


Article

Robust Frame Synchronization Scheme for Continuous-Variable Quantum Key Distribution with Simple Process

Rui Chen ¹, Peng Huang ^{1,*} , Dengwen Li ¹, Yiqun Zhu ² and Guihua Zeng ¹

¹ State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiaotong University, Shanghai 200240, China; 118034910040@sjtu.edu.cn (R.C.); dengwen_li@sjtu.edu.cn (D.L.); ghzeng@sjtu.edu.cn (G.Z.)

² School of Electronic Information, Shanghai Dianji University, Shanghai 201306, China; zhuyiq@sdju.edu.cn

* Correspondence: huang.peng@sjtu.edu.cn; Tel.: +86-021-3420-4361

Received: 12 November 2019; Accepted: 22 November 2019; Published: 23 November 2019



Abstract: In continuous-variable quantum key distribution (CVQKD) systems, high-quality data synchronization between two legitimate parties, Alice and Bob, is the premise of the generation of shared secret keys. Synchronization with specially designed frames is an efficient way, but it requires special modulating devices to generate these special frames. Moreover, the extra requirement of special modulating devices makes it technically impossible for some passive preparation schemes. We propose a novel approach to realize synchronization in this paper, which is different from those special-frame-based methods. In our proposed scheme, Alice publishes parts of the original signals as the synchronization frames and Bob takes these frames to perform the synchronization algorithm. Besides, a synchronization feature is applied to deal with phase shifts. The simulation results based on practical data demonstrate that the proposed synchronization scheme not only maintains a high success rate but simplifies the data processing flow at the same time, which dramatically reduces the computational complexity.

Keywords: continuous-variable quantum key distribution; frame synchronization; phase shifts

1. Introduction

Quantum key distribution (QKD) has become a popular topic for its confidentiality, which allows two legitimate parties far away to share secure secret keys through an untrusted channel with unconditional security [1–3]. Generally speaking, dominated protocols of QKD can be divided into two categories, which can be defined as discrete-variable QKD (DVQKD) [4,5] and continuous-variable QKD (CVQKD) [2,6,7]. In the DVQKD scheme, secret keys would be encoded on polarization states, phases, or other discrete variables of single photons. In the CVQKD system, information is encoded on the position and momentum quadrature of the light field. Then the receiver, Bob, uses homodyne detectors or heterodyne detectors to measure one or both quadrature components. By controlling excess noise, the CVQKD system can be achieved beyond 100 km at present through standard single-mode optical fibers [8,9]. Moreover, the CVQKD can utilize existing optical communication components, which provides a prospect of good integration with classical optical communications.

In a typical CVQKD system, Alice first prepares quantum states. Then secret information, which is produced from the true random number generator, is encoded on the position or momentum quadrature of quantum states by amplitude and phase modulations. After that, the modulated quantum states, which can be expressed as $|x_A + ip_A\rangle$, are sent to Bob through a quantum channel. Affected by quantum noise and other classical noise, Bob will receive a noise state $|x_B + ip_B\rangle$.

Transmission of the quantum signal over a lossy and noisy channel may highly affect the performance of the frame synchronization algorithm. For homodyne detection, Bob randomly chooses X or P measurement bases. Afterward, he compares them with Alice's bases and selects the variables with the same bases. After reconciliation and privacy amplification processes, Alice and Bob will share the same key data.

It is worth noting that synchronization in CVQKD plays an important role. Simply speaking, if the data of Alice and Bob are not aligned, decoding key information in Bob's side will be independent with the one Alice prepared, which results in inconsistent secret key strings after the reconciliation process, and thus deteriorates the overall performance. In a CVQKD system, clock synchronization makes two communication entities share the same clock to acquire accurate data. So far, clock synchronization schemes include the transmitted local oscillator (TLO) [10] and local local oscillator (LLO) schemes [11,12], where the latter can thoroughly remove the related loopholes [13,14] introduced by transmitted LO signals. Frame synchronization determines the head of every signal string, so even minor synchronization errors will lead to a huge decrease in the mutual information between Alice and Bob. Most previous methods tend to use specific modulations to generate synchronization frames, and the well-organized frames are periodically inserted into the data frames by Alice [15–17]. Although these methods have been proved efficient in some situations, the performances of them are far from satisfied under low signal-to-noise ratio (SNR) scenarios. To overcome this shortcoming, a frame synchronization scheme based on phase disassembling and matching by comparing correlation was put forward [18]. However, in the synchronization procedure, computing correlation requires a lot of multiplication and the previous calculations cannot be reused in subsequent calculations. An expected frame synchronization scheme should have high-efficiency at a low SNR and low computational complexity at the same time.

Besides, in practical CVQKD applications, the quantum state will suffer unpredictable nonlinear effects, and the quadrature components of the optical field of quantum states will suffer phase shifts during signal transmissions [19,20], which means a well-designed frame synchronization scheme should be well tolerable of phase shifts. If the two legitimate entities have been successfully synchronized, the phase shifts can be removed by phase compensation methods [21,22]. So the synchronization process is usually previous to phase compensation, and frame synchronization should tolerate a certain amount of phase shifts.

To simplify the frame synchronization scheme and improve the efficiency and robustness of the CVQKD system, we propose a novel scheme here. In particular, a new feature is designed, which can tolerate phase shifts and synchronize in a strong noise environment. Each synchronization process requires only a few addition and subtraction operations and a Hamming distance comparison. In particular, we analyze the performance of this method under different phase shifts and various SNR settings. The results show that this scheme can tolerate different phase shifts and performs well at a low SNR. Moreover, the proposed scheme also keeps a good balance between performance and computational complexity.

The rest of the paper is organized as follows: In Section 2, we first introduce the synchronization process and the designed feature in detail, then illustrate the reason why this feature can tolerate different phase shifts. In Section 3, the simulations of the proposed algorithm under different parameter settings are performed. Finally, a brief conclusion is given in Section 4.

