

ZENG He-ping, WU Guang, WU E.,
PAN Hai-feng, ZHOU Chun-yuan,
F. Treussart, J.-F. Roch

Generation and Detection of Infrared Single Photons and their Applications

© Higher Education Press and Springer-Verlag 2006

Abstract Unbreakable secret communication has been a dream from ancient time. It is quantum physics that gives us hope to turn this wizardly dream into reality. The rapid development of quantum cryptography may put an end to the history of eavesdropping. This will be largely due to the advanced techniques related to single quanta, especially infrared single photons. In this paper, we report on our research works on single-photon control for quantum cryptography, ranging from single-photon generation to single-photon detection and their applications.

Keywords single-photon emitter, single-photon detector, quantum key distribution

PACS numbers 03.67.Hk, 03.67.Dd, 03.67.-a, 42.50-p

1 Introduction

The competition between code makers and code breakers has been a neck-and-neck race until the brilliant invention of quantum key distribution (QKD) was proposed. Now, under the great power of quantum mechanics, absolutely secure telecommunication is no longer a dream, and the code breakers may lose their jobs forever. Such an advanced research field has attracted considerable interests from all around the world. In China, the research of QKD was started only in the early 1990s, and demonstrations of

QKD using B92 and BB84 were separately carried out by groups in the East China Normal University (ECNU) and the Chinese Academy of Science. The first long-distance fibre-based QKD test-bed system in China was realized by ECNU in 2003 [2]. Recently, researchers in the University of Science and Technology of China have reported the longest fibre-optic QKD experiment in the world [3]. However, there still exist some challenges on single-photon control to eventually put this technique in practical use. The most challenging techniques that need to be developed include the generation of single photons on demands and efficient single-photon detection at telecom wavelengths. In this article, we review our recent progress on single-photon generation, detection and control and their application in the QKD experiments.

2 Single-photon emission from colour centres in diamond

The security of the QKD system is partly dependent on the single-photon source due to the principle of quantum mechanics that one cannot duplicate an unknown state of single quantum system without disturbing it [1]. From this point, the generation of single photons on demand is one of the important targets in QKD [4–6]. Emission from a single dipole can be considered as an efficient triggered single-photon source [7], because a single dipole has to undergo a full cycle of excitation, emission and re-excitation between the emission of two consecutive single photons. Consequently, a sufficiently short and intense excitation pulse will permit the single dipole to emit only one photon within one excitation pulse.

Single defects in diamond stand out as one of the promising candidates among different kinds of solid-state single-photon sources due to their unsurpassed efficiency and photostability. Among them, nitrogen–vacancy (NV) colour centre is well known as an optically active defect in diamond [8–11]. Consisting of a substitutional nitrogen atom (N) and a vacancy (V) in an adjacent lattice site, NV colour centres emit around 670 nm with a zero-phonon line

ZENG He-ping (✉), WU Guang, WU E.,
PAN Hai-feng, ZHOU Chun-yuan
Key Laboratory of Optical
and Magnetic Resonance Spectroscopy,
and Department of Physics,
East China Normal University,
Shanghai 200062, China
E-mail: hpzeng@phy.ecnu.edu.cn

WU E., F. Treussart, J.-F. Roch
Laboratoire de Photonique Quantique et Moléculaire,
UMR CNRS 8537, ENS Cachan,
61 avenue du Président Wilson,
94235 Cachan Cedex, France

(ZPL) at 637 nm. However, it is difficult to efficiently extract the emitted photons from bulk diamond because of the high refraction index of the material ($n = 2.4$). Refraction at the sample–air interface leads to a small collection of solid angle limited by total internal refraction and to optical aberrations. An efficient way to circumvent these problems is to use diamond nanocrystals containing NV centres, with a size much smaller than the radiated light wavelength [12,13]. Refraction becomes irrelevant, and the colour centre can simply be assimilated to a point source radiating at the air–sample interface. Moreover, the small volume of diamond excited by the pumping laser yields lower background light than the one from the bulk diamond sample. Such property is of crucial importance for single-photon emission, since residual background light will contribute to a non-vanishing probability of having more than one photon within the emitted light pulse.

A reliable triggered single-photon source was recently built, based on the pulsed, optically excited photoluminescence of a single NV colour centre in a diamond nanocrystal [14]. This single-photon source was applied to the observation of single-photon wavefront-splitting interferences [15] and to the realization of open-air QKD experiments [5,16]. However, in the second application, broadband emission of the NV colour centre [full width at half-maximum (FWHM) ≈ 70 nm at room temperature] precludes daylight operation of the QKD set-up due to difficulties in filtering the transmitted single photons from daylight background.

Lately, the nickel–nitrogen NE8 defects in the diamond provoke researchers’ interest for their intense narrow near-infrared emission band [17,18]. We also reported the observation on similar diamond colour centres tentatively ascribed to nickel–nitrogen impurities as well [19]. Photoluminescence of these single emitters shows perfect photostability at room temperature. Compared to NV colour centre emission, it has several remarkable properties. First, the narrow emission band around 780 nm is almost entirely

concentrated in a ZPL even at room temperature. Second, the short photon emission lifetime lasts about 2 ns. Third, photoluminescence from the single defect is measured to be linearly polarized.

We have studied such narrow emitters in natural diamond wafer using a conventional scanning confocal microscope [see Fig. 1(a)] to select single defects in the sample. This set-up has been described in detail elsewhere [14,19]. For each isolated emitter, we simultaneously record the spectrum of the emitted light and the histogram of time delays between the consecutively detected photons in order to identify whether it is a single emitter through antibunching effect. Figure 1(b) shows the spectrum of the light from such an emitter. The narrow peak at 782 nm (about 2 nm FWHM) corresponds to the ZPL of what we suppose to be nickel–nitrogen-related impurities [20,21], and the sharp peak at 757 nm is the one-phonon Raman scattering line of the diamond lattice ($1\,332\text{ cm}^{-1}$) associated to the 687 nm excitation wavelength. Note the remarkable property that photoluminescence is concentrated in the ZPL even at room temperature. The ZPL-integrated intensity corresponds to 68% of the full spectrum area, a value much higher than that of NV colour centre.

The histogram of time delays is recorded with the HBT set-up after filtering of the ZPL with a narrow band-pass filter having its inclination relative to the beam normal incidence tuned for maximal transmission. Since the signal-to-background ratio is quite large (60:1), we neglect the residual background light effect on the $g^{(2)}$ measurement. Figure 2(a) shows the intensity autocorrelation function $g^{(2)}(\tau)$ of the light from the same emitter as the one studied in Fig. 1(b). A clear dip of the autocorrelation function is observed at zero delay with $g^{(2)}(0) = 0.12$, proving that we address a single emitter. However, the non-zero $g^{(2)}(0)$ value cannot be attributed to background Poissonian light, the intensity of which is negligible owing to very high signal-to-background ratio. This residual value is indeed due to the

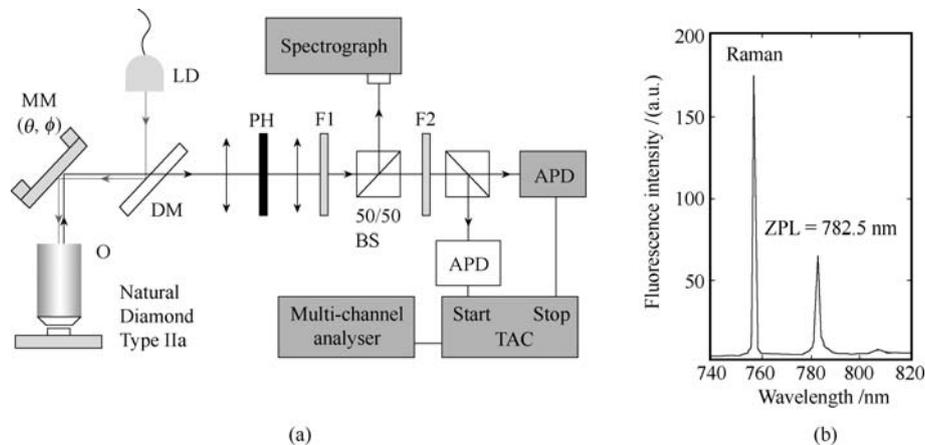


Fig. 1 (a) Experimental set-up. *LD* Laser diode emitting at 687 nm, *MM* mobile mirror fixed on a piezoelectric transducer providing orthogonal angular displacements, *O* microscope objective (NA = 0.95, $\times 100$), *DM* dichroic mirror, *PH* pinhole (100- μm diameter), *F1* interference filter transmitting $\lambda > 740$ nm and removing the remaining light at the excitation wavelength, *BS* non-polarized beam

splitter, *F2* band-pass filter (FWHM ≈ 10 nm), *APD* silicon avalanche photodiode in photon counting regime, *TAC* time-to-amplitude converter. (b) Photoluminescence spectrum from a single nickel–nitrogen impurity in the diamond sample. The sharp intense line at a wavelength of 757 nm corresponds to the one phonon Raman scattering of the diamond matrix for excitation at 687 nm

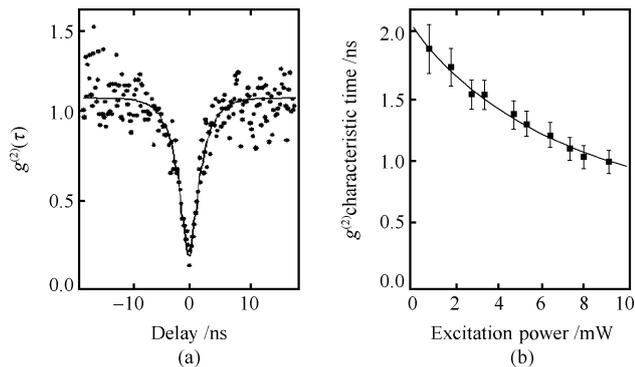


Fig. 2 (a) Normalized correlation function $g^{(2)}(\tau)$ measured with CW excitation power of 0.68 mW. The experimental data are shown as *dots*, whereas the *solid line* represents a fit by a convolution of a symmetrical exponential function (characteristic time τ_c) with IRF. (b) Characteristic time τ_c of the $g^{(2)}$ function for various excitation powers. *Solid line*: fit in the framework of a three-level model. Extrapolated value of the fit at zero pump power yields the excited-state lifetime of about 2 ns

detection set-up time instrumental response function (IRF) with a characteristic time 0.7 ns FWHM. Taking into account this finite time response, the measured autocorrelation function can be well fitted by the convolution of the IRF with a $g^{(2)}(\tau)$ function going perfectly to zero at $\tau = 0$ and modelled by a symmetrical exponential function in the framework of a three-level model [see Fig. 2(a)] [10]. Note that the value of $g^{(2)}(\tau)$ higher than unity at delays larger than about 10 ns is due to the leakage of the system towards a dark metastable state, inducing photon bunching at the corresponding time scale. In order to determine the intrinsic excited-state lifetime of the single defect, we measured the characteristic time of the $g^{(2)}$ on short time scale and at different excitation powers. Fit of this time in the framework of a three-level model yields a value of the excited-state lifetime of the single colour centre of about 2 ns, obtained by extrapolating the fit at zero excitation power [Fig. 2(b)].

We also investigated the polarization properties of the single colour centre relative to absorption and emission of light. We monitored the photoluminescence intensity while rotating the excitation laser linear polarization angle. The polarization contrast of 96% proves that the single colour centre behaves like a dipole relative to absorption of light. Using quarter wave plate method, we studied the emitted light polarization properties and observed that light is perfectly elliptically polarized with an aspect ratio of 0.25. This measurement indicates that the single defect also behaves like an emitting dipole. The linear polarized light becomes elliptical after propagation through optics including high numerical aperture objective and dichroic mirror, both known for modifying the polarization state of light.

Let us finally point out that the single colour defect is a quite strong emitter. For the maximum available excitation power of 9 mW, an overall counting rate of about 80 000 counts/s is obtained corresponding to an excited-state population occupancy of about 60%.

