 410083, China
[b] State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China

UNCORRECTED PROOF

ARTICLE INFO

Article history:
Received 30 October 2017
Received in revised form 22 December 2017
Accepted 4 January 2018
Available online xxxx
Communicated by A. Eisfeld

Keywords:
CV-QKD
Security analysis
Clock synchronization
Jitter

ABSTRACT

How to narrow the gap of security between theory and practice has been a notoriously urgent problem in quantum cryptography. Here, we analyze and provide experimental evidence of the clock jitter effect on the practical continuous-variable quantum key distribution (CV-QKD) system. The clock jitter is a random noise which exists permanently in the clock synchronization in the practical CV-QKD system, it may compromise the system security because of its impact on data sampling and parameters estimation. In particular, the practical security of CV-QKD with different clock jitter against collective attack is analyzed theoretically based on different repetition frequencies, the numerical simulations indicate that the clock jitter has more impact on a high-speed scenario. Furthermore, a simplified experiment is designed to investigate the influence of the clock jitter.

© 2018 Published by Elsevier B.V.

1. Introduction

Quantum key distribution (QKD) allows two distant parties, the sender Alice and the receiver Bob, to establish a coincident secret key through an untrusted channel [1–3]. Unfortunately, there still exist a big gap between the theory and practice of QKD [4–6]. Indeed, many attacks which exploit security loopholes in practical realizations have been presented, such as the time-shift attack [7], faked states attacks [8,9], Trojan-horse attacks [10], phase-remapping attacks [11] for discrete-variable QKD systems, and the local oscillator attacks [12,13], saturation attacks [14], state-discrimination attack [15] for continuous-variable (CV) QKD systems. These afore-mentioned loopholes usually come from the imperfect devices or transmission channels, which can be exploited by Eve to break the unconditional security of quantum communication proved in theoretical security proofs.

Specifically, there is a vulnerability exists permanently in practical CV-QKD system comes from the clock synchronization, namely clock jitter, has not been investigated throughly at present. The clock synchronization is of significant importance in a practical CV-QKD system, as it can provide a common clock source for generating modulated signals and collecting transmitted signals [16,17]. In a general practical CV-QKD system, the signal light and local oscillator (LO) are generated by the same laser and then modulated simultaneously to pulses using a modulator. Therefore, the LO and the signals have the identical frequency, which allows Bob to extract the synchronous clock from the LO [18–20]. However, the LO is notoriously vulnerable to attacks due to its classical features [21]. Indeed, by exploiting the loopholes of the LO, several attacks have been successfully launched against practical CV-QKD systems, such as the calibration attack [13], LO fluctuation attack [22] and wavelength attack [23,24]. Fortunately, all this attacks can be defeated by using an extra homodyne detector to monitor the real-time shot noise, monitoring the power of LO and adding wavelength filters before Bob's detector, respectively. In contrast to the previous loopholes, the clock jitter is a random noise which exist permanently in clock signals due to the imperfect time base and phase locked logic [25–27]. Thus it can not be removed by a simple monitoring.

In order to fix the vulnerability of the clock synchronization, we analyze the clock jitter effect on the practical CV-QKD system. In our scheme, the clock jitter exists in the clock synchronization signals which transmit from Alice to Bob through LO, thus affecting the preciseness of signals acquisition at Bob side. This clock jitter effect may leave security loopholes for Eve to attack the system. As we will show in this paper, the clock jitter effect on CV-QKD is characterized and the system security against collective attack is analyzed theoretically. In the aspect of experiment, a low com-

[*] Corresponding author.
E-mail address: lingzhang2017@foxmail.com (L. Zhang).

https://doi.org/10.1016/j.physleta.2018.01.006
0375-9601/© 2018 Published by Elsevier B.V.

Please cite this article in press as: C. Xie et al., Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization, Phys. Lett. A (2018), https://doi.org/10.1016/j.physleta.2018.01.006

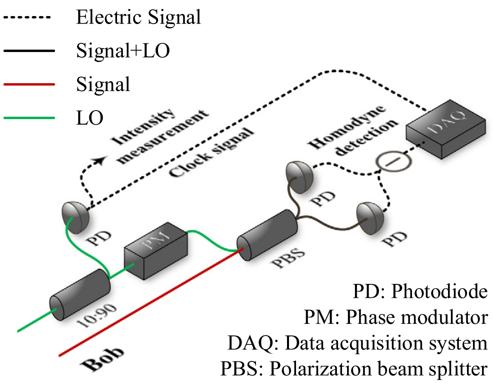

Fig. 1. (Color online.) The practical homodyne detection scheme in the CV-QKD system.

plexity setup is designed to demonstrate the influence of the clock jitter. Both the simulation and experimental results indicate that the system performance is reduced by manipulating the clock jitter. Moreover, we find that the jitter effect bring more negative influence in the CV-QKD system with a high repetition frequency. Therefore, with the rapid growth in the field of the high-speed CV-QKD [28–31], the clock jitter will be increasingly important for the practical CV-QKD systems.

This paper is organized as follows: In Sec. 2, we characterize the clock jitter effect on the detection in the practical CV-QKD system. Subsequently the system security with different clock jitter is analyzed in Sec. 3. Moreover, the low complexity experiment is given in Sec. 4. Finally, the conclusion is drawn in Sec. 5.

