Continuous variable quantum key distribution[*]

Yong-Min Li(李永民)[1,2,†], Xu-Yang Wang(王旭阳)[1,2], Zeng-Liang Bai(白增亮)[1,2],
Wen-Yuan Liu(刘文元)[1,2], Shen-Shen Yang(杨申申)[1,2], and Kun-Chi Peng(彭堃墀)[1,2]

[1] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan* 030006, *China*

[2] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan* 030006, *China*

(Received 21 November 2016; revised manuscript received 28 December 2016; published online 20 February 2017)

Quantum key distribution enables unconditionally secure key distribution between two legitimate users. The information-theoretic security is guaranteed by the fundamental laws of quantum physics. Initially, the quantum key distribution protocol was proposed based on the qubits. Later on, it was found that quantum continuous variables can also be exploited for this target. The continuous variable quantum key distribution can build upon standard telecommunication technology and exhibits a higher secret key rate per pulse at a relatively short distance due to the possibility of encoding more than 1 bit per pulse. In this article, we review the current status of the continuous variable quantum key distribution research, including its basic principle, experimental implementations, security and future directions; the experimental progress in this field made by our group is also presented.

Keywords: quantum key distribution, continuous variable, quantum optics, quantum communication

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/26/4/040303

1. Introduction

In the past three decades, quantum theory has found various applications in the domain of communication. The combination of quantum mechanics and information theory enables new forms of communication techniques, which are more powerful than their classical analogs in certain scenarios. At present, the most mature application of quantum communication is quantum cryptography, which can provide unconditional security based on the so-called one-time pad encryption invented by Vernam in 1917.[1] On the contrary, the security of most modern cryptographic applications is based on some difficult mathematic problems, which can be broken in principle if the adversaries possess strong enough computational power. For example, the security of the public-key encryption method-RSA rests on the assumption that the problem of factoring a large number is hard.[2] The intrinsic security of quantum cryptography comes from the quantum key distribution (QKD) technique which provides a secure approach to sharing a secret key between two legitimate parties required by the one-time pad encryption.

Since Bennett and Brassard[3] proposed the first QKD protocol (BB84 protocol or four-state protocol), a lot of theoretical and experimental progress[4–9] has been made (for the basics of the quantum key distribution, readers can refer to Refs. [4]–[8]). In the theoretical aspect, theoretical tools have been developed to assess the security and the unconditional security of several QKD protocols against arbitrary attacks has been proved rigorously in the asymptotic limit. The composable security in a finite-key regime has also made significant progress. Long-distance QKD over a distance of more than one hundred kilometers based on various protocols has been demonstrated in both fibers and free space. Several QKD networks have been tested in a field environment.[10–16] Recently, it is noted that QKD products have also been launched commercially.

Although various QKD protocols have been proposed, they can be classified as three main families: discrete-variable coding, continuous-variable (CV) coding and distributed-phase-reference coding. The discrete-variable QKD protocol employs the discrete variables of a quantum state, such as the polarization or phase of single photons, whereas in the CV scheme, the key information is encoded in continuous quantum variables, such as the quadratures of quantized electromagnetic modes (coherent states or squeezed states). Unlike the other two coding schemes, where each bit of the key is encoded in an independent single signal state, the distributed-phase-reference coding scheme resorts to the phase difference between two successive signal pulses or the photon arrival times to encode the key information. Both the discrete-variable coding and distributed-phase-reference coding scheme utilize photon counting and post-selection techniques, while homodyne detection is adopted in continuous-variable coding.

The introduction of CV coding provides a useful alternative approach for quantum information processing. It can build

[*] Project supported by the National Natural Science Foundation of China (Grant Nos. 61378010 and 11504219), the Key Project of the Ministry of Science and Technology of China (Grant No. 2016YFA0301403), the Natural Science Foundation of Shanxi Province, China (Grant No. 2014011007-1), and the Program for the Outstanding Innovative Teams of Higher Learning Institutions of Shanxi Province, China.

[†] Corresponding author. E-mail: yongmin@sxu.edu.cn

upon standard telecommunication technology, for instance, instead of a sophisticated single photon counting technique, the coherent detection method (homodyne detection) widely used in the classical optical communications field is exploited. The quantum efficiency of the homodyne detector at 1550 nm (the lowest-loss window of telecom single mode fiber) determined by PIN photodiodes can reach above 90%. On the other hand, the local oscillator (LO) in homodyne detection can act as a built-in mode filter both in the spatial and temporal domains for the background noisy photons. This feature is beneficial to the coexistence of QKD with intense classical optical signals in dense-wavelength-division multiplexing networks. Due to the possibility of encoding more than 1 bit per pulse, the CV QKD can achieve a higher secret key rate per pulse at a relatively short distance.