In this section, we summarize our experimental studies on photoluminescence properties at the single emitter level

of optically active colour centres based on supposedly nickel–nitrogen impurities in natural diamond samples. Under CW excitation at room temperature, these colour centres reveal a narrow-band emission around 782 nm, a short photon emission lifetime of 2 ns and a fully polarized photoluminescence. Thanks to this narrow spectral emission, it will be easy to pick up the useful photoluminescence while removing stray light. Thanks to short photon emission lifetime, the implementation of the single-photon source in QKD set-up will be compatible with narrow time-window analysis. This will limit the effect of photodetection dark counts and will lead to an increase in the limit of propagation distance compatible with perfectly secure communications [16,22]. We can also take advantage of the perfectly polarized light, which can easily be turned into linear polarization with a properly oriented quarter wave plate, virtually without any loss. Finally, note that the emission wavelength of the single emitter is in an open-air and a telecom optical fibre communication windows.

With all of those striking features, the colour centres based on diamond nickel–nitrogen impurity appear to be very good candidates for realizing a stable triggered single-photon source at room temperature for an efficient and practical open-air QKD system.

3 Efficient non-linear control of single photons

Recent progress in non-linear optics has enabled frequency upconversion at single-photon level with complete quantum conversion [23], which makes use of sum-frequency mixing of 1.55 μm single photon with a strong pump laser in either an external cavity or a non-linear waveguide to generate single-photon replica in the visible or near-infrared (VIS–NIR) region [24,25]. This technique facilitates many novel applications not only in quantum optics, such as quantum interface to transfer quantum entanglement [26], linear-optics quantum gates [27], single-photon polarization switch [28] and non-linear control of single photons [29], but also in many traditional areas, such as classical optical communication, imaging, photobiology and astronomy. In particular, quantum conversion in sum-frequency generation makes it possible to detect 1.55- μm single photons efficiently by counting its upconverted replica in the VIS–NIR region, where commercially available high-performance Si-APD single-photon counting module (SPCM) can be used. This consequently allows the experimental implementation of long-distance QKD to take full advantages of both the excellent characteristics of Si-APD SPCM and the inherently low transmission loss of optical fibres at 1.55 μm (≈ 0.2 dB/km) [30,31]. As limited by current immature InGaAs avalanche photodiodes (APDs), InGaAs APD-based single-photon counting at telecom wavelengths exhibits very poor performance and sets a troublesome bottleneck for many applications. For instance, single-photon detection efficiencies at 1.55 μm are generally in the 10%–15% range, and InGaAs APDs are unsuitable for continuous-wave detection due to severe after-pulsing. In contrast, single-photon counting in the

VIS–NIR region has already become a close-to-mature technique by use of the commercially available Si-APD SPCM with excellent performance such as high quantum efficiencies ($>70\%$) with extremely low dark count rates and the possibility of continuous-wave operation at rates as high as tens of megahertz [32]. Frequency upconverted counting of $1.55\ \mu\text{m}$ single photons can take full advantages of the sophisticated Si-APD SPCM by means of efficient upconversion from $1.55\ \mu\text{m}$ to VIS–NIR, which offers significant improvements over existing InGaAs photon counters: continuous-wave operation, higher detection efficiency, higher counting rates and negligible afterpulsing.

Frequency upconversion of $1.55\ \mu\text{m}$ single photons has been demonstrated by sum-frequency mixing with a strong pump laser at $1.064\ \mu\text{m}$ in a bulk periodically poled lithium niobate (PPLN) and PPLN waveguide. The bulk PPLN scheme requires a resonant pump cavity to enhance circulating pump power, and a highly stable cavity lock should be included in the experimental implementation. In practice, the cavity lock can only be maintained stably within minutes, and high circulating power may cause the servo less stable [24]. The PPLN waveguide scheme requires subtle processes to prepare a monolithic fibre-pigtailed PPLN waveguide with a reasonably low insertion loss. Also, high pump intensity due to tight mode confinement in the waveguide may bring about some undesired non-linear processes that cause spurious counting [33]. We demonstrate stable and efficient single-photon counting at $1.55\ \mu\text{m}$ by means of intracavity sum-frequency mixing in a bulk PPLN placed inside a diode-pumped Nd:YVO₄ laser. The intracavity frequency upconversion offers advantages over external-cavity ones such as long-term stability without the requirements of sensitive cavity lock,

ease of operation, suppression of spurious non-linear processes and the possibility to combine the whole system as a simple, stable and robust SPCM.

The experimental realization is schematically shown in Fig. 3. The upconversion system was based on a solid-state Nd:YVO₄ laser at $1\ 064\ \text{nm}$ pumped by a fibre-coupled 808-nm laser diode (LD). The PPLN chip used in the experiment was housed in an oven and temperature controlled with a fluctuation less than 0.1°C , which had multiple grating periods varying from 11.0 to $12.0\ \mu\text{m}$ with $0.2\ \mu\text{m}$ per step, allowing temperature-controlled quasi phase matching of sum-frequency generation in a broad spectrum with a temperature coefficient of about $0.18\ \text{nm}/^\circ\text{C}$. The arrangement of laser cavity was optimized for mode matching between the intracavity pump and input signal beams. Sum-frequency mixing of $1.55\ \mu\text{m}$ single-photon signal with the $1\ 064\ \text{nm}$ intracavity pump took place during one pass of the input signal in the PPLN crystal, which generated 631-nm single-photon replica.

Under continuous-wave pump, photorefractive effects within PPLN may cause instability of the intracavity laser. In principle, it is possible to operate a PPLN chip at an elevated temperature to avoid the photorefractive problem. We experimentally investigated the influence from photorefractive effects by comparing the intracavity sum-frequency mixing in PPLN channels with grating periods of 11.4 and $11.2\ \mu\text{m}$. The corresponding quasi phase-matching temperatures for the maximal conversion efficiency are near 108.2 and 180.5°C , respectively. In the $11.4\ \mu\text{m}$ PPLN channel operated for quasi phase matching at a low temperature of 108.2°C , the intracavity pump and frequency-upconverted output fluctuated (the standard deviation of the output power at $1\ 064\ \text{nm}$ was measured as 3.73%) mainly due to photorefractive effects. In

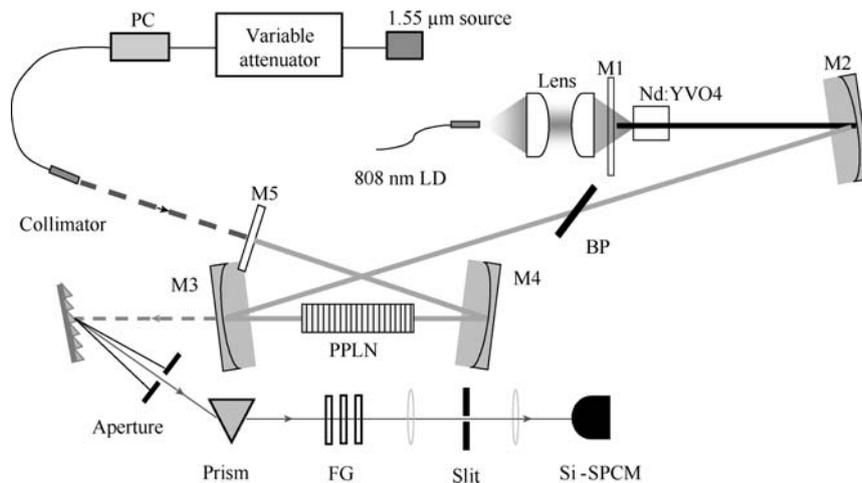


Fig. 3 The schematic of our experimental set-up for intracavity single-photon upconversion. The cavity is composed of five mirrors M1–M5, which is well designed according to the ABCD matrix and mechanical permissibility. The pump mirror M1 is a flat mirror with antireflection coating at $808\ \text{nm}$ on both surfaces and high-reflection coating at $1.06\ \mu\text{m}$ on the inner surface. M2 is a concave mirror with radius-of-curvature of $500\ \text{mm}$, high-reflection coated at $1.06\ \mu\text{m}$ and antireflection coated at $808\ \text{nm}$ to minimize the unexpected background noise from the LD emission. M3 and M4 are concave

mirrors with radius-of-curvature of $300\ \text{mm}$ and high-reflection coating at $1.06\ \mu\text{m}$. M3 is also high-transmission coated at $631\ \text{nm}$ on both sides to output the upconverted signal. The end mirror M5 is a 98% output coupler at $1.06\ \mu\text{m}$. A PPLN is placed inside the laser cavity between the concave mirrors M3 and M4. A fused silicon plate is inserted between M2 and M3 at the Brewster angle to adjust the polarization of the intracavity beam. BP Brewster plate, PC fibre polarization controller, FG filters group

contrast, the 11.2 μm PPLN channel showed a better stability at a working temperature near 180.5°C. The standard deviation of the output laser power was less than 2%, as shown in Fig. 4. As a result, the 11.2 μm channel was finally chosen in our experiments to achieve frequency-upconverted single-photon counting.

For experimental convenience, we firstly optimized the intracavity frequency upconversion with a weak input probe of 0.55 mW. We measured the output power of the upconverted beam at 631 nm as a function of the intracavity pump power. As shown in Fig. 5, a maximum output power of 1.0 mW was obtained at the strongest pump power. We noted that the working temperature of the PPLN bulk should be set a little lower to compensate for the heating effect of the strong pump field when the pump field intensity increased. The highest upconversion efficiency of the weak probe was about 74.0%, and the working temperature dropped to 179.2°C. Due to the high stability of the intracavity laser field at 1,064 nm, the intensity of the output field was very stable in several hours. As the probe field was strong enough, no evident background noise was found at the power meter. The red output also functioned as the alignment reference of the filter system in the coming processes.

When the intensity of the input probe was attenuated to 1.1 photons/ μs , the single-photon counting of the output signal was demonstrated by using a Si-SPCM with the dark count rate less than 200/s. In order to filter the accompanying beams, the upconverted output beam was steered to pass through the filter system that includes a grating, a Brewster-angle prism, a group of filter plates and a variable slit. The total transmission of the signal was about 44%. Then, the signal at 631 nm was collected and reached the sensitive area of the Si-SPCM whose quantum efficiency at this wavelength approached 64%. Figure 6 exhibits the single-photon upconversion efficiency and background noise as functions of the pump power. At the peak of the pump intensity, the upconversion efficiency reached 74.3%, whereas the background noise was no

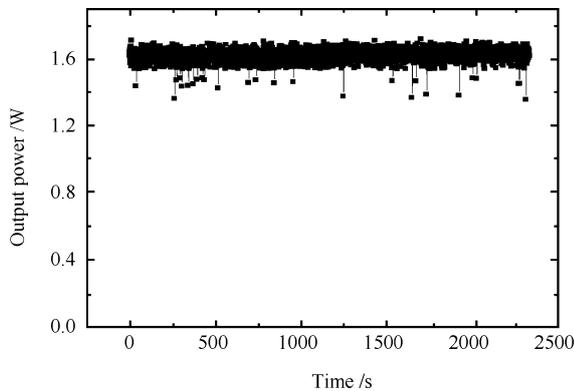


Fig. 4 The stability of the Nd:YVO4 laser output power with the insertion of the bulk PPLN. The output laser power is stable over tens of minutes. In the case of an output laser power around 1.61 W, the standard deviation is less than 2% as the PPLN is temperature-controlled at 179.2°C

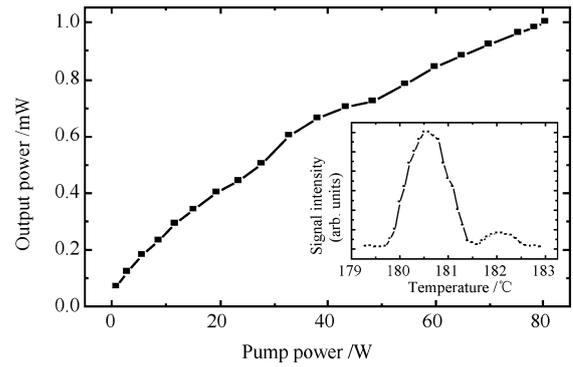
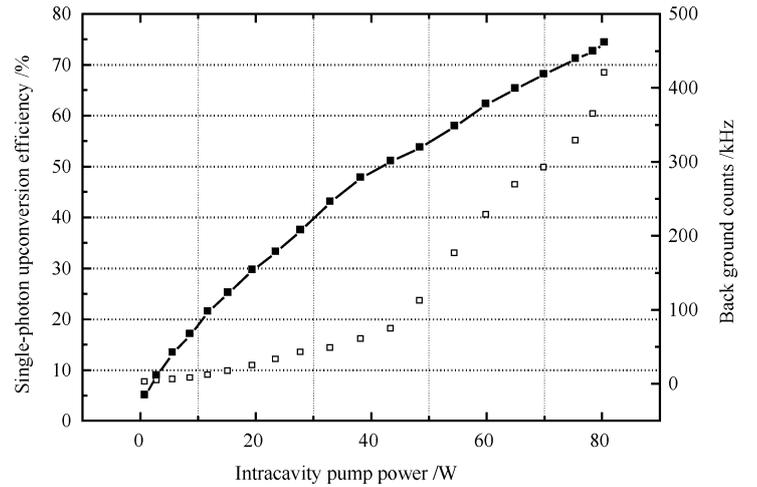


Fig. 5 The output power at 631 nm is shown as a function of the LD pump power, when the power of the input probe at 1 550 nm was 0.55 mW. *Inset:* the converted signal intensity curve depends on the working temperature of the PPLN crystal

more than $4.20 \times 10^5/\text{s}$. The efficiency is mainly limited by the intensity of the pump field and is slightly reduced by the mode mismatching of the two input fields. The background noise mainly composed of the following factors: the SHG of the pump field, the 1 064 nm laser, the emission of 808 nm LD and, most importantly, the fluorescence induced by the strong pump. After passing through the filter system, the background noise counts were basically caused by the fluorescence, which was of the same wavelength as the output signal. The stability of the counting rate here was almost the same as in the status of the weak probe input.

