ARTICLE IN PRESS

[Physics Letters A](https://doi.org/10.1016/j.physleta.2018.01.006) ••• (••••) •••-•••

Contents lists available at [ScienceDirect](http://www.ScienceDirect.com/) 1 67

\mathbb{P}^n and \mathbb{P}^n are \mathbb{P}^n

www.elsevier.com/locate/pla

11 Departical socurity applying of continuous variable quantum low $\frac{11}{12}$ Practical security analysis of continuous-variable quantum key $\frac{77}{78}$ ¹³ distribution with jitter in clock synchronization **179** and 179 14

 15 Cilliang Via d, Ving Cua d, Oin Line d, Wei Zhand, Duan Huang d, Iing Zhang d,* ¹⁵ Cailang Xie^a, Ying Guo^a, Qin Liao^a, Wei Zhao^a, Duan Huang^a, Ling Zhang^{a,∗}, Theory of the ⁸¹ $\frac{17}{17}$ sunda $\frac{1}{2}$ Guihua Zeng b

18 84 ^a *School of Information Science and Engineering, Central South University, Changsha 410083, China*

¹⁹ State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Information Sensing and Processing, method and Processing, 20 86 *Shanghai Jiao Tong University, Shanghai 200240, China*

23 ARTICLE INFO ABSTRACT 89

24 90 *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:*

 34 and 100 CV-QKD Security analysis Clock synchronization Jitter

25 Article history:
25 Article history: **Example 2017 How to narrow the gap of security between theory and practice has been a notoriously urgent problem in** ²⁶ Received in revised form 22 December 2017 the practical continuous-variable quantum key distribution (CV-QKD) system. The clock jitter is a random $\frac{92}{100}$ 27 Accepted 4 January 2018
noise which exists permanently in the clock synchronization in the practical CV-QKD system, it may 28 Available online xxxx
Communicated by A. Fisfald **Sample of the system security because** of its impact on data sampling and parameters estimation. In 29 Communicated by A. Eistend **Exercice 2018** particular, the practical security of CV-QKD with different clock jitter against collective attack is analyzed ⁹⁵ ³⁰ *Keywords*: **Example 20 EXECUTE:** Theoretically based on different repetition frequencies, the numerical simulations indicate that the clock ⁹⁶ ³¹ CV-QKD **1978** 10 31 31 ST Separation and ST Serian CO 37 31 ST Serian Structure Terminent is designed to ⁹⁷ 32 Security analysis **1988 investigate the influence of the clock jitter.** The security analysis **1988 98** quantum cryptography. Here, we analyze and provide experimental evidence of the clock jitter effect on

33 Clock synchronization **Server B.V.** 99

1. Introduction

 $_{40}$ Quantum key distribution (QKD) allows two distant parties, the lated simultaneously to pulses using a modulator. Therefore, the $_{106}$ 41 sender Alice and the receiver Bob, to establish a coincident se- ± 10 and the signals have the identical frequency, which allows Bob $_{107}$ 42 cret key through an untrusted channel [\[1–3\].](#page--1-0) Unfortunately, there $\;$ to extract the synchronous clock from the LO [18–20]. However, $\;$ ₁₀₈ 43 still exist a big gap between the theory and practice of QKD the LO is notoriously vulnerable to attacks due to its classical fea- $_{109}$ 44 $[4-6]$. Indeed, many attacks which exploit security loopholes in tures [21]. Indeed, by exploiting the loopholes of the LO, several 1_{10} 45 111 practical realizations have been presented, such as the time-shift 46 attack [\[7\],](#page--1-0) faked states attacks [\[8,9\],](#page--1-0) Trojan-horse attacks [\[10\],](#page--1-0) systems, such as the calibration attack [13], LO fluctuation attack 112 47 phase-remapping attacks [\[11\]](#page--1-0) for discrete-variable QKD systems, $\lfloor 22 \rfloor$ and wavelength attack [23,24]. Fortunately, all this attacks can $\lfloor 13 \rfloor$ 48 and the local oscillator attacks $[12,13]$, saturation attacks $[14]$, be defeated by using an extra homodyne defector to monitor the 144 49 state-discrimination attack [\[15\]](#page--1-0) for continuous-variable (CV) QKD real-time shot noise, monitoring the power of LO and adding wave- 115 50 systems. These afore-mentioned loopholes usually come from the hength filters before Bob's detector, respectively. In contrast to the hig 51 imperfect devices or transmission channels, which can be exploited previous loopholes, the clock jitter is a random holse which exist 117 52 by Eve to break the unconditional security of quantum communi- permanently in clock signals due to the imperfect time base and the 53 cation proved in theoretical security proofs. The same sphase locked logic [\[25–27\].](#page--1-0) Thus it can not be removed by a simcation proved in theoretical security proofs.