2. Synchronization in CVQKD

In the common frame synchronization scheme of CVQKD [15,16], the training frames should be added to realize data synchronization between Alice and Bob. The synchronization frames are modulated into a special format, known by Alice and Bob and can be easily recognized. However, in some special CVQKD schemes, it is difficult or even impossible to add synchronization frames into key data by modulation devices, such as the passive-state-preparation CVQKD scheme [23]. In the passive-state-preparation CVQKD scheme, Alice can split the output of a thermal source by

a beam splitter and one mode is measured by herself while the other mode is transmitted into the other legitimate entity, Bob. As Alice directly split the output of the source and did not use any modulation devices to encode information onto the mode, it is hard to add synchronization frames into the signal. This inspired us to look for ways to synchronize using random number strings. Moreover, the traditional synchronization process usually needs a high range switch of light intensity. These light switching schemes make CVQKD systems more complicated and unstable.

These issues prompted us to improve the training-frame-based scheme into a modulation-free one without specified synchronization frames. In addition, phase drifts between the LO and signal will introduce extra trouble into the synchronization process. A practical scheme should overcome the phase drifts to successfully implement synchronization. In classical optical and wireless communications, synchronization can be performed by measuring the Hamming distance between the outputs of the transmitter and the received signals [24]. The Hamming distance equals to the different bits of two 0–1 sequences S_1, S_2 . Comparing to the calculation of correlation, the Hamming distance has low computation complexity. Here, we can first convert the signals into 0-1 sequences by certain algorithms and then measure their Hamming distance. It should be mentioned that these transform algorithms must be robust against different environment noises.

2.1. Finding Robust Feature

In this part, we will mainly analyze the influence of the phase shift on the synchronization process, then introduce a robust feature. Alice sends quantum states $|X_A + iP_A\rangle$ to Bob through a quantum channel with Gaussian distributed noise ξ and phase shift $\Delta\varphi$. In fact, the noise in the channel can be divided into two parts. The one added by the channel is called channel-added noise. It can be expressed as $\chi_{line} = 1/T - 1 + \varepsilon_c$ (T is the transmittance of the quantum channel and ε_c means the excess noise). The other noise is added by the thermal motion of detectors, called detection-added noise. The detection-added noise can be expressed as $\chi_{hom} = (1 - \eta + v_{el})/\eta$ (homodyne detector) or $\chi_{het} = (1 + (1 - \eta) + 2v_{el})/\eta$ (heterodyne detector), in which η means the attenuation factor and v_{el} means the thermal noise caused by electronics in homodyne detectors or heterodyne detectors. And the total noise referred to the channel input can be given by $\chi_{tot} = \chi_{line} + \chi_{hom}/T$. From reference [25], X_A and P_A are Gaussian distributed random variables. For simplicity, here we temporarily omit the attenuation. When Bob measures the quantum states $|X_B + iP_B\rangle$ with a homodyne or a heterodyne detector, the measurement results can be expressed as

$$X_B = A \cos(\theta + \Delta\varphi) + \xi = X_A \cos(\Delta\varphi) - P_A \sin(\Delta\varphi) + \xi, \tag{1}$$

$$P_B = A \sin(\theta + \Delta\varphi) + \xi = P_A \cos(\Delta\varphi) + X_A \sin(\Delta\varphi) + \xi, \tag{2}$$

where $X_A = A \cos(\theta), P_A = A \sin(\theta)$. Without loss of generality, in the following analyses, we assume that ξ is a Gaussian distributed random variable with expectation 0 and variance σ , and the phase shift $\delta\varphi$ keeps the same within a small period time. From the above formula, we know that if we want to eliminate the effect of phase shifts in synchronization, some stable features must be found.

To cope with the phase shifts, here we introduce a new operator $\Delta X_{(AorB),n} = \sum_{i=1}^L X_{(AorB),n+i} - \sum_{i=1}^L X_{(AorB),n-i}$ ($\Delta P_{(AorB),n}$ can be defined in the same way) called incremental label. Now we investigate the effect of phase drift on it. The conditional expectation of the operator can be written as

$$\begin{aligned} E(\Delta X_{(B,n)} | \Delta X_{(A,n)} = V_{th}) &= E[\Delta X_{(A,n)} \cos \Delta\varphi - \Delta P_{(A,n)} \sin \Delta\varphi | \Delta X_{(A,n)} = V_{th}] \\ &= V \cos \Delta\varphi, \end{aligned} \tag{3}$$

where V_{th} is a positive threshold and $\Delta\varphi \in (-\pi, \pi)$ means phase shift. If $\Delta\varphi \in (-\pi/2, \pi/2)$, then the conditional expectation is positive. Otherwise, it will be a negative one. $sign(x)$ is the sign function that outputs the sign of number x . The sign of the above conditional expectation is,

$$\text{sign}[E(\Delta X_{(B,n)}|\Delta X_{(A,n)} = V_{th})] = \text{sign}(V \cos \Delta\varphi) = \text{sign}(\cos \Delta\varphi). \tag{4}$$

So when $\Delta X_{(A,n)}$ is larger than a significant positive threshold, the operator $\Delta X_{(B,n)}$ can be regarded as a quasi-stable feature. Here we can apply this operator on a string of random numbers and yield a binary sequence. We first apply it on Alice’s key string to get the binary sequence S_A , and then apply it on Bob’s one to get S_B . Suppose that the phase shift $\Delta\varphi$ keeps the same for a while; if $\cos \Delta\varphi$ is positive, the result will be $S_A = S_B$, else $S_A = -S_B$.

In the above discussion, we do not consider one case that $\Delta\varphi$ is approaching $\pm\pi/2$. In fact, when $\Delta\varphi$ is close to $\pm\pi/2$, X_B is similar to the quadrature component P_A . When this happens, another conditional expectation should be explored,

$$\text{sign}[E(\Delta X_{(B,n)}|\Delta P_{(A,n)} = V_{th})] = \text{sign}(-V \sin \Delta\varphi) = -\text{sign}(\sin \Delta\varphi). \tag{5}$$

From the above expression, we can see that if $\cos \Delta\varphi$ approximately becomes 0, taking component P into consideration is another good way. In the following section, we will show how the above conclusion can be applied to real synchronization.

The conditional expectation of the incremental label and its sign give us some ideas that the sign of $\Delta X_{(AorB),n}$ is stable in a noisy environment, and a robust 0–1 string can be constructed in this way. The relationship between the conditional expectation and phase shifts can help to deal with the phase drift problems in the synchronization process. This will be elaborated on in the following section.