The advantages of intracavity single-photon frequency upconversion over the external cavity pump scheme include its long-term stability and no requirements of sensitive cavity lock. In order to explore further the potential of intracavity single-photon upconversion for practical applications, some useful improvements of our experiments are worthy of discussions. Firstly, comparing with the bulk PPLN, the MgO- or ZnO-doped PPLN crystals are more advanced because of their lower photorefractive effect and infrared absorption [34]. The promotions of the pump intensity and the conversion stability can be explored by using the PP-MgO:LN chip instead of the bulk PPLN. Secondly, we consider that if the pump beam is of smaller photon energy than the input probe, the non-linear processes that produce the fluorescence as the background noise will be sufficiently suppressed. The pump sources whose operating wavelength is beyond 1.55 μm can be performed by some other solid-state lasers or stimulated Raman lasers [35,36], both of which are able to be conveniently employed in our system. Furthermore, because the intracavity field is easily actively modulated to operate in pulsed mode (Q-switching or mode locking), our system can be used to upconvert the input probe with the pulsed pump field of extremely high peak intensity. In that case, some standard non-linear crystals, such as BiB_3O_6 , $\beta\text{-BaB}_2\text{O}_4$ and LiB_3O_5 , can be used for single-photon frequency upconversion. At last, the competition of the intracavity longitudinal modes oscillating is considered to induce the slight instability of the pump field as well as

Fig. 6 The dependence of single-photon upconversion efficiency (*diamonds*) and the background noise (*open squares*) upon the intracavity pump power



the upconversion efficiency. The instability could be further minimized by suppressing the multilongitudinal-mode oscillation with a unidirectional ring laser or twisted-mode-cavity laser [37,38].

4 High-performance single-photon counting at 1.55 μm

In Section 3, we have demonstrated a promising technique of upconverted single-photon detection. However, for the current research of optic-fibre QKD, InGaAs/InP APD is still the commonly used device for high-performance single-photon counting at 1.55 μm . In order to minimize the deleterious influence of dark counts, InGaAs/InP APD typically works in a gated mode with a reverse bias above the breakdown voltage, consisting of a short-pulse gate and a DC bias. The avalanche gain of the APD and the single-photon detection efficiency (η) can be increased by applying a high reverse bias, which nevertheless causes an increment of dark-count probability (P_{dark}). Dark counts can be reduced by operating APDs with very short gates at the optimized temperatures. However, short pulses used in the gated-mode detection produce strong spikes, which obscure the avalanche signals. In order to improve the ratio P_{dark}/η , we devised a robust and simple spike-cancellation method to get high-quality balanced avalanche signals on the basis of automatic cancellation of spikes with a transformer, by which common-mode inputs from an InGaAs/InP APD and a complementary capacitor are balanced in the magic-T network. The spike cancellation supports accurate discrimination of avalanche signals at a low threshold without affecting the detection efficiency. The spike-cancellation single-photon detection at the optimized temperature eventually produces a ratio $P_{\text{dark}}/\eta \approx 1.7 \times 10^{-6}$. By using such high-performance single-photon detectors, a “plug and play” (P&P) single-photon routing has been realized in 155-km optical fibres with the average photon number $\langle n \rangle = 0.1$ per pulse and a fringe contrast of 87% [41–44].

Figure 7 is the schematic diagram of short-pulse gated single-photon detectors with balanced outputs by using transformer-based spike cancellation. The essential part for

spike cancellation is the electronic circuit using a so-called magic-T network that is actually a self-winded transformer. An InGaAs/InP APD is connected in parallel with a normal diode of a comparable capacitance. The junction capacitance of the diode produces an imitative spike of the APD. The transients from the APD and diode are directed to the 0 and π inputs of the magic-T network. The first part of the transformer is used to distil differential signals so that the two spikes from the diode and APD cancel each other, and the avalanche is left through. The remaining part of the transformer is a balance/unbalance converter and serves as an impedance-matching device. At the output port of the transformer, the differential output signal is obtained. The transformer is designed for weak signals up to 500 MHz bandwidth. As the common mode, spikes from the APD and diode are balanced at the output. Experimentally, we set the APD and the diode IN4148 in a liquid nitrogen thermostat with a temperature controller. Two 75 Ω resistors are connected symmetrically in series to the electronic ground. Short-gate pulse of 7 Vpp and 2.2 ns FWHM are applied to the APD and IN4148 after being combined with the DC bias voltage by Bias-Tees, which unavoidably induce spike signals. Owing to cancellation of

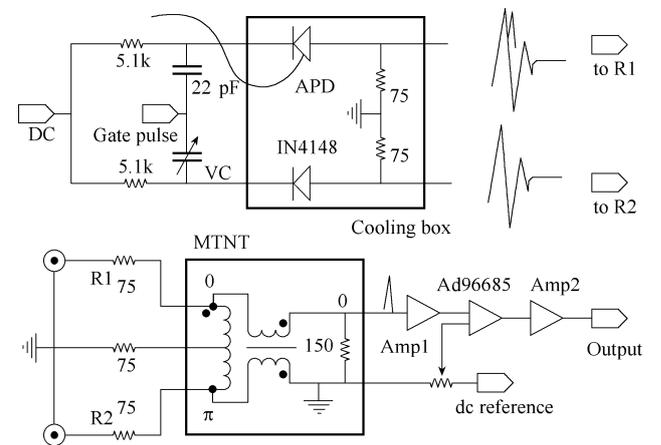


Fig. 7 The schematic diagram of the spike-cancellation single-photon detector, where AMP1 and AMP2 are two high-speed amplifiers

common-mode inputs in the 180° magic-T network based on transformer (MTNT), only the differential signals (avalanche signals) are induced at the asymmetrically single output.

The avalanche signals are double amplified by AMP1 and are then transmitted to a discriminator AD96685. Finally, the output signals of AD96685 are transmitted to a photon counter (Stanford SR400) after differential amplification by AMP2. We can set the threshold of AD96685 within 30–140 mV to discriminate the avalanche signals accurately and faithfully, avoiding any disturbances of spikes. Figure 8 shows the waveforms of spike cancellation in MTNT. Figure 8(a) represents the spike-cancelled signal with no avalanches, whereas Fig. 8(b) shows the avalanche signals after spike cancellation. It is clear that the original ~ 80 mV spikes are efficiently suppressed. It is difficult, in practice, to match exactly the junction capacitances of the APD and IN4148: the spike signals may differ a little, resulting in a small residue of common-mode signals. However, these differences can be compensated by adjusting their Bias-Tees. As a consequence, spike noises can be almost completely cancelled, whereas the avalanche signals are not affected.

In the demonstration, we used commercial InGaAs/InP APDs from JDS Uniphase (JDSU EXT 40-X00408052) to construct our single-photon detectors. Several researchers have already tested the commercial APDs, and high performance of single-photon detection at $1.55 \mu\text{m}$ has been achieved [39–41,45,46]. We at first connected single-mode fibre pigtails for the JDSU EXT 40-X00408052 APDs, and then placed the APD with IN4148 and two resistors in the thermostat carefully to avoid bending the fibre. Moreover, the temperature was controlled from 138.0 to 268.0 K with ± 0.1 K precision. First, we measured the temperature dependence of P_{dark}/η . At each temperature point, we adjusted the DC bias to set η around 20% and accumulated 10^8 counts to minimize the fluctuation of P_{dark} . Figure 3 depicts the curve of P_{dark}/η as the operation temperature varying from 143.0 to 263.0 K. P_{dark}/η shows a tendency to decrease with the operation temperature. It reaches the lowest value of $P_{\text{dark}}/\eta = 1.4 \times 10^{-6}/\text{pulse}$ at

Fig. 8 The waveforms of spike cancellation. (a) Spike cancellation without avalanche signals in the APD; (b) spike cancellation with avalanche in the APD. Dotted, dashed and solid lines denote signals from the APD, IN4148 and output of MTNT, respectively

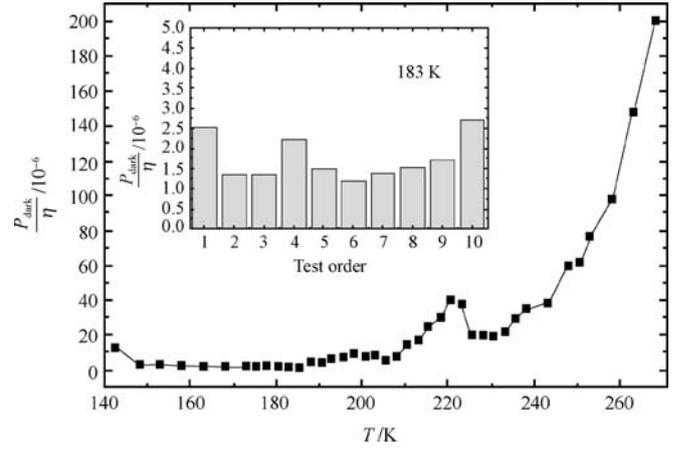
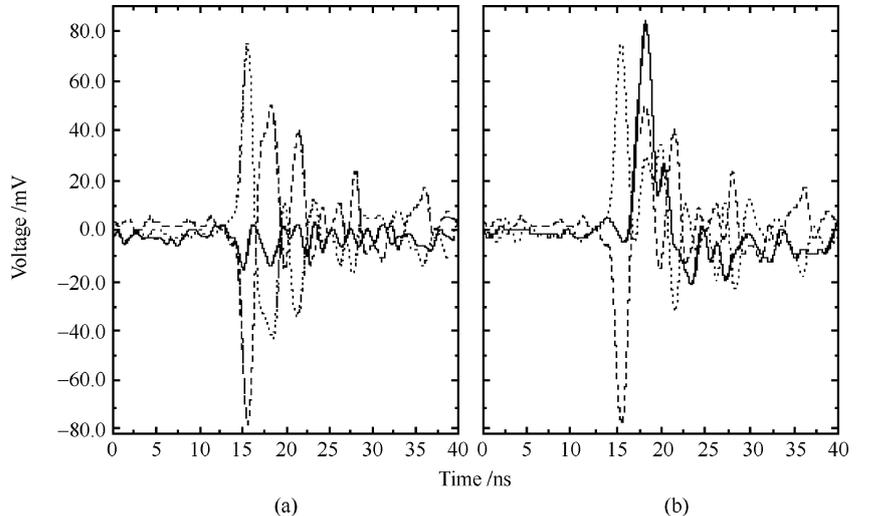


Fig. 9 The ratio P_{dark}/η with the operation temperature varying from 148.0 to 268 K, and the inset is the repetition measurement at 183 K

183 K and does not decrease further even when the temperature goes down below 183.0 K. According to [47], we believe that the breakdown voltage of the APD operated below 183.0 K is close to the reach-through voltage, and that the carrier pileup cannot be neglected. To affirm the accuracy and repeatability of the measurement, we have tested the value at 183.0 K for ten times of the measurements during a period of 3 months.