The rest of this paper is organized as follows. In Section 2 we present the basic principle and experimental progress of CV QKD. Our recent work in long-distance fiber-based CV QKD is described in Section 3. In Section 4, we review the progress of security analysis including the security in the practical environment; then some future research directions and the efforts towards solving these issues are presented including the device-independent QKD, the issues of excess noises and data post-processing which limit the secret key rate and key transmission distance, the advances in multiplexing of CV QKD with classical optical signals in a single fiber, and the photonic integration technology. In Section 5 we give a brief conclusion.

2. Basic principle of CV QKD and experimental progress

Since Ralph suggested encoding key information on the amplitude and phase quadrature amplitudes of the light field and successively detecting the signal by homodyne detection in QKD,[17] a variety of CV QKD protocols have been proposed. The early proposals mainly concentrate on discrete modulation,[17–19] i.e., the encoded key information is binary. Shortly after that, continuous modulation (Gaussian modulation) CV protocols were devised based on squeezed states[20,21] and coherent states of light.[22] In the above two protocols, the key receiver Bob randomly chooses to measure the amplitude or phase quadrature, this implies the need for sifting; Alice and Bob need to discard half of their data (for doubly modulated coherent states,[22] only Alice needs to discard half of her data). Later, the heterodyne based Gaussian-modulated coherent state protocol was proposed[23] and demonstrated.[24] In this case, neither active basis choice nor key sifting is required, and the key rate can often be increased. By exploiting the quantum correlations of Einstein–Podolsky–Rosen (EPR) entangled states, it is shown that CV QKD can also be realized without signal modulation.[25] In 2009, a CV protocol based on squeezed states and heterodyne detection was proposed, which is shown to exhibit higher secret key rates than any previous Gaussian protocols.[26] Recently, it was shown that by modulating the entangled states of light, one can enhance greatly the robustness of the CV QKD to channel noise, and therefore attain a high key rate and key distribution distance.[27,28]

There are two kinds of ways to implement a QKD, i.e., a prepare and measure (PM) scheme, and an entanglement-based (EB) scheme. The PM scheme is usually easier and simpler to implement, whereas the EB scheme can simplify the theoretical calculation of the key rates and provide a unified description of the different protocols.[29] These two different versions are equivalent for Gaussian protocols.[30] In the following, we describe the basic procedure of the Gaussian-modulated coherent state PM protocol.

2.1. State preparation, distribution and measurement

Alice prepares randomly a weak coherent state $|x_{\mathrm{A}}+\mathrm{i}p_{\mathrm{A}}\rangle$, where x_{A} and p_{A} are independent Gaussian variables with variance V_{A}. The coherent state is sent to Bob through a quantum channel, usually accompanied with an LO for a phase reference. Bob measures randomly the $\hat{x}$ or $\hat{p}$ quadrature (homodyne detection), or both quadratures (heterodyne detection). The above step is repeated N times.

2.2. Key sifting and Parameter estimation of the quantum channel

For homodyne detection, Bob tells Alice over an authenticated classical channel which quadratures he has measured. They keep only the relevant quadrature values for which they have used the same bases. After such key sifting, Alice and Bob share a series of Gaussian numbers (usually called a raw key). If Bob performs a heterodyne detection instead of homodyne, no key sifting is required. At this stage, Alice and Bob reveal a random portion of the raw keys to evaluate the parameters of the quantum channel. For CV QKD, such parameters are channel transmission T and excess noise ε. Combined with other system parameters: V_{A}, detection efficiency η, dark electronic noise of the homodyne detection υ_{el}, the secret key rate can be calculated from $\Delta I=\beta I_{\mathrm{AB}}-\chi_{\mathrm{BE}}$, where β is the reconciliation efficiency, I_{AB} is the mutual information between Alice and Bob, χ_{BE} is Eve's accessible information which is upper bounded by the Holevo quantity. If $\Delta I\leq 0$, the protocol is aborted and restarted from Step 1.

2.3. Error correction (information reconciliation)

Even if no eavesdropping exists and the signal state is prepared perfectly, the errors between Alice's and Bob's raw keys are inevitable due to the vacuum noise of the coherent state, detector dark noise, etc. In order to obtain a common binary string out of partially correlated raw keys, a classical error correction algorithm is required, for instance, low-density parity-check (LDPC) codes. To this end, Bob sends the syndrome of his data to Alice over a public channel (reverse reconciliation), based on the syndrome, Alice corrects her data into those that are in accord with Bob.

2.4. Privacy amplification

Alice and Bob perform privacy amplification to erase the information Eve could obtain and distill the final secure key. This can be realized by using two-universal hash functions, more precisely, by multiplying the key bits by a random Toeplitz matrix.