2.2. Incremental Label

Based on the above analysis, the incremental label can be constructed. This labeling method will transform a random number sequence X , which can be expressed as (x_1, x_2, \dots) into a binary sequence $Y (y_1, y_2, \dots)$ by the rules:

Step 1. Sum the next L numbers of the current position, such as shown in Figure 1 X_{i+3}, X_{i+4} for current position X_{i+2} and $L = 2$. Then subtracting the sum of the former L numbers, the output is used as a descriptor. We call the $2L + 1$ interval a transformation unit.

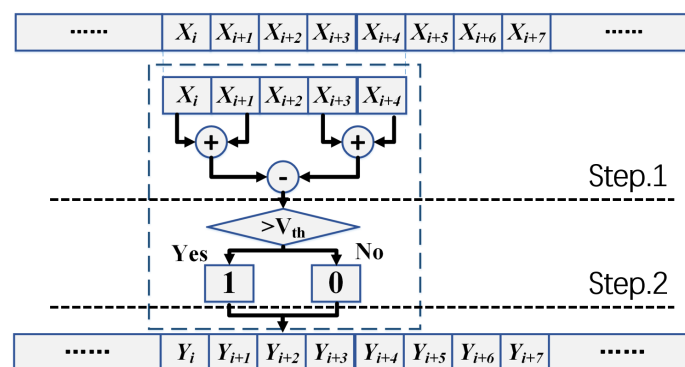


Figure 1. The proposed synchronization scheme.

Step 2. If $\sum_{j=i+1}^{i+L} x_j - \sum_{j=i-L}^{i-1} x_j > V_{th}$, we mark this position with symbol “1” ($y_i = 1$). If $\sum_{j=i+1}^{i+L} x_j - \sum_{j=i-L}^{i-1} x_j \leq V_{th}$, we mark this position with symbol “0” ($y_i = 0$).

Step 3. After all the received signals are marked, the synchronization process begins. Every successive N bits of conversion sequence Y are seen as a feature, and we can calculate the Hamming distance of the two signal sequences to measure their similarity.

It should be mentioned that noise with zero expectation will be suppressed and their impact on synchronization is weakened. This transformation method is simple and efficient, and we will show its performance in the next section and analyze computation complexity in the computational analysis section.

To compete with phase drifts, the sender Alice can prepare four transformation sequences of her synchronization frames. Firstly, Alice generates the binary sequences TX_A and TP_A by using the rules listed in steps 1 and 2. Then their complements, $\overline{TX_A}$ and $\overline{TP_A}$, can directly get a not operator. For example, if TX_A is "0101," then $\overline{TX_A}$ is "1010;" the rules are the same for TP_A and $\overline{TP_A}$. Bob also transforms the received X_B or P_B with the same rules.

After the sequence transformations, the similarity can be measured by calculating the Hamming distance between the transformed sequences of Alice's synchronization symbols and every segment of Bob's received signal. Here we want to make the cost function reach its peak value when synchronization succeeds, so the cost is rewritten

$$D(TX_A, TX_B) = n - H(TX_A, TX_B), \tag{6}$$

where $D(X_1, X_2)$ means the similarity of sequences X_1 and X_2 , and $H(X_1, X_2)$ means the Hamming distance of X_1 and X_2 . Here, we define a new function,

$$F(A, B) = \max \left[D(TX_A, TX_B), D(\overline{TX_A}, TX_B), D(TP_A, TX_B), D(\overline{TP_A}, TX_B) \right]. \tag{7}$$

The location of synchronization is where the function $F(A, B)$ reaches its peak value.

2.3. The Synchronization Flow

From the above derivations, we have now found a stable feature to endure phase drifts. The following synchronization scheme is based on this feature.

Step 1. Alice (the sender) selects parts of the random strings as the synchronization frame (see Figure 2a).

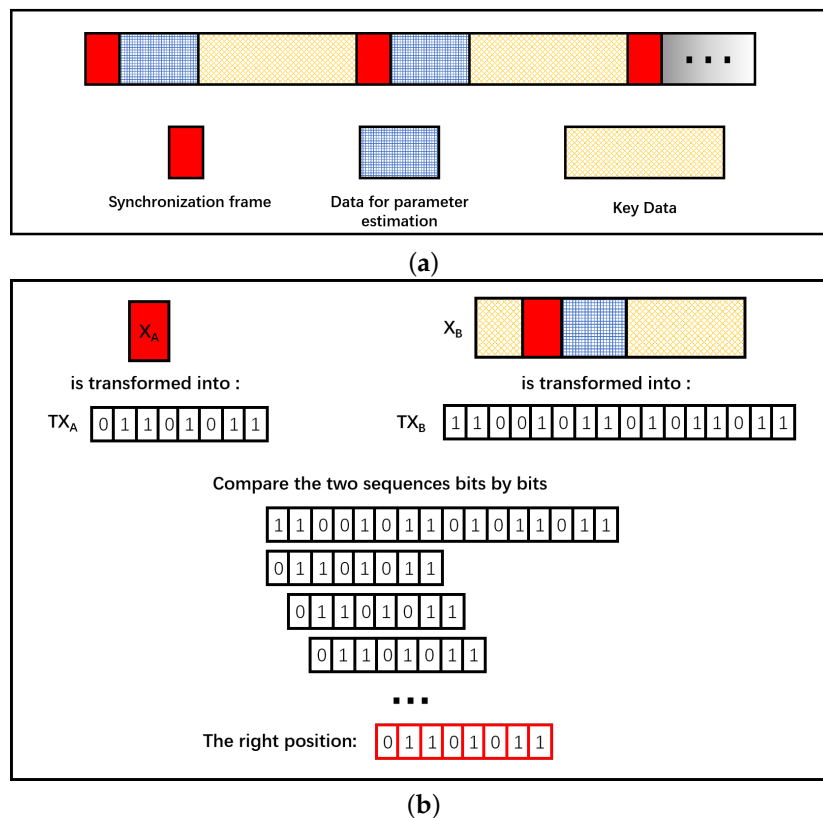


Figure 2. (a) The structure of the data frame in the continuous-variable quantum key distribution (CVQKD) system; (b) the synchronization process in the CVQKD system.

Step 2. Alice transforms the selected sequences into 0–1 sequences using the incremental label algorithm proposed above. Both X and P components must be transformed. We get two 0–1 sequences: TX_A and TP_A .

Step 3. Alice publishes the two 0–1 sequences TX_A and TP_A through the classical channel.