The inset of Fig. 9 shows the measurement results; half of the measurements give the results of $P_{\text{dark}}/\eta < 1.5 \times 10^{-6}$, and the average value is $P_{\text{dark}}/\eta = 1.7 \times 10^{-6}$. We measured the relation between P_{dark} and η at the operation temperature of 183.0, 205.5, 228.0 and 248.0 K by changing the DC bias voltage. As shown in Fig. 10, when the APDs work in the Geiger mode, P_{dark} and η increase with DC voltage within a certain range. It is convenient to change the P_{dark} and η by adjusting the DC bias. It is well known that an APD operated in the gated-mode possesses a decreasing ratio P_{dark}/η as the gate width decreases. In the experiments, we measured P_{dark}/η with a fixed gate width of 2.2 ns. It was proved that the spike cancellation was

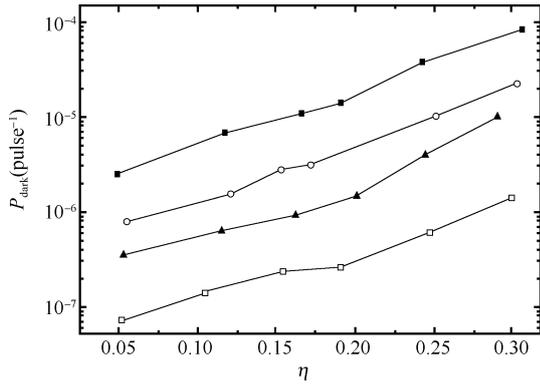


Fig. 10 The dark-count probability P_{dark} vs the detection efficiency η , where *square*, *circle*, *triangle* and *diamond* denote the values at 248.0, 228.0, 205.5 and 183.0 K, respectively

helpful to discriminate avalanche signals at a reasonable low threshold in the short-gate mode.

At the repetition frequency of 10 kHz, the dark counts are mainly caused by thermal effects, which can be reduced by operating the APD at the optimized temperature (183.0 K) in the gated mode with a very short gate. After-pulses of signals are the key obstacle against high repetition frequency operation of InGaAs/InP APDs. We applied two successive gate pulses on the spike-cancellation single-photon detector to measure the after-pulse probabilities (P_{after}) at temperatures 248.0 and 183.0 K under the detecting efficiency $\eta = 10\%$ and $\eta = 20\%$. As shown in Fig. 11, the after-pulse effects are more serious at lower temperatures. At 248.0 K, P_{after} is less than 0.2% 5 μs after the avalanche, and P_{after} under $\eta = 10\%$ is much larger than that under $\eta = 20\%$ because a higher DC bias is helpful to sweep the after-pulses [45]. At 183.0 K, P_{after} remains as high as 0.4% even 18 μs after the avalanche, and it becomes less sensitive to the DC bias. For instance, there is no visible difference between P_{after} under $\eta = 10\%$ and $\eta = 20\%$.

By using the spike-cancellation single-photon detector of $P_{\text{dark}} \approx 1.7 \times 10^{-6}$, a 155 km single-photon routing was

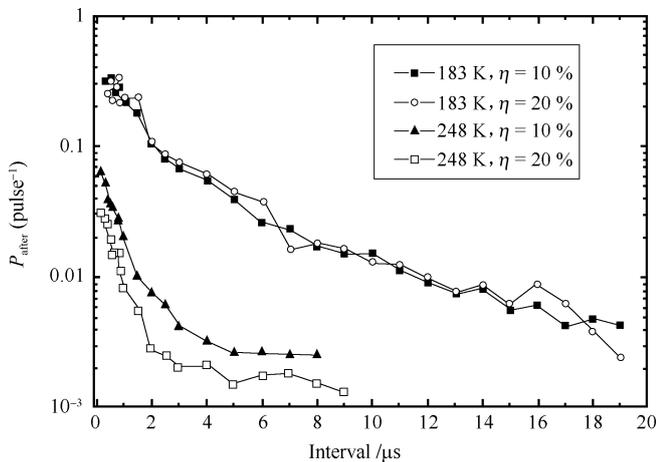


Fig. 11 The after-pulse probability P_{after} of the single-photon detector

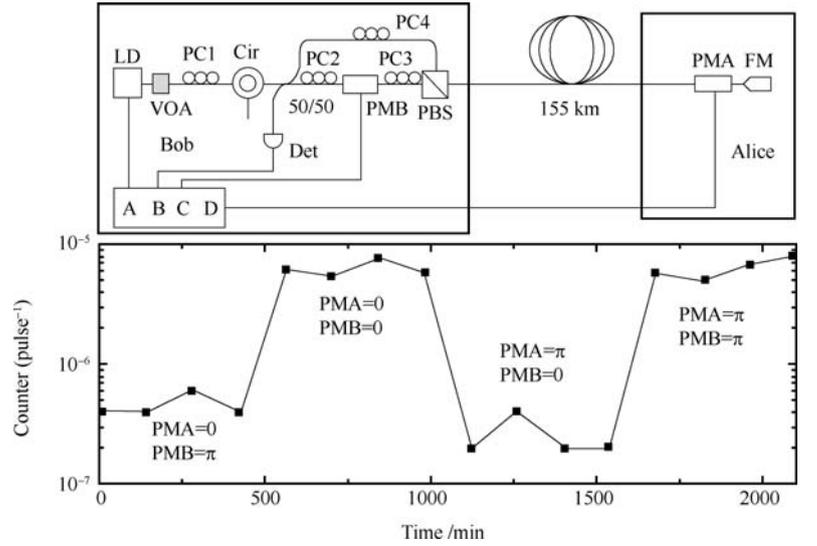
achieved with a ‘‘P&P’’ system as shown in Fig. 12. It makes full use of the round-way structure, which passively compensates the phase shift and polarization fluctuation. Therefore, it can maintain a high interference fringe contrast for a long period. But the Rayleigh back-scattering is remarkable in the 155 km fibre. The main obstacle is to operate the system at a high repetition frequency. In the experiment, a 600 Hz repetition rate was chosen to avoid influence from Rayleigh back-scattering. We note that higher rate can be possibly obtained by using pulse trains. The delay generator DG535 provided four clock signals to trigger the DFB LD, the single-photon detector, the phase modulator of Bob (PMB) and the phase modulator of Alice (PMA), respectively. The laser of 0.8 nW with 400 ps FWHM was attenuated by -35.0 dB. The losses of the optical set-ups in Bob’s and Alice’s sites were 5.0 and 10.0 dB, respectively. After the 155-km fibre (-30.5 dB at 1,550 nm), the average photon number $\langle n \rangle$ was 0.1 per pulse before leaving Alice. $\langle n \rangle$ was only 3.0×10^{-5} when the photon pulse returned to Bob. Taking the detection efficiency $\eta = 23\%$ of the single-photon detector into account, we estimated that the count at Bob’s site was about 7.0×10^{-6} per pulse. As shown in Fig. 12, each of the data was accumulated by 5.0×10^6 counts. The average results of turn-on (the sum phase shift of PMA and PMB was π) and turn-off (the sum phase shift of PMA and PMB was 0) were 6.0×10^{-6} and 4.0×10^{-7} per pulse, respectively. The contrast fringe was 87%. Also, most counts of turn-off were caused by dark counts of the single-photon detector.

In this section, we have introduced the unique spike-cancellation technique using the gated-mode operation of InGaAs/InP APDs with very short pulses. The spike-cancellation avalanche signals support accurate discrimination at a low threshold without affecting the detection efficiency. A detailed investigation was carried out to determine the optimized temperature to reduce thermal and after-pulse dark counts for JDSU EXT 40-X00408052. At 183.0 K, we obtained $P_{\text{dark}}/\eta = 1.7 \times 10^{-6}$ per pulse, which is, as far as we know, one of the best ratios for single-photon detection at 1.55 μm to date. With such a spike-cancellation single-photon detector, a ‘‘P&P’’ single-photon routing was realized in the 155-km optical fibre, with a fringe contrast of 87% at an average photon number $\langle n \rangle = 0.1$ per pulse.

5 Time-division phase encoding of single photons in a Sagnac interferometer

The core of a QKD system is a single-photon interferometer. In a practical long-distance QKD system, the single-photon interferometer should be stable. However, single photons as the information carriers are encoded by either phase or polarization in standard single-mode optic fibres, which encounter not only phase fluctuations varying with the fibre-length drifts sensible to environmental temperature but also non-deterministic changes of polarization states randomly varying with the polarization mode dispersion (PMD) due to uncontrollable changes of local

Fig. 12 The schematic diagram and experimental results of 155-km single-photon routing. *VOA* variable optical attenuator, *PC1–PC4* polarization controllers, *Cir* a three-port circulator, *PBS* polarization beam splitter, *FM* Faraday mirror, *Det* spike-cancellation gated-mode single-photon detector



stress on optic fibres and unavoidable elliptic cross-sections of fibres. Up to now, various techniques to obtain stable single-photon interference in long-distance optical fibres have been introduced and developed [48,49,52], among which the Faraday-mirror (FM) scheme is so far the best choice for autocompensation of the PMD and optical phase drifts [53,54].

Here, we introduce the stable single-photon interference in a Sagnac interferometer. The Sagnac interferometer [55] is based on an annular symmetric set-up as schematically shown in Fig. 13. The clockwise and counterclockwise pulses travel exactly the same Sagnac loop with exactly the same duration independent of any low-frequency fluctuation of the optic-path drifts. In order to control the single-photon interference at the output ports, we use time-division phase modulation (TDPM) to introduce different phase shifts ($\Delta\Phi$) between the clockwise and counterclockwise pulses. Consider a pulse a_0 with a duration of τ injected from the input port0 to the port3 of the coupler at $t_0 = 0$. After the coupler, it randomly chooses to travel

through the clockwise or counterclockwise path with equal probabilities. To establish a TDPM, we place PM within the fibre loop in such a location that a_1 pulse reaches PM at time t_1 and a_2 at t_2 . The lengths of the Sagnac loop and delay fibre are set to satisfy $t_1 \neq t_2$, $t_1 + t_2 = T$. Then we apply an electric modulation voltage V_m with a duration Δt to the PM at the time slot t_1 or t_2 , where $|t_1 - t_2| > \Delta t > \tau$. By changing the modulation voltage V_m , we correspondingly scan the phase difference $\Delta\Phi = (V_m/V_\pi) \times \pi$ between clockwise and counterclockwise paths, which determines the probability for the single-photon pulses to exit at port3 and port4 as $[1 \pm \cos(\Delta\Phi)]/2$, where V_π is the half-wave modulation voltage.