Early proposals of CV QKD adopted the forward reconciliation which limits the quantum channel loss to less than 3 dB. Later it was found that such a loss limit can be broken by the technique of postselection[31] or reverse reconciliation.[30] The first reverse-reconciliation Gaussian-modulated coherent state protocol was implemented with bulk optical elements over a short free-space of an optical table.[32] After this, the CV QKD experiments were extended to long distances by exploiting telecom fiber. Based on a go-&-return configuration, a high stable QKD was demonstrated over 14-km fiber.[33] With both polarization and temporal multiplexing, a CV QKD system was demonstrated over a 25-km fiber which includes the procedure of signal modulation and measurement, authentication, reverse reconciliation, and privacy amplification.[29] A 5-km distribution experiment was also reported by combining polarization and frequency multiplexing.[34] All of the implementations above utilized the Gaussian modulation. To simplify the modulation procedure, discrete modulation protocols have been demonstrated experimentally over a 24-km and 30-km fiber, respectively.[35–37] With an improvement of the data reconciliation efficiency, i.e., by employing both the multidimensional reconciliation and the multi-edge Low Density Parity Check (LDPC) codes,[38–40] the secure key distribution can be achieved over 80 km.[41] Recently, efforts toward a high speed key distribution experiment have been pursued.[42]

3. Our experimental progress

Figure 1 shows the sketch of our experimental setup for long-distance CV QKD. By exploiting two cascaded intensity modulators, high-extinction-ratio optical pulses with 100-ns-wide and repetition rate of 500 kHz are produced from a 1550-nm continuous-wave (CW) single frequency fiber laser. The generated optical pulses are further separated into a weak signal field and an intense LO through a fiber coupler (99/1). The pulsed coherent states are modulated with bivariate Gaussian modulation in the phase space through a combination of an intensity modulator and a phase modulator. The signal and LO are then directed to a 50-km single mode fiber spool through time multiplexing and polarization multiplexing, which are realized by an 80-m fiber and a polarizing beam splitter (PBS), respectively. When Bob receives the quantum states sent by Alice, he measures randomly the amplitude or phase quadrature of the signal by using a pulsed balanced homodyne detector (BHD). Here, both the random basis switch and the relative phase locking between the signal and LO are implemented with a phase modulator located in the LO path. In order to correctly measure the peak voltage of the BHD output and synchronize the system, a small portion of the LO beam is picked off to recover the system clock, which is then delayed precisely to a desired value.

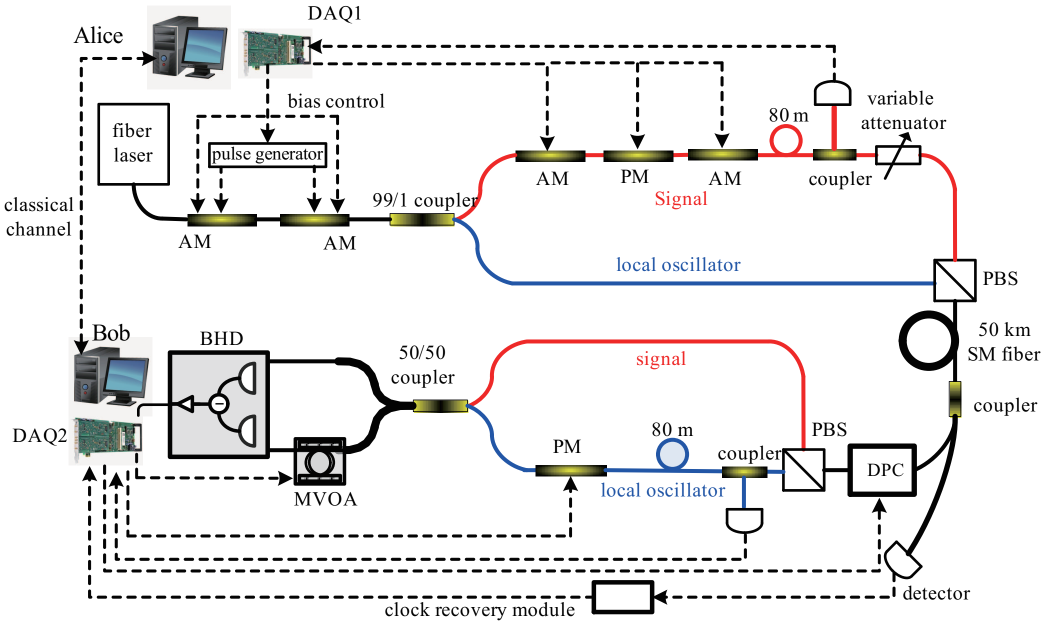

Fig. 1. (color online) Experimental setup of 50-km CV QKD, where DAQ denotes the data acquisition module, AM the amplitude modulator, PM the phase modulator, PBS the polarizing beam splitter, DPC the dynamic polarization controller, MVOA the motor variable optical attenuator, and BHD the balanced homodyne detector.