54 120 Specifically, there is a vulnerability exists permanently in practi-

* Corresponding author.

E-mail address: lingzhang2017@foxmail.com (L. Zhang).

64 130 <https://doi.org/10.1016/j.physleta.2018.01.006>

 65 0375-9601/© 2018 Published by Elsevier B.V. 131

66 and the contract of the con

 $_{38}$ **1. Introduction** $_{104}$ \sim 39 105 105 105 11 20 lated 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 [\[21\].](#page--1-0) Indeed, by exploiting the loopholes of the LO, several attacks have been successfully launched against practical CV-QKD systems, such as the calibration attack [\[13\],](#page--1-0) LO fluctuation attack [\[22\]](#page--1-0) and wavelength attack [\[23,24\].](#page--1-0) 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 ple monitoring.

55 cal CV-QKD system comes from the clock synchronization, namely the order to fix the vulnerability of the clock synchronization, we the 56 clock jitter, has not been investigated throughly at present. The analyze the clock jitter effect on the practical CV-QKD system. In 122 57 clock synchronization is of significant importance in a practical CV- our scheme, the clock jitter exists in the clock synchronization sig- 123 58 124 QKD system, as it can provide a common clock source for gener-59 ating modulated signals and collecting transmitted signals $[16,17]$. The preciseness or signals acquisition at Bob side. This clock jitter $\frac{125}{25}$ 60 126 effect may leave security loopholes for Eve to attack the system. 61 **61** 127 **127 As we will show in this paper, the clock jitter effect on CV-QKD 127** 62 128 is characterized and the system security against collective attack 63 63 63 E-mail address: lingzhang2017@foxmail.com (L. Zhang). The street street is analyzed theoretically. In the aspect of experiment, a low com-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

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

2 *C. Xie et al. / Physics Letters A* ••• *(*••••*)* •••*–*•••

15 81 **Fig. 1.** (Color online.) The practical homodyne detection scheme in the CV-QKD sys-16 tem. 282 and 282 an tem.

 18 plexity setup is designed to demonstrate the influence of the clock 10^{10} 19 fitter. Both the simulation and experimental results indicate that the state of the state 20 the system performance is reduced by manipulating the clock jit-
20 **Examples are also assumed as a set of the system of** $_{21}$ ter. Moreover, we find that the jitter effect bring more negative $\frac{1}{2}$ and $\frac{1}{2}$ 22 influence in the CV-QKD system with a high repetition frequency. The exameter contract the exercision of the securition of the se 23 Therefore, with the rapid growth in the field of the high-speed CV- T_s and T_s an 24 QKD [\[28–31\],](#page--1-0) the clock jitter will be increasingly important for the $\frac{\Delta t_j}{\Delta t}$ and $\frac{\Delta t_j}{\Delta t}$ contribution of the set 25 91 practical CV-QKD systems.

26 This paper is organized as follows: In Sec. 2, we characterize T_0 and T_0 and T_0 and T_1 pulse period to the second to the s 27 the clock jitter effect on the detection in the practical CV-QKD sys- w_0 and w_0 and w_0 are not the proportion of w_0 28 94 tem. Subsequently the system security with different clock jitter 29 is analyzed in Sec. [3.](#page--1-0) Moreover, the low complexity experiment is the precision gustave and it are not be controlled by Fig. 110 95 30 given in Sec. [4.](#page--1-0) Finally, the conclusion is drawn in Sec. [5.](#page--1-0)

 $_{34}$ In a general CV-QKD protocol, Alice usually encode information but signal of balanced nomodyne detector to Gaussian shape [36]. 100 $_{35}$ in the quadratures of the light field with Gaussian modulation. Due to the presence of clock jitter Δt_j , the kth sample will not be $_{101}$ $_{36}$ The modulated quantum states are subsequently transmitted to taken exactly at time kT_s, but at kT_s + Δt_j . Thus the jitter noise ₁₀₂ $_{37}$ Bob over a lossy channel which is characterized by transmittance Δv reads Δv reads 38 104 and excess noise. After receiving the states, Bob perform homo-39 dyne (or heterodyne) detection to measure randomly one of the $\Delta V = S(K1_S) - S(K1_S + \Delta t_j)$, 40 quadrature (or both quadratures). A fraction of the measurements where $s(t)$ corresponds to the input signal that can be expressed 106 $_{41}$ are applied to estimate the channel parameters, and the remaining $_{\text{bv}}$ and the remaining to the channel parameters, and the remaining to the channel state of the channel state of the channel state of the channe $_{42}$ measurements are used for key generation. Eventually, Alice and $_{2}$ 43 Bob extract a string of the secret key using information reconcilia-
43 Bob extract a string of the secret key using information reconcilia-44 tion and privacy amplification. $S(t) = V_p e^{-2\omega_s}$, $\tag{2}$ 110 quadrature (or both quadratures). A fraction of the measurements