In a Sagnac interferometer, the clockwise and counterclockwise pulses pass through a certain point of the Sagnac loop at times differing at most the duration T that a photon travels around the whole loop. The fluctuation of fibre length within a time period less than T is negligible. So the annular configuration of the Sagnac interferometer can enable efficient automatic compensation of the slowly varied

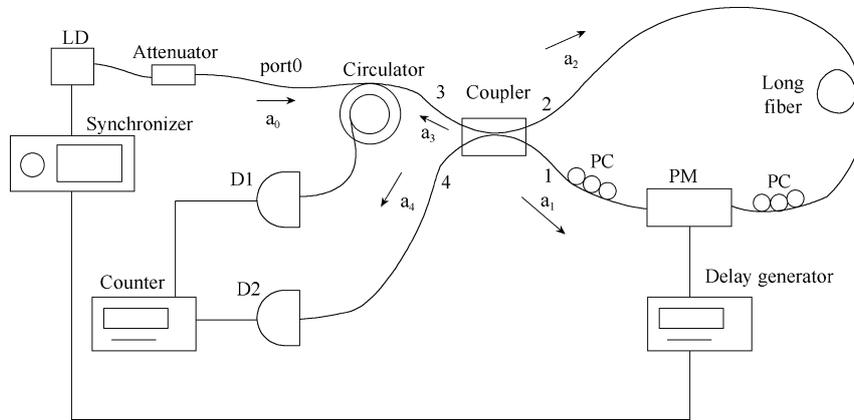


Fig. 13 Schematic of single-photon Sagnac interferometer, consisting of a 50%:50% coupler, an integrated phase modulator (*PM*), a long fibre, a delay fibre and two polarization controllers. After passing through a circulator and a fibre-optic coupler, the quasi single-photon pulse, denoted as a_0 , enters the Sagnac loop where it

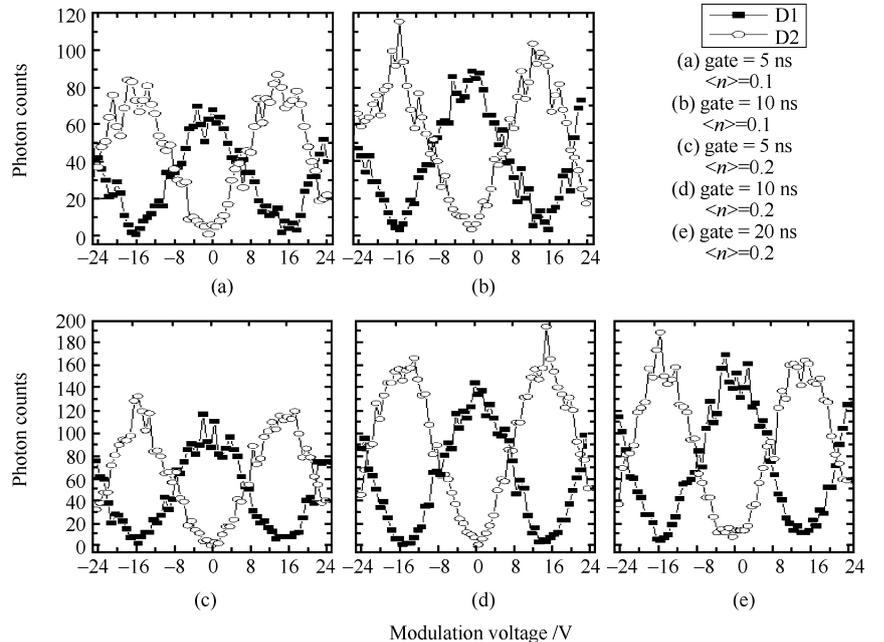
travels along the counterclockwise or clockwise path, denoted as a_1 and a_2 , respectively, and later returns to the coupler through the annular Sagnac loop. Finally, the single photon interfered with itself at the coupler, which is consequently detected by avalanche

phase drifts. On the other hand, although PMD makes observable change of their polarizations during travelling through the Sagnac loop, the clockwise and counter-clockwise pulses encounter approximately the same PMD and, as a consequence, have the same changed polarizations at the exit port, since they pass through the Sagnac loop sequentially within a time duration T that PMDs differ trivially. Automatic removal of the detrimental effects from the PMD on the single-photon interference is therefore achieved. The unique annular geometric configuration of the Sagnac loops can therefore support very high stabilities for long-distance single-photon Sagnac interferometers.

Experimentally, TDPM was carefully controlled by selecting an appropriate driving pulse to exert on the PM. Our experiments employed laser pulses from a 1,550-nm LD with about 2-ns duration. Appropriate attenuation was used to get weak coherent pulses at the quasi single-photon level [56]. The single-photon detectors D1 and D2 were made from InGaAs/InP APDs (EG&G 30644EJT-07) operated in the Geiger mode [57,58] at a temperature of 210 K by Peltier cooling. The single-photon interference fringe visibility is determined by the signal-to-noise ratio (S/N). The noises were mainly from the dark counts of the single-photon detectors. To reduce the dark counts of the single-photon detectors to obtain high interference fringe visibilities, we developed a pulse-bias gated quenching circuit to drive APD. A DC voltage, which was set 3 V lower than avalanche breakdown, was applied to the cathode of the APD. At times when single-photon pulses arrived, 200 ns-wide squared pulses of 5 V were triggered to couple to the DC driving voltage to switch on the avalanche detection. The avalanche signals were then coincidentally counted in a gated mode of the photcounter SR400.

We first scanned the single-photon interference curves of a 5 km-long Sagnac interferometer, as presented in Fig. 14.

Fig. 14 Single-photon interference with a 5 km fibre loop at $\langle n \rangle = 0.1$ and 0.2 with various coincident gates. The interference fringe visibilities are higher than 96% at $\langle n \rangle = 0.1$ by using a coincident gate of 5 ns (a) and 10 ns (b), respectively. For comparison, (c)–(e) give the interference curves at $\langle n \rangle = 0.2$ with coincidence gates of 5, 10 and 20 ns, respectively, which show that the maximum count increases more rapidly by increasing coincident gate from 5 to 10 ns than that from 10 to 20 ns, whereas the dark counts increase obviously when the gate is set to 20 ns. The optimized gate for coincident counting in our experimental condition is about 10 ns

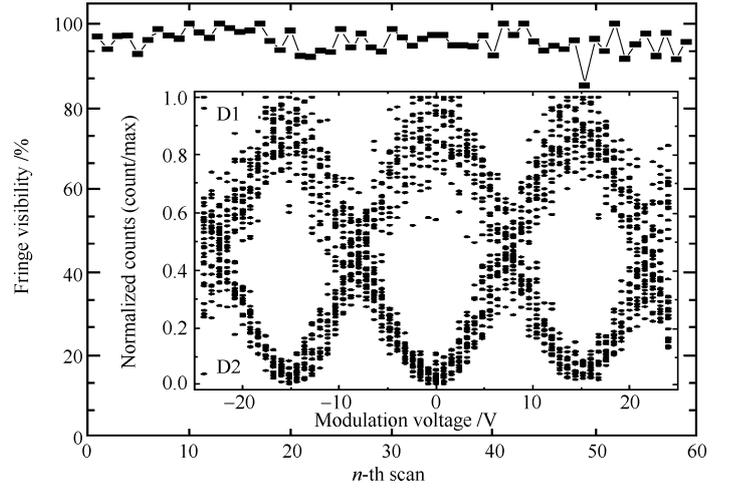


To test the long-term stability, we kept scanning the single-photon interference curves in a 5-km-long Sagnac interferometer for 2.5 h after a proper initial alignment without any readjustment of fibre-optic set-ups. Figure 15 clearly indicates that the interferences have remained stable for at least 2.5 h with a mean fringe visibility of 95.8%.

Secondly, we increased the length of the single-photon Sagnac interferometer to 27 km. Note that our Sagnac interferometer can work at arbitrary rates that, in principle, are only limited by the modulation frequency and APD dead time [57]. While in the measurements, we intentionally set that a second photon pulse should not be fired before the first photon reached the detectors merely in order to simplify the control system. For this purpose, the repetition rate of the laser pulse was decreased with increasing length of the Sagnac loop. In the 5 km-long Sagnac interferometer, the repetition rate was fixed at 10 kHz, and a lower rate of 5 kHz was used for the 27 km Sagnac loop. As shown in Fig. 16(a), the fringe visibilities of 93.8% and 95% were obtained for port3 and port4, respectively. To explore the autocompensation effects and crossover interference between sequential pulses on single-photon interferences at long-distance Sagnac interferometers, we further increased the interferometer length to 52 km and the pulse repetition rate to 15 kHz by using pulse trains at a repetition rate of 3 kHz with five pulses in each pulse train. The five pulses experienced the same phase setting to enhance the count number. Stable single-photon interference was observed in a 52-km Sagnac interferometer without crossover interference between sequential pulses. As shown in Fig. 16(b), we obtained the fringe visibilities of 90% and 85% for port3 and port4, respectively.

In this section, we have demonstrated that long-distance Sagnac single-photon interferometers exhibited excellent long-term stabilities with very high interference fringe

Fig. 15 Long-term stability of the single-photon interference with a 5 km fibre loop at $\langle n \rangle = 0.2$. Fifty-nine interference curves were superposed in the *subset*. Slight alignments of the polarization controllers inside the Sagnac loop would improve the stability of the single-photon interference, since polarization controlling could maximize the polarization-dependent phase modulation of the integrated PM



visibilities, which showed the promising prospect for applications in practical QKD and quantum devices for single-photon routing.

6 Differential phase shift in a Faraday-mirror-based Michelson interferometer

After the creative works of Bennett and Brassard [59] and Bennett [69], scientists have done many encouraging experiments for QKD. Due to its promising prospect in cryptocommunication, people are mostly attracted by the works done in optical fibre [49–53, 59–69, 72–75], which were roughly classified into two categories as “one-way” and “P&P” schemes. The first category is represented by Bennett’s [69] proposal of a double Mach–Zehnder (MZ) system. The main difficulty associated with this QKD scheme lies in two aspects. First, the PMD in optic fibres introduced by imbalanced arms causes variable degradation of photon interferences. Second, the arm differences of Alice’s and Bob’s interferometers must be kept stable within a fraction of the photon wavelength to maintain correct phase relations. To avoid inconvenience of active control of phase drifts and PMD, Muller et al. [52] invented

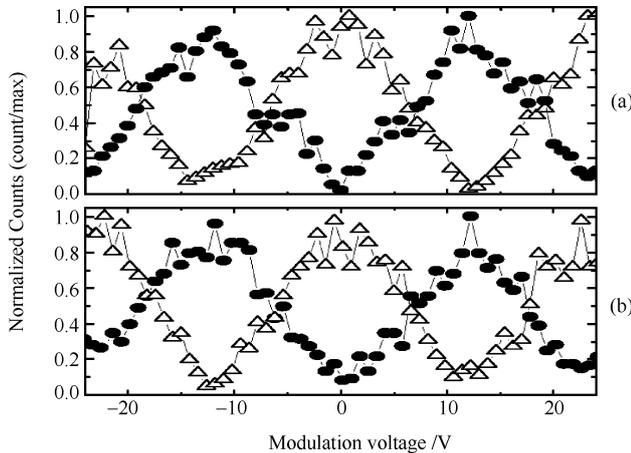
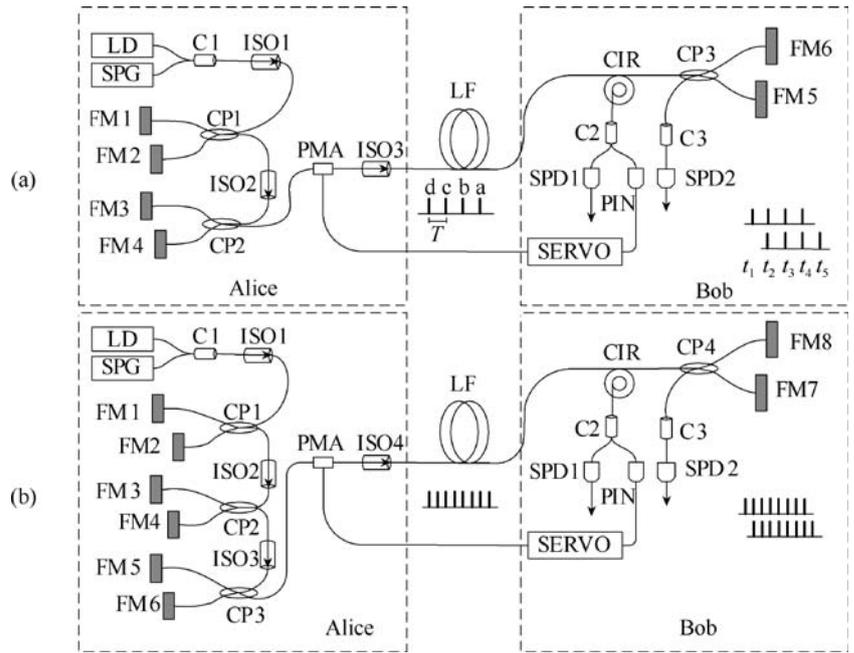


Fig. 16 Single-photon interference with (a) 27 km fibre loop at $\langle n \rangle = 0.6$ and (b) 52 km fibre loop at $\langle n \rangle = 1.0$

a round-way “P&P” QKD system based on polarization-orthogonal reflection from FMs, which enables high-quality interference without any initial calibration step or active compensation in the optical circuits. With the P&P scheme, Stucki et al. [53] successfully implemented the 67-km outdoor QKD experiment. But this scheme still bears some deficiencies. For example, the requirement that the signal must travel both directions along the transmission line not only leads to nontrivial technical difficulties such as Rayleigh backward-scattering of the strong forward pulses, but also may even leave a backdoor for Eve to make “Trojan horse” attack. On the other hand, a round-way scheme is not preferred if one considers to use ideal single photons as information carriers. From the practical points of view, a QKD system based on either one-way or round-way scheme faces a troublesome problem of impractically low rate of key distribution, which is mainly limited by the immaturity of up-to-date techniques for single-photon generation and detection. To enhance the secret key creation rate, a differential phase shift (DPS) scheme is proposed by splitting a single-photon pulse into three sequential time slots, followed by DPS encoding with half-wave phase modulations randomly applied to the adjacent components of the photon. At the detection stage, the key creation efficiency reaches as high as two thirds [49].

