ISSN: 0256-307X

中国物理快报
Chinese Physics Letters

Volume 30 Number 1 January 2013

A Series Journal of the Chinese Physical Society
Distributed by IOP Publishing

Online: http://iopscience.iop.org/0256-307X
http://cpl.iphy.ac.cn

CHINESE PHYSICAL SOCIETY
Institute of Physics PUBLISHING

CHIN. PHYS. LETT. Vol. 30, No. 1 (2013) 010305

Four-State Modulation Continuous Variable Quantum Key Distribution over a 30-km Fiber and Analysis of Excess Noise *

WANG Xu-Yang(王旭阳), BAI Zeng-Liang(白增亮), WANG Shao-Feng(王少锋), LI Yong-Min(李永民)**, PENG Kun-Chi(彭堃墀)

State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006

(Received 5 November 2012)

We report a fiber-based four-state discrete modulation continuous variable quantum key distribution system based on homodyne detection. A secret key rate of 1 kbit/s is achieved at a transmission distance of 30.2 km. Two factors that result in the excess noises of the quantum key distribution system are analyzed. The first is the relative phase dithering between the signal and local fields, and the second is the local field leakage into the signal field due to the scattering process that depolarizes the local field. It is found that the latter has a significant impact on the excess noise, which is the main limiting factor to the long-distance secure quantum transmission. Some protocols are also given to decrease the excess noise effectively.

PACS: 03.67.Dd, 03.67.Hk, 03.67.−a DOI: 10.1088/0256-307X/30/1/010305

Coherent-state continuous variable quantum key distribution (CVQKD) protocols based on quadratures of the quantized electromagnetic field have seen significant progress during the last decade. Various kinds of protocols have been proposed,[1−17] some of which have been implemented experimentally and field testing was also performed recently.[18−25] Compared with its counterpart discrete variable quantum key distribution (DVQKD), CVQKD has some technological advantages such as better efficiency of homodyne detection over single photon counting at the telecom wavelength.

To achieve a long-distance CVQKD, two approaches have been proposed. One is based on a discrete modulation technique which includes two-state and four-state protocols,[10,13] etc. Such protocols allow high reconciliation efficiency for SNR close to 0. Meanwhile, the corresponding modulation procedure is simpler than that of Gaussian modulation and thus more practical. The other is to build a good reconciliation code with high efficiency for a Gaussian modulation coherent state protocol at a low SNR and it is shown that a long distance of 120 km can be realized for reasonable physical parameters.[16] Recently, a 24-km fiber-based discretely signaled CVQKD system using the technique of reverse reconciliation and post-selection was reported, in which the security against the collective attack was guaranteed by quantum state tomography on a subset of Bob's data.[23] Experimental implementation of a no-switching discrete modulation protocol was also presented in free space.[22]

In this Letter, we present a fiber-based four state discrete modulation CVQKD system. It is found that the relative phase fluctuations between the signal and local fields, and local field leakage into the signal field due to the depolarized scattering process can cause a significant amount of excess noises, in particular the latter one, which degrades the performance of the long-distance quantum distribution significantly.

The unconditional security of the four-state protocol based on homodyne detection has been proved and the protocol can be briefly described as follows.[10] Alice prepares and sends randomly one of the four coherent states: $|\alpha\exp[i(2k+1)\pi/4]\rangle$ with $k\in\{0,1,2,3\}$ (here α is taken as a real number). The receiver Bob measures randomly one of the quadratures $\hat{X}$ or $\hat{P}$ and obtains his results. The sign of Bob's results encodes the bit of the raw key.

The experimental setup of the fiber-based four-state CVQKD is shown in Fig. 1.[19,21] The output beam of a continuous-wave 1550 nm single frequency fiber laser is modulated to 100-ns-wide pulses using the two cascaded high extinction ratio intensity modulators which are driven by a pulse generator at a repetition rate of 500 kHz. The optical pulses are divided into a strong local oscillator and a weak signal field by a 99/1 asymmetric fiber coupler. With variable attenuator and computer-driven intensity modulators and phase modulators, the coherent states can be prepared with random distribution in phase space as shown in Fig. 2. Through time multiplexing which is achieved by an 80 m fiber and polarization multiplexing realized by a PBS, the signal and local pulses are directed to a 30-km single mode fiber coil. After long-distance transmission the receiver Bob measures the quadrature amplitude or phase of the signal field randomly using a PHD. The phase modulator is used for randomly switching the measurement basis and locking the relative phase between the signal and local fields.