Step 4. Bob transforms X_B or P_B into 0–1 sequences by the incremental label algorithm, and matches them to the received two 0–1 sequences TX_A and TP_A bits by bits. Then he calculates the function $F(A, B) = \max [D(TX_A, TX_B), D(\overline{TX_A}, TX_B), D(TP_A, TX_B), D(\overline{TP_A}, TX_B)]$ (see Figure 2b).

Step 5. Alice and Bob synchronize at the position where the function $F(A, B)$ reaches its peak value.

To verify the correctness of the proposed scheme, the synchronization process is simulated as follows. The encoded random strings in Alice’s side are X_A and P_A , and Bob’s received signals are X_B and P_B . Figure 3 shows the cost function $D(TX_A, TX_B)$ and $D(TP_A, TX_B)$ under different phase shifts.

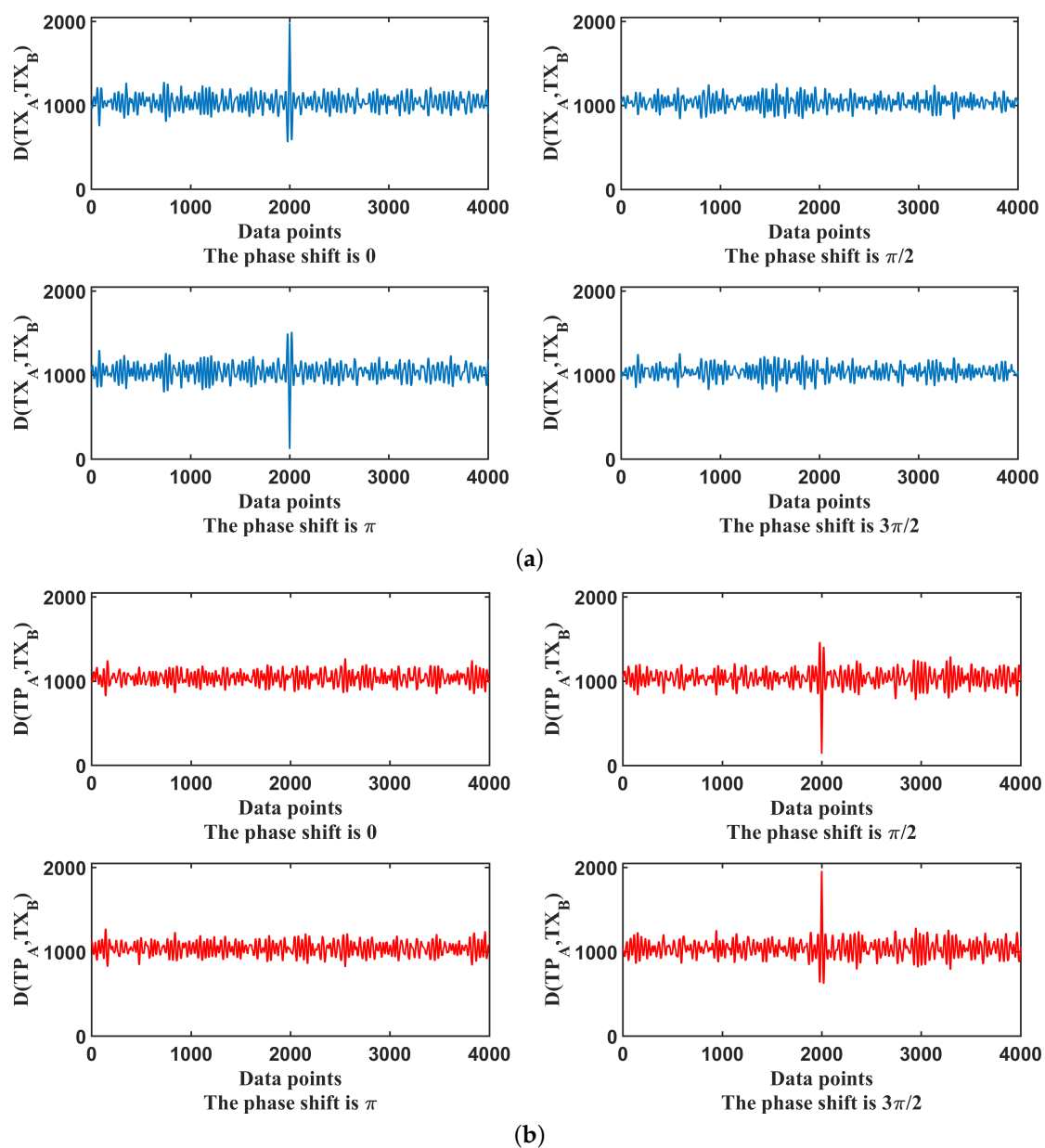


Figure 3. (a) Cost function $D(TX_A, TX_B)$ under different phase shifts; (b) Cost function $D(TP_A, TX_B)$ under different phase shifts.

The cost function $D(TX_A, TX_B)$ reaches its peak value when the synchronization succeeds if the phase shift is 0. However, the value will bottom out when the phase shift comes to π . There will be no peak or valley values when the phase shift reaches $\pi/2$ or $3\pi/2$. Similarly, the cost function $D(TP_A, TP_B)$ has a valley value corresponding to the $\pi/2$ phase shift situation while it reaches its maximum if the phase shift changes to $3\pi/2$. The results also provide further evidence on how reasonable and feasible the proposed new function is in Equation (7).

3. Performance Analysis

To explore the influence of SNR (signal-to-noise ratio) and phase shifts on the performance of the proposed frame synchronization algorithm, we prepare several strings of data with natural Gaussian distributions generated from ASE output signals with length 200,000. We add Gaussian white noise of different variance to the output signal to simulate different noise environments. Here we randomly select some segments of the signals as synchronization frames, and we define the proportion of the times of successful synchronization as the success rate. To improve the success rate, the parameter L should be longer than 10 and the threshold V_{th} could be set as the variance of the received signals.