45 According to the key establishment procedure of the CV-QKD where V_p is the pulse peak, *μ* and $δ_s²$ denote the mean and vari-
austem heth the parameter estimation and leve establishment de 46 system, both the parameter estimation and key establishment de-
112 47 pend on the measurements of the receiver s detector $[32,33]$. In order to derive the mean value and the variance of the in-48 der to collect the signal light accurately, bob heed to sample each put signal, the repetition rate f_{rep} and the duty cycle R_{duty} of $\frac{114}{\text{d}t}$ $_{49}$ pulse and integrate them together if the pulse period is longer than $_{20}^{115}$ and 50 the photodiode response time [\[30\].](#page--1-0) This approach involves the $\frac{100 \text{ N}}{1 \text{ N}}$ is the subsequently in the 116 51 data acquisition system with a high sampling rate, which results $\frac{99}{21}$ Maury $\frac{1}{2}$ and $\frac{1}{2$ 52 in more challenges for data processing. To avoid such a complex $\frac{1}{2}$ in $\frac{1}{2}$ is $\frac{1}{2}$ in $\frac{1}{2}$ is $\frac{1}{2}$ $_{53}$ situation, an alternative method is proposed with an assumption $W0 = R_{\text{duty}}/J_{\text{rep}}$. In a practical CV-QKD system, the parameters J_{rep} $_{119}$ 54 that the optical pulse period is much short than the photodiode and R_{duty} are given, and nence we can assume the mean value 120 $_{55}$ response time. In this case, the quadrature of the signal field is and variance of the input signal to $\mu = w_0/2$ and $\delta_s = w_0/8$, re- $_{56}$ linearly proportional to the peak value of the balanced homodyne spectively. For a general sampling process, the synchronous clock $\frac{122}{122}$ $_{57}$ detector [\[34\].](#page--1-0) Therefore, it is deterministic whether or not Bob is usually multiplied at the DAQ circuit to restore the signal pulses $_{123}$ ₅₈ would sampling the accurate peak values. As shown in Fig. 1, the as authentic as possible. Therefore, the sampling frequency can be $_{124}$ $_{59}$ sampling clock of the data acquisition (DAQ) system is extracted expressed as $f_{\rm samp}$ = $M_{\rm rep}$, where M is the multiple. After substi- $_{60}$ from the LO using a beam splitter. It is one of the important fac-
 $_{126}$ turing the above equations, we obtain 61 tors to determine the accuracy of the pulse peak value. 127 127 According to the key establishment procedure of the CV-QKD pend on the measurements of the receiver's detector [\[32,33\].](#page--1-0) In order to collect the signal light accurately, Bob need to sample each sampling clock of the data acquisition (DAQ) system is extracted

62 As known, there are two types of noises that reduce the accu- $T_s = \frac{1}{\sqrt{2\pi}} W_0$. (3) 128 63 1 racy of the DAQ system, i.e., the quantization noise and the clock the state of the duty of the DAQ system, i.e., the quantization noise and the clock 64 jitter [\[35\].](#page--1-0) The former can be directly calculated as $N_q = (LSB)^2/12$, For the sampling the peak value of pulse at $\mu = w_0/2$. ⁶⁵ where the LSB stands for the least significant byte of the DAQ sys-
For example, with the assumption that the parameters $R_{\text{duty}} = 131$ 66 tem. With the factor that the value of N_q is usually negligible for 50% and $M=16$, the resulting jitter noise can be derived as 132

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

31
20 **2 The clock jitter effect on practical CV-OKD system**
20 **2 The clock** jitter in the DAQ system is $\frac{97}{100}$ 32 98 **2. The clock jitter effect on practical CV-QKD system** $\frac{1}{33}$ 33 and $\frac{1}{39}$ illustrated in Fig. 2 (see also Table 1). Here we assume the outa high-precision system and it can not be controlled by Eve, we only confine our discussion to the clock jitter. The sampling pro-put signal of balanced homodyne detector to Gaussian shape [\[36\].](#page--1-0) 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 *-v* reads

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

by

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

ance of the Gaussian pulse, respectively.

pulse have to be determined. These two parameters are related by $R_{\text{duty}} = w_0/T_0$, where w_0 is the pulse width and T_0 is the pulse period. As $T_0 = 1/f_{\text{rep}}$, the relationship can be rewritten as $w_0 = R_{\text{duty}}/f_{\text{rep}}$. 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 tuting the above equations, we obtain

$$
T_s = \frac{1}{MR_{\text{duty}}} w_0. \tag{3}
$$

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

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

Download English Version:

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

Download Persian Version:

<https://daneshyari.com/article/8203746>

[Daneshyari.com](https://daneshyari.com)