We demonstrate that the virtue points of PMD autocompensation from the FM-based design and high key-creation efficiency from DPS encoding can be combined on a one-way optical-fibre structure that skilfully uses FM-armed Michelson interferometers (FM-MI), where the FM-MIs consist of unequal arms tailed with FM reflections. At Alice’s station, the FM-MI allows an automatic alignment of the polarization states of the sequential DPS pulses to pass through the long-distance quantum channel with the same polarization states, reaching Bob’s station with the same unknown polarization states. At Bob’s station, any possible polarization difference between the interfering pulses due to PMD in the unequal arms is also autocompensated by the FM-MI. This design eventually results in a stable key distribution immune to the PMD in the quantum channel, typically a long-distance optical fibre. Such a DPS QKD scheme

Fig. 17 Set-up of the autocompensating DPS QKD system with FM-MIs in series for a key creation efficiency of 3/4 (a) and 7/8 (b)

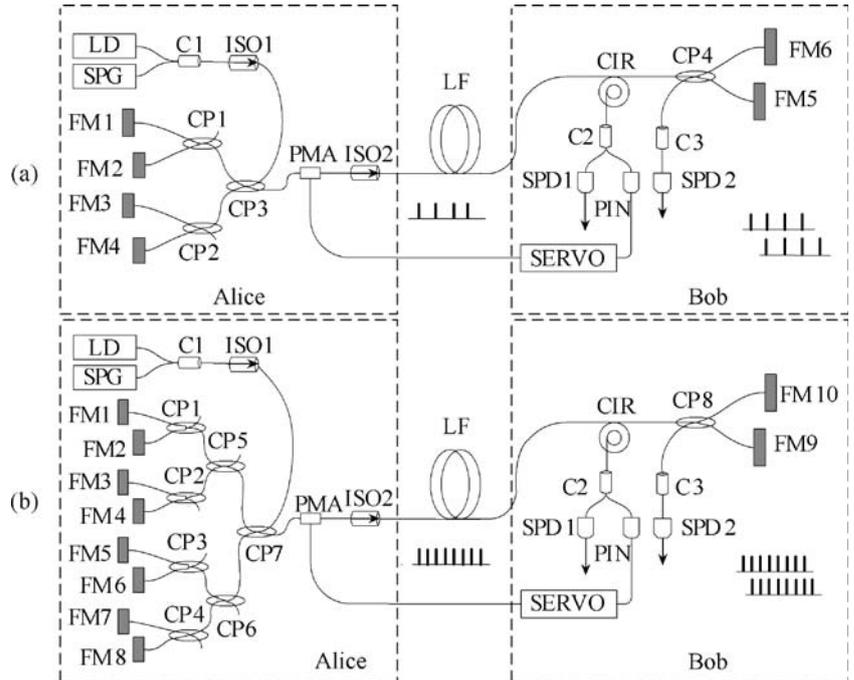


features perfect stability, high key creation efficiency, immunity to “Trojan horse” attack and capability to be used for ideal single photons.

High efficiency is a strong point of the DPS scheme. In conventional QKD systems, the most popular protocols employed are phase-encoding BB84 [59] and B92 [69]. It has been proved that the efficiency in a DPS scheme is much higher than that in conventional system and can be readily expanded by increasing the time slots [49,50]. To show this, two kinds of expandable systems are presented in Figs. 17 and 18. Figure 17(a) presents a scheme to split a photon into four time instances. In order to get more time

slots, two FM-MIs are connected in series in Alice’s site. Two couplers and four FMs are needed to form the two cascaded FM-MIs. The first FM-MI divides the photon from a single photon source into two pulses with a time delay $2T$, and then the two pulses are respectively divided into two pulses with a time delay T by the second FM-MI, resulting in four sequential pulses (a, b, c and d) with the same time interval T . The four pulses are randomly modulated with a phase 0 or π . In Bob’s site, there are five time instances as shown in Fig. 17(a). As pulses a and d contribute 50% while pulses b and c contribute 100% to the key distribution, the key creation efficiency of this

Fig. 18 Set-up of the autocompensating DPS QKD system with FM-MIs in parallel for a key creation efficiency of 3/4 (a) and 7/8 (b)



system is three fourths. Higher efficiency can be achieved by increasing the number of the FM-MIs connected in series as shown in Fig. 17(b). If n FM-MIs are used in Alice's site, the key creation efficiency reaches up to $(2^n - 1)/2^n$. As shown in Fig. 18, FM-MIs in parallel can also be used to increase the efficiency up to $n/(n + 1)$, where n is the number of couplers used in Alice's site.

The security of DPS QKD has already been partly demonstrated in [49,51]. The proposed system is also immune from Trojan horse attack, although FM reflection is used. In a standard two-way quantum cryptography system, Eve may eavesdrop the secret key information by using an exploring light pulse to experience the same phase modulations in Alice's site as the single-photon pulse. In the proposed system, Alice can simply put an isolator to ensure unidirectional propagation of the single-photon pulses from Alice to Bob, obviating divulgence of the secret phase modulations to any possible exploring light pulses.

The present scheme is immune to PMD influence in the quantum channel. In a traditional system with a MZ interferometer, PMD in the imbalanced arms debases the stability of the interference visibility. Since FMs are used in our system for polarization-orthogonal reflection at the unbalanced arms of the FM-MIs [70], PMDs for the pulses on their ways to FMs are automatically compensated on their return ways. While the pulses are travelling through the quantum channel, the sequential pulses, which enter the quantum channel in Alice's site with the same polarization states, reach Bob's site with the same polarization states,

although PMD in the quantum channel makes random polarization changes. FMs are also used in Bob's site to guarantee that the interfering pulses have the same polarization state. As a consequence, the single-photon interference becomes independent upon the PMD of the quantum channel.

To further illustrate the immunity of polarization changes in the quantum channel for the present scheme, we briefly discuss in what follows the transformation of polarization in the system by using Jones matrix [70]. Suppose A_n represents the Jones matrix of fibre in the n th fibre paths of the FM-MI in Alice's site, Q the Jones matrix of the long-distance fibre (quantum channel) and B_0 and B_T the Jones matrices of fibre in the respective paths of the FM-MI in Bob's site. The total transformation matrices can be described by $P \propto [B_0^+ M B_0 e^{i\beta_0} + B_T^+ M B_T e^{i\beta_1}] \cdot Q e^{i\phi}$.

$\sum_n [A_n^+ M A_n e^{i\alpha_n + i\varphi_n}]$, where M represents the Jones matrix of an FM, α_n and β_n are the round-trip phases through the n th fibre path of Alice's and Bob's FM-MIs, ϕ_n is the modulated phases for the n th pulse through the PM and φ is the phase through the transmission fibre. Single-photon interference takes place at the time slot nT with the corresponding output Jones vector of the electric field given by $E_{\text{out}} \propto \{B_0^+ M B_0 \cdot Q \cdot A_{n+1}^+ M A_{n+1} e^{i(\alpha_{n+1} + i\varphi_{n+1} + \phi + \beta_0)} + B_T^+ M B_T \cdot Q \cdot A_n^+ M A_n e^{i(\alpha_n + \varphi_n + \beta_1 + \phi)}\} E_{\text{in}}$, where E_{in} represents the Jones vector of the input field. The output power at the time slot nT is given by

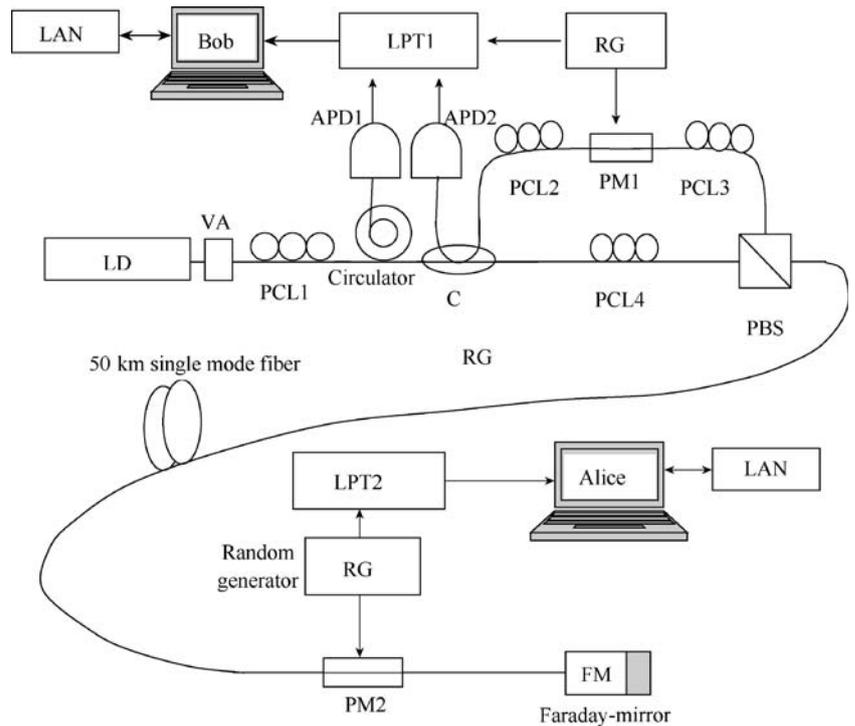
$$P_{\text{out}} \propto 2P_{\text{in}} + E_{\text{in}}^+ \left[\begin{array}{l} A_{n+1}^+ M A_{n+1} \cdot Q^+ \cdot B_0^+ M B_0 \cdot B_T^+ M B_T \cdot Q \cdot A_n^+ M A_n e^{-i(\Delta\alpha + \Delta\beta + \Delta\phi)} \\ + A_n^+ M A_n \cdot Q^+ \cdot B_T^+ M B_T \cdot B_0^+ M B_0 \cdot Q \cdot A_{n+1}^+ M A_{n+1} e^{i(\Delta\alpha + \Delta\beta + \Delta\phi)} \end{array} \right] E_{\text{in}}$$

where $\Delta\alpha = \alpha_1 - \alpha_2$, $\Delta\beta = \beta_2 - \beta_1$ and $\Delta\phi = \phi_1 - \phi_2$. Note that A_n , B_n and Q are time-dependent due to the randomness of the PMD; the interferential terms depend not only on the polarization changes in Alice's and Bob's sites but also on the PMD in the transmission fibre. If polarization-dependent loss is negligible, all the Jones matrices are unitary, and the unique features of the Jones matrix of the FM ensure $A_{n+1}^+ M A_{n+1} \cdot Q^+ \cdot B_0^+ M B_0 \cdot B_T^+ M B_T \cdot Q \cdot A_n^+ M A_n = I$ and $A_n^+ M A_n \cdot Q^+ \cdot B_T^+ M B_T \cdot B_0^+ M B_0 \cdot Q \cdot A_{n+1}^+ M A_{n+1} = I$. The output power can then be simplified as $P_{\text{out}} \propto P_{\text{in}} [1 + \cos(\Delta\alpha + \Delta\beta + \Delta\phi)]$, which means a complete immunity of interferential output power from the PMD influence in the quantum channel. Nevertheless, P_{out} is still dependent on the phase drifts $\Delta\alpha$ and $\Delta\beta$, which are not invariable due to arm-length changes of Alice's and Bob's FM-MIs. Typically, the phase drifts are slow and can be compensated by using a feedback control. For such a purpose, a servo system can be used with an injected pulse to offer the feedback signal. The injected

pulses propagate along the same route as the single-photon pulse, but it is behind the single-photon pulse with a time delay $T_0 > 2T$; in Alice's site, we can add phase modulation to the single-photon pulses while keeping the injected light to be non-modulated by PMA, which ensures that the injected light would not bring any insecurity to the scheme. The servo system records the interferential signal of the injected light pulse to detect the slow phase drifts $\Delta\alpha$ and $\Delta\beta$, and then gives a feedback to adjust the DPS phase modulations in Alice's phase modulator to ensure that $\Delta\alpha + \Delta\beta + \Delta\phi$ is 0 or π . In this way, the stability of the scheme is guaranteed.