To facilitate the key transmission, the pulses are split into blocks. For the pulse repetition rate of 500 kHz/s, the time duration of each block is 100 ms, which is also the calibration time that we lock the relative phase between the local and signal fields. The

*Supported by the National Science Foundation of China (11074156), the TYAL, the National Basic Research Program of China (2010CB923101), the NSFC Project for Excellent Research Team (61121064), and the Shanxi Scholarship Council of China.

**Corresponding author. Email: yongmin@sxu.edu.cn

relative phase for each block can be determined in real time by using a portion of the block pulses. In order to synchronize the pulses between Alice and Bob accurately, the whole system shares one common clock source generated by a data acquisition module (NI, USB 6259) located on Alice's site. On Bob's site, a 50/50 coupler is used to extract half the beam to recover the clock. To ensure the peak value of the PHD output that can be acquired accurately, a delay box is connected to the recovered clock signal to generate the desired time delay.

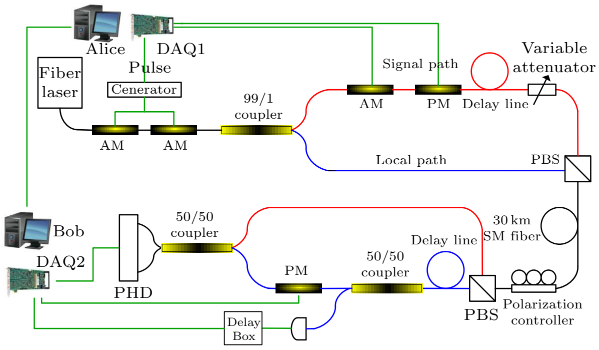

Fig. 1. The schematic diagram of the experimental setup. DAQ1, DAQ2, data acquisition module; AM, amplitude modulator; PM, phase modulator; SM, single mode; PHD, pulsed homodyne detector; PBS, polarizing beamsplitter.

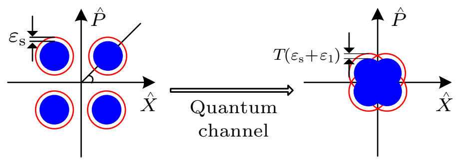

Fig. 2. Conceptual schematic of the four-state protocol in phase space. Here ε_s is the source noise generated by the modulation error, etc.; ε_1 is the channel noise due to the dithering of the relative phase and the depolarized scattering process of the local field, etc; T is the transmission efficiency of the channel.

In order to achieve a precise secret key rate, the parameters of the system are calibrated in detail. The losses at Alice's site do not affect the system performance because the signal level is set at Alice's output port. The transmission efficiency of the quantum channel (30.2 km single mode fiber) is 0.251. At Bob's site the transmission coefficient of the PBS is $\eta_1 = 89.5\%$. The detection efficiency of the pulse homodyne detector with the 50/50 coupler is $\eta_2 = 66\%$. Thus the total efficiency of Bob's setup is $\eta = \eta_1\eta_2 = 59.1\%$.

To find the optimum amplitude of the signal field,[10] we plot the secret key rate as a function of the signal field amplitude with different excess noises at the distance of 30 km, as shown in Fig. 3. It is clear that the optimum signal amplitude α remains almost unchanged for different excess noises. For a fixed excess noise, the corresponding curve is flat near the optimum amplitude point. In our experiment, the signal amplitude was adjusted to be around 0.45.

Assuming that the attenuation of the single mode fiber is constant and linear, the amplitude of the signal field sent by Alice can be determined from the measured signal amplitude at Bob's site. At this stage, the experimental excess noise can be determined. With the reconciliation efficiency $\beta = 80\%$ and the theoretical results in Refs. [10,12], the security key rate per pulse can be given for each 80 blocks, as shown in Fig. 4. For each of the three points, the corresponding excess noise is less than 0.01. The estimated secret key rate for our system can be as much as 1 kbit/s at the current pulse repetition rate of 500 kHz. It is found that there were fluctuations for the measured values of excess noise and sometimes the excess noise can exceed 0.02. There are several factors which can contribute to the excess noises, including the source noise, modulation error, finite size effect, and the dithering of the relative phase between the signal and local fields,[11,20,26] etc. Besides the above-mentioned factors, we find that leakage from the local field into the signal path due to the depolarized scattering process of the local field can also contribute to the excess noise. In the following, we will concentrate on the issues of relative phase fluctuations and local field leakage.