3.1. Performance Influenced by Phase Shifts

Figure 4a,b shows that the influence of different phase shifts on the proposed algorithm. The synchronization process operates at an SNR of -13 dB with feature-lengths of $N = 512, 1024, 2048$. It can be found that increasing the feature-length can significantly improve performance. We can find the success rate will bottom out for the phase shifts $\Delta\varphi = 45^\circ, 135^\circ, 225^\circ, 315^\circ$, and the success rate seems to be unsatisfactory. This is because when phase shifts take these values, $\cos(\Delta\varphi) = \sin(\Delta\varphi)$, the proposed algorithm merely deals with one quadrature X or P . If Bob applies a heterodyne detector to measure X_B and P_B simultaneously, these two values can both be used to perform synchronization and, thus, better results can be achieved. The above analyses show that although the proposed scheme is more suitable for protocols based on heterodyne detection, it can also be applied to homodyne-based protocols. Using a heterodyne detector to measure X_B and P_B simultaneously in the final matching step will get a better result. Merely considering one quadrature X or P can also synchronize well when the phase shifts occur.

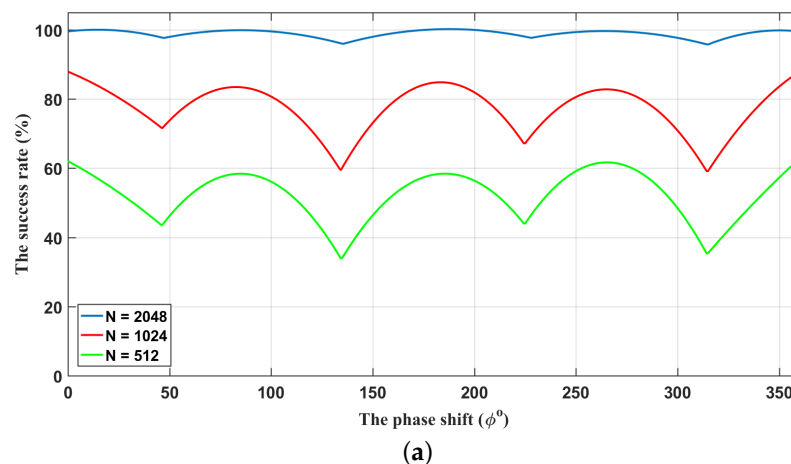


Figure 4. Cont.

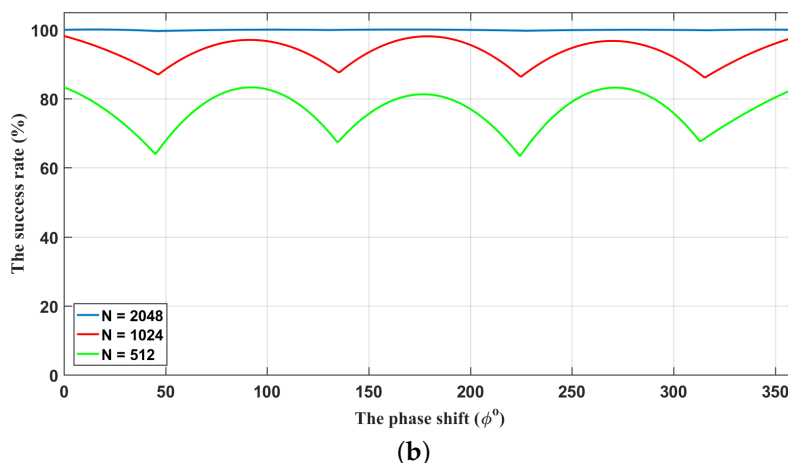


Figure 4. The relationship between the phase shifts and the success rate of synchronization. (a) Synchronization by using only one quadrature component; (b) Synchronization by using two quadrature components. The lengths of synchronization frames from bottom to top are $N = 512, 1024, 2048$. The SNR is -13 dB.

3.2. Synchronization with Different SNRs

In Figure 5a–d, we explore the performance of the proposed synchronization algorithm under different SNR conditions with phase shifts $\Delta\phi = 0^\circ, 45^\circ, 90^\circ, 135^\circ$, respectively. We find that the decrease in success rate caused by the low SNR can be effectively improved by increasing the length of features. From the above discussions, we know that the phase shifts $\Delta\phi = 45^\circ, 135^\circ$ are two points that the success rate reaches its minimum value, which is also demonstrated in these figures. When setting the feature-length as $N = 2048$, despite the phase shifts, the success rate will be higher than 90% when SNR is larger than -20 dB. Usually, the data block of a CVQKD system with a repetition rate of 100 MHz has 100,000 characters. If we set the feature-length N to maximal 2048, the fraction, which is used for synchronization, is 2.048%. Our synchronization scheme requires only a small sacrifice of data.

3.3. Algorithm Complexity

Complexity is another important factor for a practical synchronization algorithm. In a practical CVQKD system, the synchronization algorithm should work in real-time for high efficiency, otherwise, it will require a mass of storage to store all the received data. At first sight, according to the algorithm flow, every step has $2NL$ times added to operations (the transformation unit length L is mentioned above, usually it can be set as $L = 13$), N times of subtraction operation and an N -bit Hamming distance operation. This is because data reuse is not considered. In a practical synchronization, every synchronization step needs only $2L$ times add operations except for the first step, 1 time subtraction operation, and an N -bit Hamming distance operation. The previously stored transform results can be used. It should be noted that the expression $\sum_{j=i+1}^{i+L} x_j - \sum_{j=i-L}^{i-1} x_j \leq V_{th}$ (center on X_i) just needs to be calculated one time for every step and a unique binary mark will be allocated to the corresponding location Y_i . There is no need to calculate it again when generating the next feature. The analysis shows that the proposed scheme can save computation resources and maintain good performance.

Comparing to the frame synchronization method based on the correlation calculation [18], the proposed algorithm has a much lower computation complexity. In particular, if the feature-length is N , the calculation of a correlation needs multiplication operations to get the result of every $x_i y_i$ and $N - 1$ times add operations for the final result. Furthermore, the times of added to operations can be well reduced. One can first divide the entire sequence into several pairs, then calculate the sums of every pair to get the first $N/2$ results. After the final iterative process, the add operation times can

be reduced to $\log_2 N$. However, there are not any multiplication operations in the proposed scheme, which significantly reduces the computational complexity (see Table 1).