In this section, we have introduced an autocompensating DPS QKD scheme with the help of FM-based MIs. The environment-induced polarization drift was automatically compensated by the to-and-fro mechanism in the local sites, whereas the phase drift was stabilized using a mature technique of servo system. Expanded versions with higher key creation efficiencies were also presented.

Fig. 19 Schematic of our “plug and play” quantum key distribution. The variable attenuator VA was placed in series with the LD to reduce noises from the back-scattering, and the APDs were under pulse-bias mode so that the dark counts were lowered. *RG* random generator, *PCL1–PCL4* polarization controller, *C* 1:1 coupler. The insertion loss of the components: phase modulators PM1 and PM2: about -4 dB, PBS: -3 dB, Faraday mirror: -0.5 dB. The arm-length difference of the MZ was 36 m



7 Long-distance quantum key distribution

As we have mentioned previously, the technique of single-photon operation has supplied us with a good weapon for quantum information research. In this section, we describe its most direct application in QKD, which has been proved to be the only absolutely safe cryptography method whose security is guaranteed by the uncertainty principle of quantum mechanics [59,60].

In a practical QKD system, polarization coding and phase coding are often used [1]. The polarization coding scheme is mainly for free-space QKD experiments, whereas in fibre-optic systems, phase coding is preferred [63–66]. Nowadays, with the development of the Internet, scientific community has shown increasing interest in developing optic-fibre-based QKD. However, problems of PMD and phase drifts in optic fibre are a barrier in the practice of long-distance QKD. More recently, scientists in Geneva University invented a skilful scheme of “P&P” system that allows automatic and passive compensation of all polarization fluctuations [52]. In 2002, the Geneva University group reported a 67 km optic-fibre QKD experiment [53]. In 2003, we have successfully realized a transmission of “one-time-pad” keys [1] with a 50 km optic-fibre quantum cryptosystem using the technique of pulse-bias and coincident gate single-photon detection in the “P&P” set-up. Moreover, in order to reduce the noises of Rayleigh back-scattering in fibre, a variable attenuator, which controlled the photon number, was connected in series with the LD instead of being at Alice’s site. In our experiment, the B92 protocol [69] based on two non-orthogonal phases was used. Bob supplied Alice with a single-photon as a quantum bit carrier. Alice sent the single photon back to Bob in one

of the two non-orthogonal phase states, and Bob measured it randomly in two non-orthogonal bases. A secret key was created between Alice and Bob when Bob’s base matched Alice’s state, whereas those mismatching measurements were discarded. The security of the system is guaranteed by quantum mechanics, which never allows an eavesdropper to perfectly identify a state in the non-orthogonal bases by a single measurement.

The schematic of our experiment is shown in Fig. 19. Photon pulses were produced by Bob’s LD, and then they travelled through the unbalanced MZ interferometer, which split each pulse into “fast” and “slow” pulses (in terms of quantum mechanics, there were two paths for the photon to select), called P_L and P_S . After passing the polarization beam splitter (PBS), P_L and P_S were then in linear polarization state orthogonal to each other. As they reached the phase modulator PM2, Alice applied phase modulation to

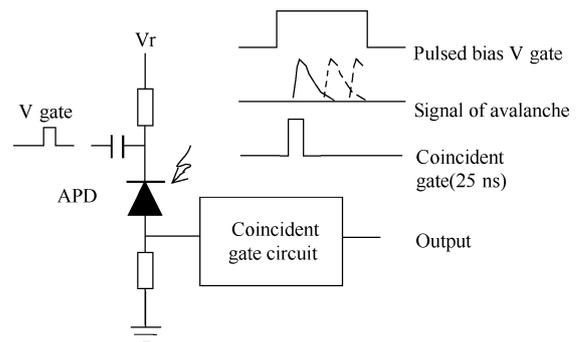
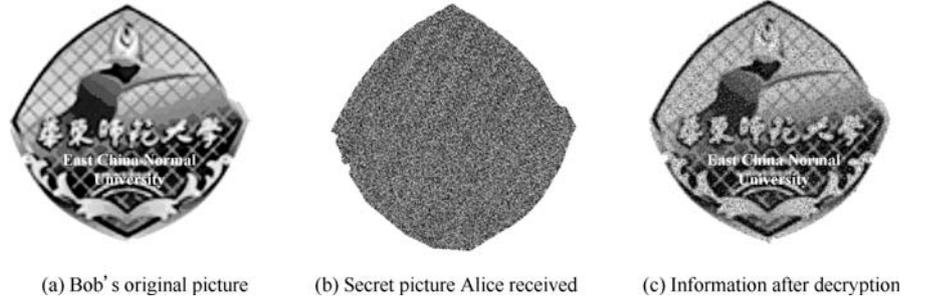


Fig. 20 Schematic of pulse bias and coincident gate single-photon detection circuit

Fig. 21 A sample picture transmitted by our QC system. The picture used was a 256-color bit map: (a) Bob's original picture, (b) secret picture Alice received and (c) information after decryption



P_L , while left P_S to be unchanged, and the information was encoded. Then the two pulses were reflected back to Bob by the FM [70]. At this stage, each photon pulse was attenuated to contain only one photon or less so that no eavesdroppers could tap the quantum channel without being noticed. Thanks to the FM, when P_L and P_S returned to Bob, they exchanged their polarization states as well as their paths in the MZ. Therefore, Bob was now able to apply a phase modulation to P_S using PM1. At last, the two pulses met at the coupler to interfere with each other according to the phase shifts of PM1 and PM2. Moreover, the result of interference was then recorded by APD1 and APD2, which was later used to obtain the secret keys by using B92 protocol.

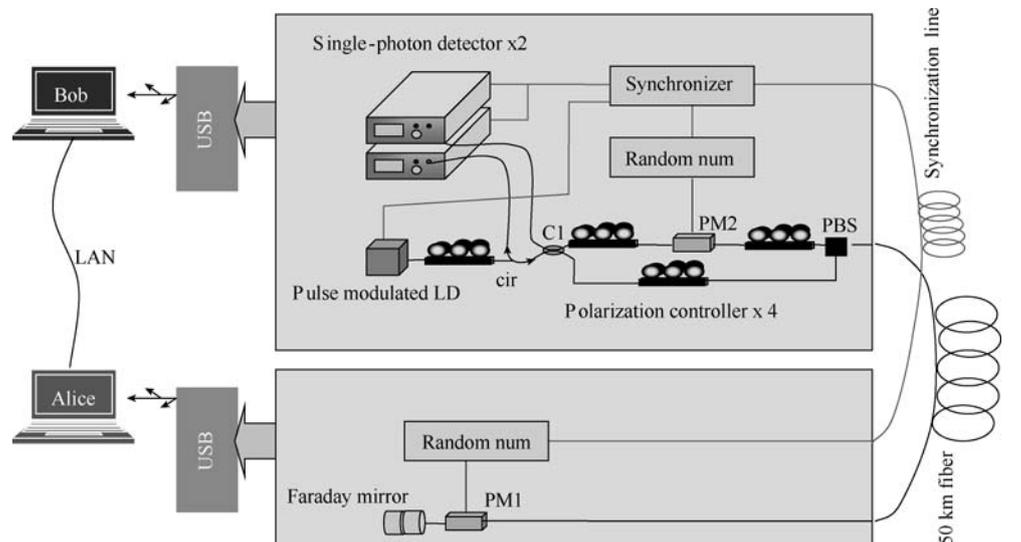
This system used the so-called B92 protocol for QKD. The detailed working condition was also described in [2]. In this system, two InGaAs APDs (EG&G 30644EJT-07) were used as single-photon detectors, which were Peltier cooled to $-60.0 \pm 0.1^\circ\text{C}$. To lower the noises from dark count and back-scattering effects, we extended the traditional gate-mode quenching [71] and designed a novel APD quenching circuit by combining the pulsed bias with the coincidence counting techniques. Figure 20 depicts the schematic of our pulse bias and coincident gate single-photon detection circuit. This scheme effectively lowered the after-pulse probability and skilfully avoided the elaborate electronic work to separate avalanche signals from transient pulses, which thus led to an easy and cost-effective

construction of single-photon-detecting module. Practically, the amplitude of the pulse bias and the width of the coincident gate must be carefully adjusted to get an optimal working state. In our experiment, the avalanche voltage of APD1 and APD2 was 44.5 and 43.3 V, respectively. The amplitude of the pulse bias was 10 Vpp, and the coincident gate width was 25 ns. According to our experiments done in 2003, the quantum efficiencies of our single-photon-detecting modules were 9 and 7% with dark count noises of 5×10^{-4} per pulse [2]. The single-photon detectors have been significantly improved with higher performance as discussed in previous sections.

The working sequence of the system was under the control of an electronic timer at Bob's site. The timer was constructed with an 8051 MPU and several resistor-capacitor delay lines, which supplied timing signals with a precision of nanosecond order. A coaxial cable was used to supply Alice with the reference timing signal. In a future experiment of outdoor system, a radio signal channel could be considered to replace the coaxial cable.

In a typical "P&P" set-up, Bob uses strong laser pulses, which may cause large dark-count rate due to the Rayleigh back-scattering effect. The problem was solved here by two steps. Firstly, we used the pulse-bias circuit for our single-photon detectors so that the APDs were only awakened to work in an active state of Geiger mode [57] for a very short period when the photon was expected. The back-scattered photons were totally omitted because they reached the

Fig. 22 Improved system of our "plug and play" quantum key distribution. Photon number $\langle n \rangle = 0.07$, QBER: 4%, fibre length: 50 km. *Cir* circulator, *C* 1:1 coupler, *PM1* and *PM2* phase modulators



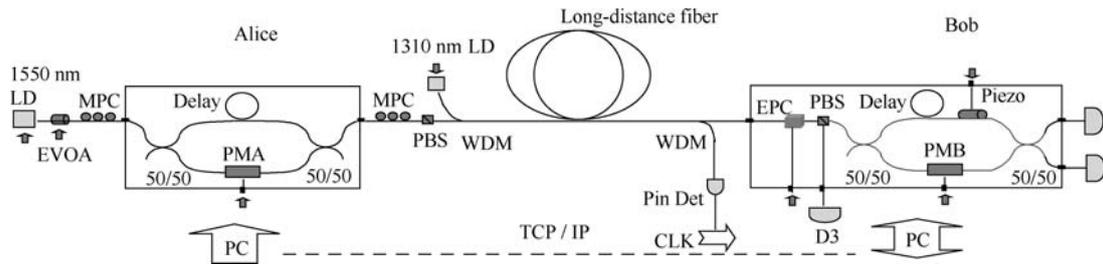


Fig. 23 Schematic of polarization maintaining fibre-based one-way QKD system. *EVOA* electronic variable optical attenuator, *MPC* manual polarization controller, *EPC* electric polarization controller, *PMA* and *PMB* phase modulators, *PBS* polarization beam splitter,

PC personal computer, *piezo* piezoelectric transducer, *CLK* synchronization signal, *WDM* 1,310/1,550 nm wavelength division multiplexer

detectors much earlier than the signal photon. Secondly, a variable attenuator was placed just after the LD to reduce much of the input energy, and the effect of back-scattering itself was greatly degraded.