The excess noise is one of the key factors which affect the system performance significantly, i.e., the secure key rate and transmission distance. In the ideal case, the excess noises only refer to those noises which are induced by Eve's eavesdropping behavior. In practice, even if there is no eavesdropping, the system can exhibit some technical noises, including the leakage of LO pulse due to the finite extinction ratio of the optical pulses, the preparation of the quantum states, nonideal phase locking between the LO and signal, nonlinear optical phenomenon of the fiber, the stability of the BHD, etc. These noises are added by Alice's or Bob's apparatus except the nonlinear optical scattering of the fiber, it is usually difficult for Eve to manipulate such noises to attack the system. However, the technical noises of the system usually vary with time, which will require real-time monitoring to characterize the system parameters. Such monitoring is a challenge in a real QKD system and in practice one usually attributes such system noises to Eve's attack when considering the security.

In our system, both the polarization and temporal multiplexing are used to isolate the contamination of the LO leakage to the signal field. The corresponding excess noise from the leakage can be given by $\varepsilon_{\text{leak}} = 2\langle n_{\text{le}}\rangle$ on the assumption that the relative phase between the LO and the leakage randomly varies from 0 to 2π, where $\langle n_{\text{le}}\rangle$ is the average photon number of the LO leakage. By combining a high stable bias locking technique with two cascaded intensity modulators, high-extinction-ratio light pulses with an extinction ratio higher than 80 dB were generated stably from the CW light.[43] After the LO and the signal propagate along the long-distance single mode fiber, a dynamical polarization controller at the entrance of Bob's site was employed to correct the polarization variations of both light fields to ensure a long-term stable operation, and the extinction of over 27 dB is achieved. Considering the average photon number of the LO pulse $\langle n_{\text{L}}\rangle = 6\times 10^7$ and the total extinction ratio (which equals the extinction ratio of the light pulses plus the polarization extinction ratio) of $\alpha = 107$ dB, the leakage can be calculated to be $\langle n_{\text{le}}\rangle = 10^{-\alpha/10}\langle n_{\text{L}}\rangle \approx 0.0012$. This results in an equivalent excess noise of 0.0024 shot noise unit (SNU).

The preparation process of the quantum states, such as Gaussian modulation can introduce excess noises. The key points are the calibration of the bias point and the half-wave voltage for the intensity modulator and the phase modulator which are exploited to fulfill the Gaussian modulation. Incorrect calibration of such parameters can lead to the wrong modulation result which deviates from a Gaussian modulation and results in excess noises. It is noted that the bias points and the half-wave voltages drift with time and should be calibrated regularly. In our system the interval of such calibrations is on the order of minutes.

Another source of the system excess noise comes from the measurement process. The first one is the phase locking uncertainty between the LO and signal. Such random phase fluctuations can cause Bob's measurement basis to change from $\hat{x}$ to $\hat{x}' = \hat{x}\cos\varphi + \hat{p}\sin\varphi$, where φ is the residual phase fluctuation when the phase locking servo system is switched on. In this case, the corresponding excess noise can be expressed as $\langle(\Delta\hat{x}')^2\rangle - \langle(\Delta\hat{x})^2\rangle \approx V_{\text{A}}\varphi^2$. In our system, the modulation variance V_{A} is ~ 17 and the residual phase fluctuation is around ± 1 degree, which leads to an excess noise of 0.005. The phase locking fluctuation mainly derives from the 80-m delay lines, which can be shortened in principle by using shorter optical pulses. It is noted that lower modulation variance is beneficial to the suppression of such a measurement excess noise. Another source of phase fluctuation is due to the finite coherent length of the laser and the imbalance between the LO and signal path. For a single frequency laser with a linewidth of $\Delta\omega$, the imbalance of the interferometer with an amount of ΔL can lead to a phase fluctuation of $\Delta\theta = \sqrt{\Delta\omega\Delta L/c}$, where c is the speed of light. This means that the LO and signal path should be well balanced.