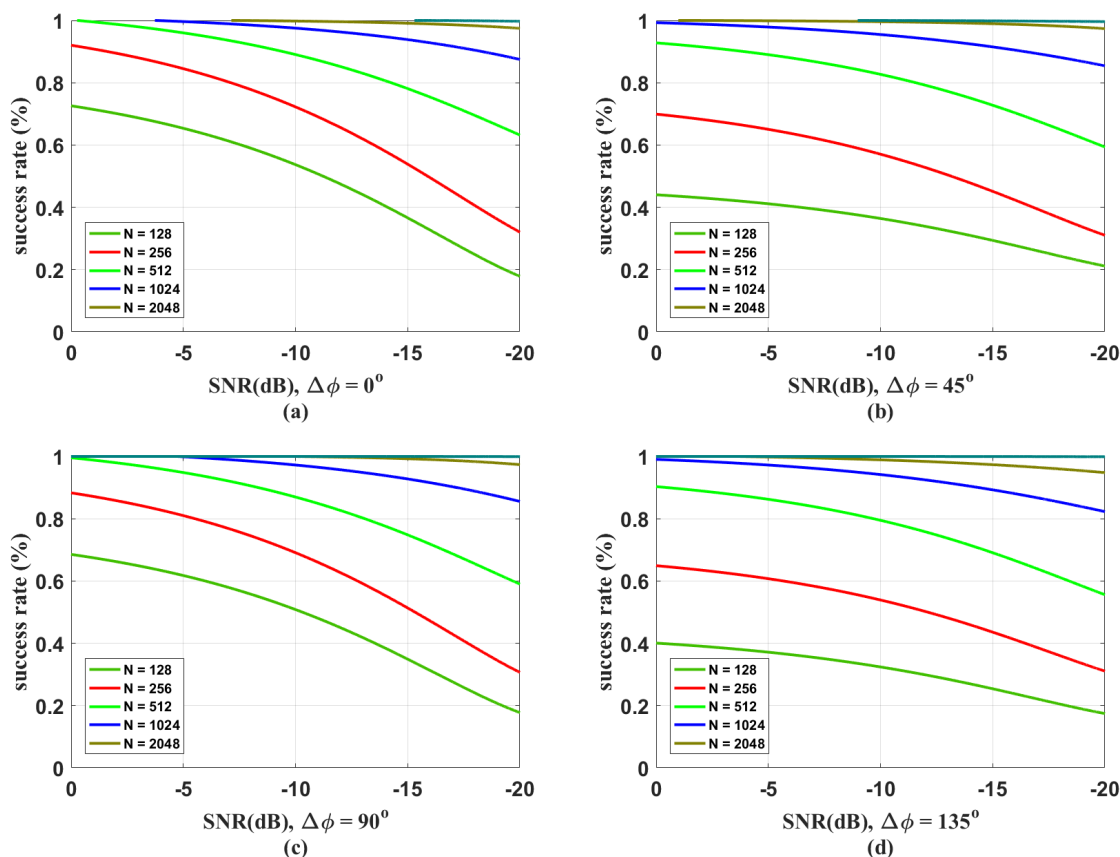


Figure 5. The success rates of the proposed algorithm under different SNR conditions. (a) Phase shift 0° ; (b) phase shift 4° ; (c) phase shift 90° ; (d) phase shift 135° . The lengths of synchronization frames for the curves from bottom to top are $N = 128, 256, 512, 1024, 2048$.

Table 1. Comparison of the algorithm complexity.

Items	Add/Subtract	Multiplication	Comparison	Hamming Distance
Correlation	$\log_2 N$	N	0	0
Incremental labeling	$2L + 1 (L \ll N)$	0	1	N

3.4. Security and Adaptivity Analysis

The realistic system may incur loopholes due to the imperfections of the implementation process, although the CVQKD protocols are theoretically proven to be secure. Traditional frame synchronization methods are performed by alternately transmitting a strong pulse. Although there has not been any practical attack on these frame synchronization schemes, the use of strong pulses can be manipulated, which may incur potential loopholes. Moreover, the frame synchronization methods based on the designing of the special frame may also introduce potential risks, since the synchronization frames can be distinguished from the key data. A well-designed synchronization method should conceal its synchronization frames into key data so that it is hard for an eavesdropper to distinguish them.

Synchronization frames of this proposed scheme are similar to data frames but they are uncorrelated, which is different from the traditional schemes. In our proposed synchronization scheme, we regard parts of the signals as synchronization frames, so the signals and synchronization frames have the same distribution and the same power. If an eavesdropper intends to attack the CVQKD system through the potential loopholes in the frame synchronization method, she must

distinguish the synchronization frames from the quantum signals. So she will detect the quantum signals and this will inevitably cause an increase in excess noise. Her attacks will be then found by the legitimate parties in the following key generation steps. Although the synchronization method in this article uses parts of data as the synchronization frame. The revealing of these synchronization frames does not leave any useful information about the secret key.

In our synchronization scheme, a fraction of data is used as a reference frame. It means that the scheme will also work at the cost of a slight drop in the secret key rate as the previously proposed frame synchronization schemes. We can evaluate the influence of using synchronization frames on the secret key rate when considering the finite-size effects,

$$K_{finite} = \frac{n}{N}(\beta I_{AB} - \chi_{BE} - \Delta(n)), \quad (8)$$

where I_{AB} means the mutual information between Alice and Bob; χ_{BE} is the Holevo bound on the information between Bob and Eve; $\Delta(n)$ can be approximated to $7\sqrt{\frac{\log_2(2/\epsilon)}{n}}$; N denotes the block length and n denotes the size of the samples used for final key generation.

Figure 6 shows the secret key rate curves with or without our synchronization scheme. In the simulation, the lengths of synchronization frames are all 2^{12} in different scenarios; the reconciliation efficiency β is set to $\beta = 0.956$; the attenuation coefficient of optical fiber is set to $\gamma = 0.2$ dB/km and the excess noise of the quantum channel is $\epsilon_e = 0.01$, as experimentally shown in Ref [8]. These two types of curves almost overlap, which indicates that the data sacrificed for synchronization have no significant influence on the secret key rate.