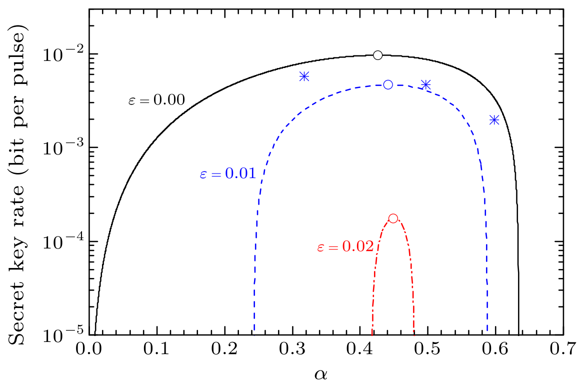

Fig. 3. The secret key rate per pulse for different single field amplitudes and excess noises. The circle marks the maximum value of each curve, the asterisks are the experimental results, α is the amplitude of the signal field.

The dithering of the relative phase is mainly due to the 80 m delay fiber. When we connect Alice's setup and Bob's setup directly without including the 80 m fiber and 30 km single mode fiber, the varying period of the relative phase between the signal and local fields is about 20–50 s. For a calibration period of 100 ms, we can lock the relative phase to be $\pm 0.54°$ (peak to peak value) using an active servo system. After inserting the 80 m fiber into the signal and local paths, the relative phase can be stabilized to be $\pm 1.98°$. The reason is that the varying period of the relative phase is now reduced to 2–5 s while the calibration period is still 100 ms, so performance of the locking servo system will degrade. After inserting the 30 km single mode fiber, the relative phase can be locked to $\pm 2.88°$. The contribution of the relative phase dithering to the excess noise can be estimated by a simple model.[20] Due to the phase variations, Bob's measurement basis will change from $\hat{X}$ to $\hat{X}'$ with $\hat{X}' = \hat{X}\cos\theta_0 + \hat{P}\sin\theta_0$; here θ_0 is the phase dithering centered on zero. The added excess noise can be given by $\langle(\Delta\hat{X}')^2\rangle - \langle(\Delta\hat{X})^2\rangle \approx \langle(\Delta\hat{P})^2\rangle\theta_0^2 = V_A\theta_0^2$, by employing the experimental value of $\theta = 2.88\pi/180$ and $V_A = 0.405$; the added excess noise is 0.001. As a result, due to the low signal modulation amplitude, the discrete modulation CVQKD protocol is quite robust against the phase locking noise. To improve the locking accuracy of the relative phase further, one can shorten the pulse width and increase the pulse repetition rate. By doing so the length of time-multiplexing fibers can be reduced and the varying period of the relative phase will increase accordingly, and at the same time the calibration period of the locking system can also be decreased effectively.

Due to the birefringence of the 30 km single mode fiber, the polarization state of the signal and local fields will drift slowly with the temperature.[27] Such drift can be solved by utilizing a dynamic polarization controller. Besides the low frequency drift, it is found that there also exist fast fluctuations of the polarization state of the local beam at frequency up to 40 kHz. Such fluctuations will lead to photon leakage from the local beam into the signal field and contribute to the excess noise.

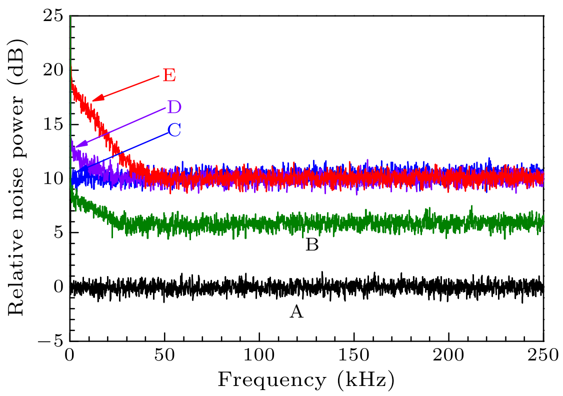

Fig. 4. The measured spectrum of PHD output for different lengths of single mode fibers when the signal path at Alice's setup is disconnected. A: electronic noise, B: 30 km fiber (local power: 1.89×10^6 photons per local pulse), C: 1 m fiber, D: 10 km fiber, E: 30 km fiber; the local power for C, D and E is 5.7×10^6 photons per local pulse.