The common mode rejection ratio (CMRR) and its long-term stability of the measurement device on Bob's side are also crucial to the evaluation of the excess noise. For a realistic BHD with a nonideal balance of its two arms: $T = 0.5 + \delta_{\text{T}}$, the detected variance of the photocurrent signal is given by

$$\langle(\Delta\hat{i}_{-})^2\rangle \approx 4\bar{n}_{\text{L}}(1-4\delta_{\text{T}}^2)\left[\langle(\Delta\hat{x}_{\text{s}})^2\rangle + \delta_{\text{T}}^2\langle(\Delta\hat{n}_{\text{L}})^2\rangle/\bar{n}_{\text{L}}\right], \tag{1}$$

where $\bar{n}_{\text{L}}$ is the average photon number of LO pulse, and $\hat{x}_{\text{s}}$ is the quadrature of the signal field. The excess noise introduced by the second term on the right-hand side of Eq. (1) can be written as

$$\varepsilon_{\text{CMRR}} = (V_{\text{B}} - 1 - \upsilon_{\text{el}})4\delta_{\text{T}}^2\langle(\Delta\hat{n}_{\text{L}})^2\rangle/(G\bar{n}_{\text{L}}), \tag{2}$$

where V_{B} is the variance of the quadrature measured by Bob, and $G = \eta T$ is the overall transmission efficiency. In our experiment, the pulsed BHD is balanced precisely by using a variable optical attenuator based on bending the fiber and the resulting CMRR can reach $1/\delta_{\text{T}}^2 > \bar{n}_{\text{L}}$,[44] which ensures that the measurement induced excess noise can be neglected in our experiment. In order to improve the long-term stability of the CMRR, a feedback control based auto-balance technique is proposed and demonstrated.[45]

In CVQKD, the signal field and the LO travel along a single fiber to alleviate their relative phase fluctuations. Due to the relatively strong intensity of the LO and the long single mode fiber, the nonlinear optical scattering, more precisely, the depolarized guided acoustic wave Brillouin scattering can scatter a small portion of the LO photons into the signal pulse and add excess noise to the system.[46] This effect is particularly evident for a high-bandwidth QKD over 1 GHz with a light pulse less than 1 ns.

The data post-processing procedure including the key reconciliation and privacy amplification is a necessary part to extract the final secure key from the raw key. We have designed long block-length irregular LDPC codes with high error-correcting capacity and achieved high-efficiency slice reconciliation based on multilevel coding/multistage decoding.[47] The reconciliation efficiency can reach $\beta > 95\%$ for a signal-to-noise ratio (SNR) from 1 to 3. Given the experimentally determined parameters of $V_{\mathrm{A}} = 17.3$, $\eta = 0.64$, $T = 0.1$, $\upsilon_{\mathrm{el}} = 0.1$, $\varepsilon = 0.03$, and $\beta = 95\%$, the secret key rate per pulse is calculated to be $\Delta I^{\mathrm{Holevo}} = 0.007$. Consider the repetition rate of the effective data pulses of $R^{\mathrm{data}} = 250$ kHz (the rest of the signal pulses are assigned to the evaluation of the shot noise and excess noise, phase locking between the signal and LO, and the CMRR monitoring), the final secret key rate we obtained is $\Delta I^{kr} = \Delta I^{\mathrm{Holevo}} R^{\mathrm{data}} = 1.4\ \mathrm{kbit/s}$. The final secure key is safely distilled through the subsequent privacy amplification after the reverse reconciliation step.

Figure 2 shows our integrated CV QKD prototype. Each device is integrated into a chasis that provides ports of power input, quantum channel interface (single mode fiber connector), data Input/Output to the data acquisition modules which are located in the control PC. The classical communication tasks between Alice and Bob are implemented by optical small form-factor pluggable transceivers on each side. To ensure an automatic operation of the CV QKD system, a dedicated software is designed to manage all the necessary modules of the system, including the signal modulation and measurement, feedback control, reverse reconciliation, privacy amplification, classical communication, etc.

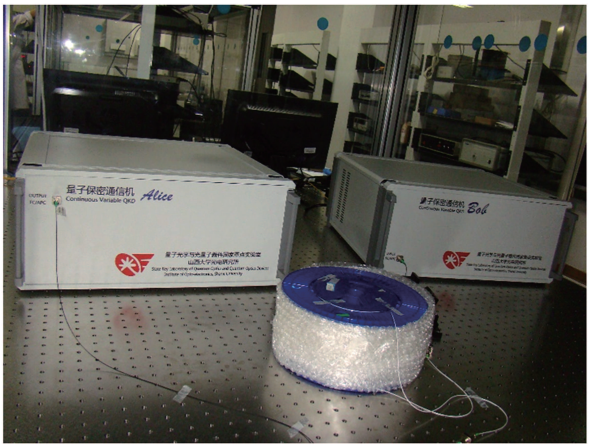

Fig. 2. (color online) QKD devices.

4. Current status of the security analysis and future research directions

The security proofs of the CV QKD protocols have made significant progress in the past ten years.[26,27,48–64] Currently, there are three kinds of security notions:[65] composable security against arbitrary attacks, composable security against collective attacks, and security against collective attacks in the asymptotic limit. The composable security[63,64] means that the security parameters of the whole system can be given by $\varepsilon_1 + \varepsilon_2$ if the QKD is employed in another application, where ε_1 and ε_2 are the security parameters of the QKD and its application subsystem, respectively. The first security notion is the strongest one without any restriction on the input state, while the second one requires the input state to be identically and independently distributed, and the last one implies that Alice and Bob exchange infinitely the number of signals and the quantum state shared by two legitimate users is known. From the above definitions, it is evident that the first two security definitions depend on how many times the channel is utilized, i.e., the finite size effect is involved and needs to be considered.