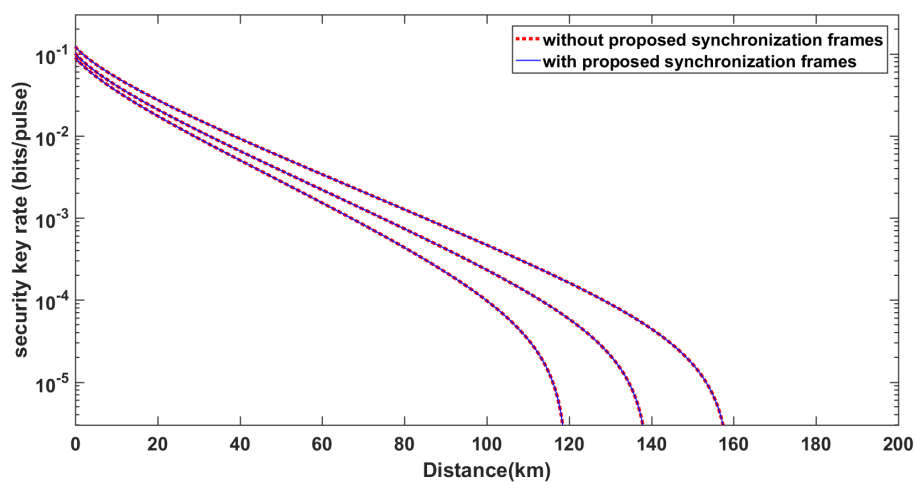


Figure 6. The secret key rates with or without the considerations of using the proposed frame synchronization. The curves from left to right respectively correspond to block lengths of $N = 10^{10}, 10^{11}, 10^{12}$, respectively. The solid blue lines correspond to the secret key rates without considering the cost of synchronization. The dotted red lines correspond to the secret key rates with consideration of using the proposed frame synchronization.

In Figure 6, we show the two types of curves (the secret key rate curves with or without our synchronization scheme) are almost consistent. Whether this consistency changes as the parameters β , γ , and ϵ_e change is worth exploring. Figure 7 reveals that the performance of our algorithm does not deviate under different parameter-settings. We keep the lengths of synchronization frames equal to 2^{12} . The standard setting in Figure 7 is the block length $N = 10^{10}$, $\beta = 0.956$, $\gamma = 0.2$ dB/km, and $\epsilon_e = 0.01$. Keeping other parameters the same, we separately set the parameters $\beta = 0.93, 0.956, 0.98$, $\gamma = 0.18, 0.2, 0.22$ dB/km and $\epsilon_e = 0.008, 0.01, 0.012$. It can be seen that the corresponding curves are all nearly coincident. Essentially, it is because the synchronization scheme uses just a little data for the synchronization frames.

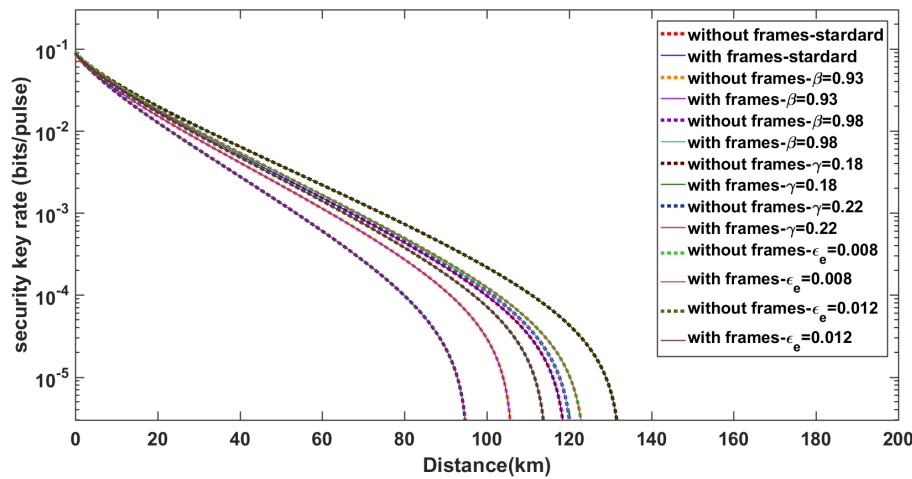


Figure 7. Comparison of how the agreement of the two curves (the secret key rate curves with or without our synchronization scheme) changes under different conditions.

Another important thing needs to be considered here is whether the proposed frame synchronization scheme is valid or not when the attenuation of the quantum channel fluctuates. Actually, except the threshold V_{th} (the threshold V_{th} could be the variance of the received signal) in the labeling procedure must be changed with the value of the received signal, the whole algorithm flow is independent of fluctuations of channel attenuation. The algorithm generates incremental labels by considering relative values rather than absolute values. So the algorithm can resist attenuation fluctuation to some extent.

We simulate the process of quantum channel attenuation fluctuation and test the performance of the proposed synchronization algorithm in this condition. We first simulate the synchronization performance of Bob receiving signals through a constant attenuation channel. Afterward, we change the channel into a fluctuation one and compare the matching cost of these two situations (see Figure 8). The matching cost curve changes little despite the existence of channel attenuation (Figure 8b,d are almost the same). Therefore, attenuation fluctuation has a limited effect on synchronization.

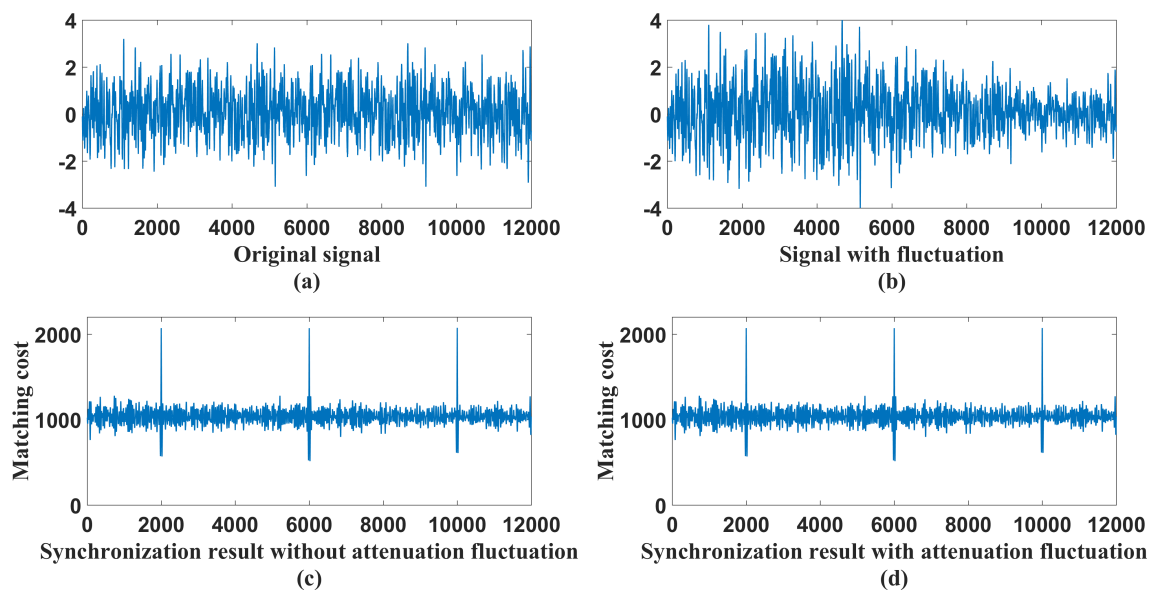


Figure 8. The influence of attenuation fluctuation on the proposed algorithm. (a) Signal without attenuation fluctuation; (b) Signal with attenuation fluctuation; (c) Synchronization result of the signal without attenuation fluctuation; (d) Synchronization result of signal with attenuation fluctuation.