To analyze the above photon leakage effect, we disconnect the signal path at Alice's setup and analyze the spectrum of PHD output for different lengths of single mode fibers (1 m, 10 km and 30 km), as shown in Fig. 4. It is clear that the added excess noise is directly proportional to the fiber length and the power of the local field. For the 1-m-long fiber, the measured spectrum is fairly flat and it is identical to the spectrum of the vacuum field which is measured by disconnecting the signal path at Bob's setup. When longer single mode fibers (10 km and 30 km) are employed, a noise peak centered on zero frequency appears on the noise spectrum. This means that the signal field is not a vacuum field now and some depolarized local light is leaked into the signal path. Such leakage is most probably attributed to the depolarized Rayleigh scattering process.[28] When the local power is such that the PHD has a 10 dB shot noise to electronic noise ratio (the photons per local pulse is around 5.7×10^6), the introduced excess noise can be above the level of 0.01. In our current setup, by decreasing the local beam's power to the level that the ratio of shot noise to electronic noise is around 6 dB (the photons per local pulse is around 1.89×10^6), the excess noise can be reduced to the level of 0.005.

To realize a long-distance secure quantum transmission, the scattering process analyzed above must be taken into account and two approaches can be pursued to decrease the influence of such noise. Firstly, one can improve the extinction ratio of optical pulses. Secondly, a high shot noise to electronic noise ratio PHD with ultra-low electronic noise can be designed and utilized, in this case, the system can operate at a lower local power level and the unwanted leakage can be suppressed effectively.

In summary, a fiber based four-state discrete modulation continuous variable quantum key distribution system has been demonstrated. A secret key rate of 1 kbit/s is achieved at a transmission distance of 30.2 km. Various factors that lead to the excess noises are analyzed, with emphasis on the influence of the relative phase fluctuations and local field scattering process. Lastly, some approaches are proposed to reduce the excess noises due to the scattering process.

References

[1] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[2] Grosshans F and Grangier P 2002 arXiv:quant-ph/0204127v1
[3] Grosshans F and Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905
[4] Weedbrook C et al 2004 *Phys. Rev. Lett.* **93** 170504
[5] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504
[6] Navascues M and Acin A 2005 *Phys. Rev. Lett.* **94** 020505
[7] Navascues M, Grosshans F and Acin A 2006 *Phys. Rev. Lett.* **97** 190502
[8] Patron R G and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[9] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[10] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[11] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev.* A **81** 062343
[12] Leverrier A and Grangier P 2010 arXiv:1002.4083v1[quant-ph]
[13] Becir A, El-Orany F A A and Wahiddin M R B 2012 *Int. J. Quantum Inf.* **10** 1250004
[14] Leverrier A and Grangier P 2011 *Phys. Rev.* A **83** 042312
[15] Shen Y J et al 2011 *Phys. Rev.* A **83** 052304
[16] Jouguet P, Jacques S K and Leverrier A 2011 *Phys. Rev.* A **84** 062317
[17] Yang J et al 2012 *Phys. Rev.* A **85** 052302
[18] Grosshans F et al 2003 *Nature* **421** 238
[19] Lodewyck J et al 2007 *Phys. Rev.* A **76** 042305
[20] Qi B et al 2007 *Phys. Rev.* A **76** 052323
[21] Fossier S et al 2009 *New J. Phys.* **11** 045023
[22] Shen Y et al 2010 *Phys. Rev.* A **82** 022317
[23] Xuan Q D, Zhang Z S and Voss P L 2009 *Opt. Express* **17** 24244
[24] Wittmann C et al 2010 *Opt. Express* **18** 4499
[25] Dai W C et al 2011 *Sci. Chin. Inf. Sci.* **54** 2578
[26] Lodewyck J et al 2005 *Phys. Rev.* A **72** 050303(R)
[27] Vanwiggeren G D and Roy R 1999 *Appl. Opt.* **38** 3888
[28] Zhu T et al 2010 *Opt. Express* **18** 22958

Chinese Physics Letters

Volume 30 Number 1 January 2013

GENERAL

THE PHYSICS OF ELEMENTARY PARTICLES AND FIELDS

NUCLEAR PHYSICS

ATOMIC AND MOLECULAR PHYSICS

CONDENSED MATTER: ELECTRONIC STRUCTURE, ELECTRICAL, MAGNETIC, AND OPTICAL PROPERTIES

CROSS-DISCIPLINARY PHYSICS AND RELATED AREAS OF SCIENCE AND TECHNOLOGY

GEOPHYSICS, ASTRONOMY, AND ASTROPHYSICS