At present, two CV QKD protocols have been proven to be composably secure.[56,58,60,61] They are a Gaussian-modulated squeezed state plus homodyne measurement protocol and a Gaussian-modulated coherent state plus heterodyne measurement protocol. However, for realistic block sizes, the security proof techniques adopted above lead to a large sacrifice in the secret rate. For other protocols, only the asymptotic key rate is known precisely, the proofs of the composable security are still in progress. Although by using de Finetti-type reduction, the collective attacks are proven to be optimal in the asymptotic regime, i.e., a protocol is unconditionally secure against arbitrary attacks whenever it is secure against collective attacks. However, it is not the case in the finite-size regime. It is still a challenge to find the right bound of the secure key rate in the finite size regime. In a word, the improvement of already known proof techniques or inventions of new methods is still necessary for the establishment and optimization of the composable securities of various CV protocols.

In the above security analysis, it is assumed that Alice and Bob's apparatuses are perfect or can be described completely. In practice, it is difficult to characterize all aspects of the apparatuses, i.e., there are always imperfections which are beyond the theoretical models. Such imperfections may be exploited by Eve and introduce the so-called side-channel attacks. Recently, several attacks of such a kind have been proposed, which concentrate on the detection stage. For instance, Eve can benefit from the fluctuations of the LO.[66] By properly controlling the LO, the shot noise can be overestimated, which further leads to an underestimation of the excess noise in the system.[67] Instead of attacking the LO, saturation attack through the exploitation of the nonlinear response of homodyne detection can open a loophole.[68] It is also shown that Eve can obtain all secret keys without being discovered by making use of the wavelength dependent property of the beamsplitter.[69,70] To defeat the above attacks, real-time shot noise measurement can be added on Bob's side.[71] Generating the LO locally is also a useful way to resist such attacks.[72–74]

Although it is possible in principle to defeat all the side-channel attacks through positioning all the imperfections carefully, another attractive alternative is the device-independent (DI) QKD, the security of which relies on the violation of a Bell inequality.[75,76] However, the DI QKD is currently unfeasible because of the loophole-free Bell test. Then, a compromised version of the DI QKD named measurement-device-independent (MDI) QKD is proposed,[77–79] which enables the faithful operation of the QKD with untrusted measurement devices and are feasible with the current technology. In the CV regime, a proof-of-principle short free-space demonstration of this approach has been realized recently.[80–82]

It is known that the CV QKD protocol is very sensitive to the excess noise. To this end, the technical noises of the system should be minimized and the feedback control systems are required to ensure a long-term stable low-noise operation. On the other hand, it is shown that the maximum transmission distance or tolerated excess noise of CV QKD in the presence of a Gaussian noisy & lossy channel can be increased by using squeezed or entangled states,[26–28] linear noiseless amplifier[83,84] and non-Gaussian postselection.[85,86] For the future high speed ($\sim$ 100-MHz repetition rate) and real-time operation of CV QKD, a fast and efficient hardware secure key extraction engine should be pursued, for instance, based on field-programmable gate array (FPGA). This is due to the fact that in the CV regime each signal pulse sent by Alice is detected by Bob's BHD which generates a useful output signal.

Recently, some efforts have also been pursed towards incorporating QKD into existing fiber optical networks and integrating the components of a QKD system on a chip. It has been shown that CV QKD is robust to the noise photons from the classical signals and can coexist with classical signals of realistic intensity in the same fiber.[87,88] The on-chip system has the advantages of scalability, low-power, small size, and flexibility. In this direction, a proof-of-principle Si photonic chip including some of the functionalities of CV QKD has been demonstrated recently.[89]

To improve the performance of the QKD protocol, efforts towards combining both the advantages of discrete-variable and CV QKD protocol have begun to be pursued. Recently, the notion of high-dimensional QKD based on the continuous-variable degree of freedom of an entangled photon was proposed to achieve high photon information efficiency and long transmission distance simultaneously.[90,91] More precisely, the key information carriers exploit the position-momentum or the time-energy entangled photon pairs.