4. Conclusions

Synchronization is a crucial step in the CVQKD. Traditional methods always need to construct special synchronization frames. We propose here a simple and robust synchronization scheme without particularly designing the frame for the CVQKD system. In the proposed scheme, the sender Alice only needs to transmit parts of the quantum signals as synchronization frames to the receiver Bob. A novel feature is designed to help find the correct synchronization location. The analysis of our scheme shows that the feature we designed can tolerate phase shifts among range $(0, 2\pi)$ and the scheme can synchronize well under low SNR conditions. The simulations of the scheme under different parameter settings indicate that the performance can be significantly improved with increasing feature-length. Moreover, the proposed feature has lower computational complexity while maintaining a good synchronization performance.

Author Contributions: R.C. designed the conception of the study, accomplished the formula derivation and numerical simulations, and drafted the article. P.H. gave the general idea of the study, checked the draft, and provided feasible suggestions and critical revision of the manuscript. D.L. gave feasible advice and helped with the calculation. Y.Z. conceived of the study and reviewed relevant studies. G.Z. reviewed relevant studies and literature, conceived of and designed the study and performed the critical revision of the manuscript. All authors have read and approved the final manuscript.

Funding: National key research and development program (2016YFA0302600); National Natural Science Foundation of China (NSFC) (61332019, 61971276, 61631014, 61671287).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **1984**, *560*, 7–11. [[CrossRef](#)]
2. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [[CrossRef](#)] [[PubMed](#)]
3. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [[CrossRef](#)] [[PubMed](#)]
4. Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, Y.H.; Chen, S.J.; Mao, Y.Q.; Huang, M.Q.; Zhang, W.J.; et al. Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [[CrossRef](#)] [[PubMed](#)]
5. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [[CrossRef](#)]
6. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381. [[CrossRef](#)]
7. Grosshans, F.; Assche, G.V.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241. [[CrossRef](#)]
8. Huang, D.; Huang, P.; Lin, D.K.; Zeng, G.H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [[CrossRef](#)]
9. Bai, D.Y.; Huang, P.; Ma, H.X.; Wang, T.; Zeng, G.H. Performance Improvement of Plug-and-Play Dual-Phase-Modulated Quantum Key Distribution by Using a Noiseless Amplifier. *Entropy* **2017**, *19*, 546. [[CrossRef](#)]
10. Qi, B.; Huang, L.L.; Qian, L.; Lo, H.K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **2007**, *76*, 052323. [[CrossRef](#)]
11. Marie, A.; Alléaume, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 012316. [[CrossRef](#)]
12. Daniel, B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. *Phys. Rev. X* **2015**, *5*, 041010. [[CrossRef](#)]
13. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Gui, M.; Zhou, Y.L.; Liang, L.M. Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator. *Phys. Rev. A* **2014**, *89*, 032310. [[CrossRef](#)]

14. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **2013**, *87*, 062313. [[CrossRef](#)]
15. Shen, Z.Y.; Fang, J.; He, G.Q.; Zeng, G.H. Study of Synchronous Technology in High-Speed Continuous Variable Quantum Key Distribution System. *Chin. J. Lasers* **2015**, *35*, 0305004. [[CrossRef](#)]
16. Liu, Y.M.; Wang, C.; Huang, D.; Huang, P.; Feng, X.Y.; Peng, J.Y.; Cao, Z.W.; Zeng, G.H. Synchronous Scheme and Experimental Realization in Continuous Variable Quantum Key Distribution System. *Acta Opt. Sin.* **2013**, *40*, 0106006. [[CrossRef](#)]
17. Li, H.S.; Wang, C.; Huang, P.; Huang, D.; Wang, T.; Zeng, G.H. Practical continuous-variable quantum key distribution without finite sampling bandwidth effects. *Opt. Express* **2016**, *24*, 20481–20493. [[CrossRef](#)]
18. Lin, D.; Huang, P.; Huang, D.; Wang, C.; Peng, J.Y.; Zeng, G.H. High performance frame synchronization for continuous variable quantum key distribution systems. *Opt. Express* **2015**, *23*, 22190–22198. [[CrossRef](#)]
19. Downing, C.A.; Carreño, J.L.; Laussy, F.P.; del Valle, E.; Fernández-Domínguez, A.I. Quasichiral interactions between quantum emitters at the nanoscale. *Phys. Rev. Lett.* **2019**, *122*, 057401. [[CrossRef](#)]
20. Casalengua, E.Z.; Carreño, J.C.; Laussy, F.P.; del Valle, E. Conventional and unconventional photon statistics. *arXiv* **2019**, arXiv:1901.09030.
21. Li, D.; Huang, P.; Wang, T.; Wang, S.; Chen, R.; Zeng, G.H. Phase compensation based on step-length control in continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 20670–20687. [[CrossRef](#)] [[PubMed](#)]
22. Huang, P.; Lin, D.K.; Huang, D.; Zeng, G.H. Security of continuous-variable quantum key distribution with imperfect phase compensation. *Int. J. Theor. Phys.* **2019**, *54*, 2613–2622. [[CrossRef](#)]
23. Qi, B.; Evans, P.G.; Grice, W.P. Passive state preparation in the Gaussian-modulated coherent-states quantum key. *Phys. Rev. A* **2018**, *97*, 012317. [[CrossRef](#)]
24. Scholtz, R.A. Frame synchronization techniques. *IEEE Trans. Commun.* **1980**, *28*, 1204–1213. [[CrossRef](#)]
25. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B At. Mol. Opt. Phys.* **2009**, *42*, 114014. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).