2. The clock jitter effect on practical CV-QKD system

In a general CV-QKD protocol, Alice usually encode information in the quadratures of the light field with Gaussian modulation. The modulated quantum states are subsequently transmitted to Bob over a lossy channel which is characterized by transmittance and excess noise. After receiving the states, Bob perform homodyne (or heterodyne) detection to measure randomly one of the quadrature (or both quadratures). A fraction of the measurements are applied to estimate the channel parameters, and the remaining measurements are used for key generation. Eventually, Alice and Bob extract a string of the secret key using information reconciliation and privacy amplification.

According to the key establishment procedure of the CV-QKD system, both the parameter estimation and key establishment depend on the measurements of the receiver's detector [32,33]. In order to collect the signal light accurately, Bob need to sample each pulse and integrate them together if the pulse period is longer than the photodiode response time [30]. This approach involves the data acquisition system with a high sampling rate, which results in more challenges for data processing. To avoid such a complex situation, an alternative method is proposed with an assumption that the optical pulse period is much short than the photodiode response time. In this case, the quadrature of the signal field is linearly proportional to the peak value of the balanced homodyne detector [34]. Therefore, it is deterministic whether or not Bob would sampling the accurate peak values. As shown in Fig. 1, the sampling clock of the data acquisition (DAQ) system is extracted from the LO using a beam splitter. It is one of the important factors to determine the accuracy of the pulse peak value.

As known, there are two types of noises that reduce the accuracy of the DAQ system, i.e., the quantization noise and the clock jitter [35]. The former can be directly calculated as $N_q = (\mathrm{LSB})^2/12$, where the LSB stands for the least significant byte of the DAQ system. With the factor that the value of N_q is usually negligible for a high-precision system and it can not be controlled by Eve, we only confine our discussion to the clock jitter. The sampling process of the electric signal with clock jitter in the DAQ system is illustrated in Fig. 2 (see also Table 1). Here we assume the output signal of balanced homodyne detector to Gaussian shape [36]. Due to the presence of clock jitter Δt_j, the kth sample will not be taken exactly at time kT_s, but at $kT_s + \Delta t_j$. Thus the jitter noise Δv reads

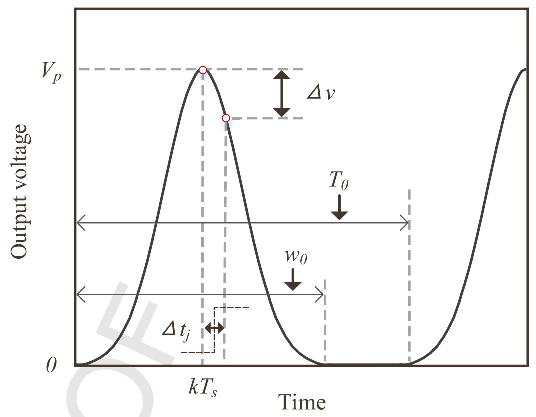

Fig. 2. (Color online.) The sampling noise of the signals acquisition due to the clock jitter.

Table 1
The parameter definitions in Fig. 2.

Parameter	Description
T_s	Sampling period
Δt_j	Clock jitter
V_p	Peak value
Δv	Jitter noise
T_0	Pulse period
w_0	Pulse width

$$\Delta v = s(kT_s) - s(kT_s + \Delta t_j), \tag{1}$$

where $s(t)$ corresponds to the input signal that can be expressed by

$$s(t) = V_p e^{-\frac{(t-\mu)^2}{2\delta_s^2}}, \tag{2}$$

where V_p is the pulse peak, μ and δ_s^2 denote the mean and variance of the Gaussian pulse, respectively.

In order to derive the mean value and the variance of the input signal, the repetition rate f_{rep} and the duty cycle R_{duty} of pulse have to be determined. These two parameters are related by $R_{\mathrm{duty}} = w_0/T_0$, where w_0 is the pulse width and T_0 is the pulse period. As $T_0 = 1/f_{\mathrm{rep}}$, the relationship can be rewritten as $w_0 = R_{\mathrm{duty}}/f_{\mathrm{rep}}$. In a practical CV-QKD system, the parameters f_{rep} and R_{duty} are given, and hence we can assume the mean value and variance of the input signal to $\mu = w_0/2$ and $\delta_s = w_0/8$, respectively. For a general sampling process, the synchronous clock is usually multiplied at the DAQ circuit to restore the signal pulses as authentic as possible. Therefore, the sampling frequency can be expressed as $f_{\mathrm{samp}} = M f_{\mathrm{rep}}$, where M is the multiple. After substituting the above equations, we obtain

$$T_s = \frac{1}{M R_{\mathrm{duty}}} w_0. \tag{3}$$

For the sampling the peak value of pulse at $\mu = w_0/2$.

For example, with the assumption that the parameters $R_{\mathrm{duty}} = 50\%$ and $M = 16$, the resulting jitter noise can be derived as

UNCORRECTED PROOF

Please cite this article in press as: C. Xie et al., Practical security analysis of continuous-variable quantum key distribution with jitter in clock synchronization, Phys. Lett. A (2018), https://doi.org/10.1016/j.physleta.2018.01.006

Download English Version:

https://daneshyari.com/en/article/8203746

Download Persian Version:

https://daneshyari.com/article/8203746

Daneshyari.com