5. Conclusions

In the past few decades, the QKD based on continuous variable of the light field has made great progress. Nevertheless, there are still some challenges that need to be resolved for its wide applications. The majority of current CV QKD protocols employ the single mode fiber as the quantum channel, it is expected that the free-space CV QKD which has the potential of building a secure link between mobile objects will attract a great deal of attention in the coming years. New kinds of protocols which own superior performance and relatively low technical complexity are anticipated also. With the fast development of QKD together with advances of other branches of quantum cryptography such as quantum digital signatures, quantum secret sharing, quantum coin flipping, etc., we believe that the quantum communication network will become part of our everyday life in the near future.

References

[1] Vernam G S 1926 *J. Am. Inst. Elec. Eng.* **55** 109

[2] Rivest R L, Shamir A and Adleman L M 1978 *Commun. ACM* **21** 120

[3] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, India, p. 175

[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[5] Braunstein S L and Loock P 2005 *Rev. Mod. Phys.* **77** 513

[6] Wang X B, Hiroshima T, Tomita A and Hayashi M 2007 *Phys. Rep.* **448** 1

[7] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[8] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C Shapiro J H and Lioyd S 2012 *Rev. Mod. Phys.* **84** 621

[9] Lo H W, Curty M and Tamaki K 2014 *Nat. Photon.* **8** 595

[10] Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J and Yeh H *Proceedings of SPIE* 5815*, Quantum Information and Computation III*, March 28, 2005, Orlando, USA, p. 138

[11] Peev M, Pacher C, Alléaume R, *et al.* 2009 *New J. Phys.* **11** 075001

[12] Stucki, Legré D M, Buntschu F, *et al.* 2011 *New J. Phys.* **13** 123001

[13] Chen T Y, Liang H, Liu Y, Cai W Q, Ju L, Liu W Y, Wang J, Yin H, Chen K, Chen Z B, Peng C Z and Pan J W 2009 *Opt. Express* **17** 6540

[14] Wang S, Chen W, Yin Z Q, Zhang Y, Zhang T, Li H W, Xu F X, Zhou Z, Yang Y, Huang D J, Zhang L J, Li F Y, Liu D, Wang Y G, Guo G C and Han Z F 2010 *Opt. Lett.* **35** 2454

[15] Sasaki M, Fujiwara M, Ishizukaet H, *et al.* 2011 *Opt. Express* **19** 10387

[16] Fröhlich B, Dynes J F, Lucamarini M, Sharpe A W, Yuan Z and Shields A J 2013 *Nature* **501** 69

[17] Ralph T C 1999 *Phys. Rev. A* **61** 010303

[18] Hillery M 2000 *Phys. Rev. A* **61** 022309

[19] Reid M D 2000 *Phys. Rev. A* **62** 062308

[20] Cerf N J, Lévy M and Assche G V 2001 *Phys. Rev. A* **63** 052311

[21] Gottesman, D and Preskill J 2001 *Phys. Rev. A* **63** 022309

[22] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[23] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504

[24] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 *Phys. Rev. Lett.* **95** 180503

[25] Su X L Wang W Z, Wang Y, Jia X J, Xie C D and Peng K C 2009 *Europhys. Lett.* **87** 20005

[26] García-Patrón R and Cerf N J 2009 *Phys. Rev. Lett.* **102** 130501

[27] Madsen L S, Usenko V C, Lassen M, Filip R and Andersen U L 2012 *Nat. Commun.* **3** 1083

[28] Usenko V C and Filip R 2011 *New J. Phys.* **13** 113007

[29] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tuaale-Brouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305

[30] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier P 2003 *Quan. Inform. & Comput.* **3** 535

[31] Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901

[32] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238

[33] Legré M, Zbinden H and Gisin N 2006 *Quantum Inform. Comput.* **6** 326

[34] Qi B, Huang L L, Qian L, Lo H K 2007 *Phys. Rev. A* **76** 052323

[35] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504

[36] Xuan Q D, Zhang Z S and Voss P L 2009 *Opt. Express* **17** 24244

[37] Wang X Y, Bai Z L, Wang S F, Li Y M and Peng K C 2013 *Chin. Phys. Lett.* **30** 010305

[38] Leverrier A, Alléaume R, Boutros J, Gilles Z and Philippe G 2008 *Phys. Rev. A* **77** 042325

[39] Jouguet P, Kunz-Jacques S and Leverrier A 2011 *Phys. Rev. A* **84** 062317

[40] Jouguet P, Elkouss D and Kunz-Jacques S 2014 *Phys. Rev. A* **90** 042329

[41] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photon.* **7** 378

[42] Huang D, Lin D, Wang C, Liu W Q, Fang S H, Peng J Y, Huang P and Zeng G H 2015 *Opt. Express* **23** 17511

[43] Wang X Y, Liu J Q, Li X F and Li Y M 2015 *IEEE J. Quantum Electron.* **51** 5200206

[44] Wang X Y, Bai Z L, Du P Y, Li Y M and Peng K C 2012 *Chin. Phys. Lett.* **29** 124202

[45] Liu J Q, Wang X Y, Bai Z L and Li Y M 2016 *Acta Phys. Sin.* **65** 100303 (in Chinese)

[46] Li Y M, Wang N, Wang X Y and Bai Z L 2014 *J. Opt. Soc. Am. B* **31** 2379

[47] Bai Z L, Wang X Y, Yang S S and Li Y M 2016 *Sci. China-Phys. Mech. Astron.* **59** 614201

[48] Devetak I and Winter A 2005 *Proc. R. Soc. A* **461** 207

[49] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504

[50] Navascues M and Acin A 2005 *Phys. Rev. Lett.* **94** 020505

[51] Wolf M M, Giedke G and Cirac J I 2006 *Phys. Rev. Lett.* **96** 080502

[52] Navascués M, Grosshans, F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502

[53] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[54] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504

[55] Usenko V C and Filip R 2010 *Phys. Rev. A* **81** 022318

[56] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502

[57] Weedbrook C, Pirandola S and Ralph T C 2012 *Phys. Rev. A* **86** 022318

[58] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502

[59] Walk N, Ralph T C, Symul T and Lam P K 2013 *Phys. Rev. A* **87** 020303

[60] Furrer F 2014 *Phys. Rev. A* **90** 042325

[61] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[62] Usenko V C and Grosshans F 2015 *Phys. Rev. A* **92** 062337

[63] Ben-Or M, Horodecki M, Leung D W, Mayers D and Oppenheim J 2005 In: Kilian J (ed.): TCC 2005, LNCS 3378, p. 386

[64] Renner R and König R 2005 In: Kilian J (ed.): TCC 2005, LNCS 3378, p. 407

[65] Diamanti E and Leverrier A 2015 *Entropy* **17** 6072

[66] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **88** 022339

[67] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev. A* **87** 062313

[68] Qin H, Kumar R and Alléaume R 2013 In: Lewis K L, Hollins R C, Merlet T J, Gruneisen M T, Dusek M, Rarity J G and Carapezza E M (ed.): *Proceedings of SPIE* 8899*, Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X*, September 23, 2013, Dresden, Germany, 8990N

[69] Ma X C, Sun S H, Jiang M and Liang L M 2013 *Phys. Rev. A* **87** 052309

[70] Huang J Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2014 *Phys. Rev. A* **89** 032304

[71] Jouguet P and Kunz-Jacques S 2015 *Phys. Rev. A* **91** 022307.

[72] Qi B, Lougovski P, Pooser R, Grice W and Bobrek M 2015 *Phys. Rev. X* **5** 041009

[73] Soh D B S, Brif C, Coles P J, Lütkenhaus N, Camacho R M, Urayama J and Sarovar M 2015 *Phys. Rev. X* **5** 041010

[74] Huang D, Huang P, Lin D, Wang C and Zeng G H 2015 *Opt. Lett.* **40** 3695

[75] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501

[76] Marshall K and Weedbrook C 2014 *Phys. Rev. A* **90** 042311

[77] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[78] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319

[79] Zhou Y H, Yu Z W and Wang X B 2016 *Phys. Rev. A* **93** 042324

[80] Li Z, Zhang Y C, Xu F, Peng X and Guo H 2014 *Phys. Rev. A* **89** 052301

[81] Ma X C, Sun S H, Jiang M S, Gui M and Liang L M 2014 *Phys. Rev. A* **89** 042335

[82] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photon.* **9** 397

[83] Blandino R, Leverrier A, Barbieri M, Etesse J, Grangier P and Tualle-Brouri R 2012 *Phys. Rev. A* **86** 012327

[84] Fiurasek J and Cerf N J 2012 *Phys. Rev. A* **86** 060302

[85] Huang P, He G Q, Fang J and Zeng G H 2013 *Phys. Rev. A* **87** 012317

[86] Li Z Y, Zhang Y C, Wang X Y, Xu B J, Peng X and Guo H 2016 *Phys. Rev. A* **93** 012310

[87] Qi B, Zhu W, Qian L and Lo H K 2010 *New J. Phys.* **12** 103042

[88] Kumar R, Qin H and Alléaume R 2015 *New J. Phys.* **17** 043027

[89] Orieux A and Diamanti E 2016 *J. Opt.* **18** 083002

[90] Zhang L J, Silberhorn C and Walmsley I A 2008 *Phys. Rev. Lett.* **100** 110504

[91] Zhong T, Zhou H C, Horansky R D, Lee C, Verma V B, Lita A E, Restelli A, Bienfang J C, Mirin R P, Gerrits T, Nam S W, Marsili F, Shaw M D, Zhang Z S, Wang L G, Englund D, Wornell G W, Shapiro J H and Wong F N C 2015 *New J. Phys.* **17** 022002