We made a demonstration of cryptographic communication with the sifted “one-time-pad” keys as follows. Let the 10 km QKD system continuously work for 2 h to exchange a bunch of secret keys, which were saved into the local disks by Alice and Bob, respectively. As long as the keys were ready, Alice encoded a picture with her own keys, such as the one shown in Fig. 21(a), and transmitted it to Bob through the local area network (LAN) using the transmission control protocol (TCP). Figure 21(b) was the received picture at Bob’s computer, which was totally unrecognizable. Then, Bob decoded the picture with his private keys to yield the picture of Fig. 21(c). Here, keys were directly used without error correction.

The performance of this system was then greatly improved in 2004. The improved version of our QKD is schematically shown in Fig. 22. Based on the spike-cancelled single-photon detection, high-speed interface (USB 2.0) for data acquisition and communication control and accurate synchronization circuit, we have achieved much better results. At the quasi single-photon pulse of mean photon number $\langle n \rangle = 0.07$, we achieved stable QKD with a QBER of less than 4%. In such a QKD system, we employed home-made single-photon detectors with the spike-balance techniques as described in the previous section. By using single-photon detectors with ratio of dark noise-to-quantum efficiency of $P_{\text{dark}}/\eta = 1.7 \times 10^{-6}$, we may even obtain a QKD in optic fibre over 150 km. Polarization-independent phase encoding and decoding were also used. To increase the key creation rate, a high-speed interface has been explored to record the quantum bit and control the communication system. With those improvements, the cryptographic communication based on the sifted “one-time-pad” keys was successfully demonstrated through a public LAN by using the TCP.

The “P&P” systems belong to the so-called “two-way” category, in which the information carrier, single photons, travels from Bob to Alice and then back to Bob. Such a scheme shows very good stability because the round trip makes perfect complimentary of phase shifts and PMDs.

But a troublesome problem is that it is often questioned for its vulnerable performance under the Trojan horse attack [76]. While people are trying every means to make up for this security problem, one can turn to one-way systems for an ultimate solution [3].

A one-way system is immune to the Trojan horse attack at the cost that it loses the ability of automatic complementary of PMD and phase shift. In a phase-coding system, the PMD and phase shift are mainly affected by the interferometers in Bob and Alice, and the long-distance fibre only contributes to the slow variation. Therefore, the main effort should be made to stabilize the single-photon interferometers. Our solution is presented in Fig. 23 by using polarization-maintaining fibre in Bob’s site so that the polarization changes in the quantum channel have negligible influence on the single-photon interference and QKD as well. The system is based on two serially connected MZ interferometers with imbalanced arms [69]. We describe how this system fights against the PMD and phase shift one by one. Let us look at the MZ interferometer in Bob’s site. The interferometer is composed of a PBS, a piezoelectric transducer, a phase modulator, polarization maintaining fibres and a 50/50 polarization-maintaining coupler. When a 45° to horizontal polarized photon enters Bob’s interferometer through Bob’s PBS, the interferometer maintains the polarization state and results in a stable interference free of PMD influence. On the other hand, in Alice’s MZ, single-mode fibres are used. At the output port, a manual polarization controller and a PBS are used to ensure fixed polarization state. Because the PMD in long fibre changes slowly, feedback control can be enabled with an electric polarization controller and a detector D3. Also, in Bob’s site, another feedback control loop is composed of a piezoelectric transducer and the APDs. There is a phase alignment period between every two key-creation periods. When the hardware of Alice and Bob are carefully packaged in isolated boxes, those feedback controllers will take effective actions against phase shift and PMD and make a stable and secure one-way QKD system. As the single-photon pulses after Alice’s site transmit the long-distance fibre (quantum channel) with a fixed polarization state, PMD in the quantum channel does not affect the single-photon interference visibility.

8 Summary and complements

Our work is concentrated on the single-photon operation for QKD. We generated ideal single photons for Alice (transmitter) and built a single-photon detector for Bob (receiver); to activate a QKD system, we presented new techniques of single-photon control and routing. As for the goal of application, we have built a 50 km “P&P” QKD.

Up to now, most QKD experiments for optical fibre were done with phase-coding protocols. However, the original idea of BB84 was demonstrated with the picture of polarization. In fact, polarization coding has many advantages. The modulation units can be easily implemented with simple components and simple operation principle. Both Alice and Bob can use very few passive components so that there can be much less attenuation in quantum channel than that in phase-coding schemes. Also, we only need to stabilize one variable, i.e. PMD, unlike that in phase coding where we must take care of both PMD and phase shift. The only problem is to track the randomly altering state of polarization on the Poincare sphere.¹ Experimental study of polarization coding QKD in optical fibre is now in progress.

Acknowledgements This work was partly supported by National Natural Science Fund (Nos. 10374028 and 60478011), National Fundamental Research Program (2001CB309301), Science and Technology Commission of Shanghai Municipality (No. 03XD14012) and National Education Ministry of China (No. 104193).

References

- Gisin N., Ribordy G., Tittel W. and Zbinden H., Quantum cryptography, *Rev. Mod. Phys.*, 2002, 74: 145–195
- Zhou C., Wu G., Chen X., Li H. and Zeng H., Quantum key distribution in 50-km optic fibers, *Sci. China, Ser. G*, 2004, 47: 182–188
- Mo X., Zhu B., Han Z., Gui Y. and Guo G., Faraday–Michelson system for quantum cryptography, *Opt. Lett.*, 2005, 30: 2632–2634
- Brassard G., Lütkenhaus N., Mor T. and Sanders B., Limitations on practical quantum cryptography, *Phys. Rev. Lett.*, 2000, 85: 1330–1333
- Beveratos A., Brouri R., Gacoin T., Villing A., Poizat J.-P. and Grangier P., Single photon quantum cryptography, *Phys. Rev. Lett.*, 2002, 89: 187901
- Waks E., Inoue K., Santori C., Fattal D., Vučković J., Solomon G. and Yamamoto Y., Quantum cryptography with a photon turnstile, *Nature*, 2002, 420: 762
- Brouri R., Beveratos A., Poizat J.-P. and Grangier P., Single-photon generation by pulsed excitation of a single dipole, *Phys. Rev. A*, 2000, 62: 063817–063823
- Gruber A., Dräbenstedt A., Tietz C., Fleury L., Wrachtrup J. and von Borczyskowsky C., *Science*, 1997, 276: 2012
- Kurtsiefer C., Mayer S., Zarda P. and Weinfurter H., *Phys. Rev. Lett.*, 2000, 85: 290
- Brouri R., Beveratos A., Poizat J.-P. and Grangier P., *Opt. Lett.*, 2000, 25: 1294
- Kilin S., Nizovtsev A., Maevskaya T., Dräbenstedt A. and Wrachtrup J., *J. Lumin.*, 2000, 86: 201
- Beveratos A., Brouri R., Gacoin T., Poizat J.-P. and Grangier P., Nonclassical radiation from diamond nanocrystals, *Phys. Rev. A*, 2001, 64: 061802R
- Treussart F., Jacques V., Wu E., Gacoin T., Grangier P. and Roch J.-F., Photoluminescence of single colour defects in 50 nm diamond nanocrystals. Proceedings of ICDS 23 Conference (23rd International Conference on Defects in Semiconductors, July 24–July 29, 2005, Awaji Island, Hyogo, Japan); *Phys. B*, in press
- Beveratos A., Kühn S., Brouri R., Gacoin T., Poizat J.-P. and Grangier P., *Eur. Phys. J. D*, 2002, 18: 191
- Jacques V., Wu E., Toury T., Treussart F., Aspect A., Grangier P. and Roch J.-F., Single-photon wavefront-splitting interference. An illustration of the light quantum in action, *Eur. Phys. J.-D*, 2005, DOI: 10.1140/epjd/e2005-00201-y. A supplementary movie showing the built-up of the interference pattern is available in electronic form at <http://www.eurphysj.org>
- Alléaume R., Treussart F., Messin G., Dumeige Y., Roch J.-F., Beveratos A., Brouri-Tualle R., Poizat J.-P. and Grangier P., *New J. Phys.*, 2004, 6: 92
- Gaeble T., Popa I., Gruber A., Domhan M., Jelezko F. and Wrachtrup J., *New J. Phys.*, 2004, 6: 98
- Rabeau J., Chin Y., Prawer S., Jelezko F., Gaeble T. and Wrachtrup J., *Appl. Phys. Lett.*, 2005, 86: 131926
- Wu E., Jacques V., Treussart F., Zeng H., Grangier P. and Roch J.-F., Single-photon emission in the near infrared from diamond colour centre, Proceedings of PDC’05 conference (Dynamical Processes in Excited States of Solids (DPC’05) August 1st to 5th, 2005, Shanghai, China), *J. Lumin.*, in press
- Yelissev A., Lawson S., Sildos I., Osvet A., Nadolinny V., Feigelson B., Baker J., Newton M. and Yuryeva O., *Diamond Relat. Mater.*, 2003, 12: 2147
- Zaitsev A.-M., *Optical Properties of Diamond, A Data Handbook*, Berlin Heidelberg New York: Springer, 2000
- Lütkenhaus N., *Phys. Rev. A*, 1999, 59: 3301
- Albota M.-A. and Wong F.-N.-C., in *Quantum Electronics and Laser Science (QELS)*, vol. 89 of OSA Trends in Optics and Photonics Series (Optical Society of America, Washington, DC, 2003), paper QThPDB11
- Albota M.-A. and Wong F.-N.-C., *Opt. Lett.*, 2004, 29: 1449
- Roussev R.-V., Langrock C., Kurz J.-R. and Fejer M.-M., *Opt. Lett.*, 2004, 29: 1518
- Yao W., Liu R.-B. and Sham L.-J., *Phys. Rev. Lett.*, 2005, 95: 030504
- Knill E., Laflamme R. and Milburn G.-J., *Nature (London)*, 2001, 409: 46
- Shapiro J.-H., *New J. Phys.*, 2002, 4: 47.1
- Resch K.-J., Lundeen J.-S. and Steinberg A.-M., *Phys. Rev. Lett.*, 2002, 89: 037904
- Diamanti E., Langrock C., Fejer M.-M., Yamamoto Y. and Takesue H., in *Conference on Lasers and Electro-Optics, OSA Technical Digest (Optical Society of America, Washington, DC, 2005)*, paper CTuY6
- Langrock C., Diamanti E., Roussev R.-V., Yamamoto Y., Fejer M.-M. and Takesue H., in *Conference on Lasers and Electro-Optics, OSA Technical Digest (Optical Society of America, Washington, DC, 2005)*, paper QThJ1
- Bienfang J.-C., Gross A.-J., Mink A., Hershman B.-J., Nakassis A., Tang X., Lu R., Su D.-H., Clark C.-W., Williams C.-J., Hagley E.-W. and Wen J., *Opt. Express*, 2004, 12: 2011
- Langrock C., Diamanti E., Roussev R.-V., Yamamoto Y. and Fejer M.-M., *Opt. Lett.*, 2005, 30: 1725
- Bryan D.-A., Gerson R. and Tomaschke H.-E., *Appl. Phys. Lett.*, 1984, 44: 847
- Sato A., Asai K. and Mizutani K., *Opt. Lett.*, 2004, 29: 836
- Chen Y.-F., Chen S.-W., Tsai L.-Y., Chen Y.-C. and Chien C.-H., *Appl. Phys. B*, 2004, 79: 823
- Kane T.-J. and Byer R.-L., *Opt. Lett.*, 1985, 10: 65
- Wu E., Pan H., Zhang S. and Zeng H., *Appl. Phys. B*, 2005, 80: 459

¹For example, the DPC5500 Deterministic Polarization Controller from THORLABS.

39. Karlsson A., Bourennane M., Ribordy G., Zbinden H., Brendel J., Rarity J. and Tapster P., *IEEE Circuits Devices*, November 1999: 34–40
40. Voss P.-L., Köprülü K.-G., Choi S.-K., Dugan S. and Kumar P., *J. Mod. Opt.*, 2004, 51: 1369–1379
41. Kosaka H., Tomita A., Nambu Y., Kimura T. and Nakamura K., *Electron. Lett.*, 2003, 39: 1199–1201
42. Bourennane M., Gibson F., Karlsson A., Hening A., Jonsson P., Tsegaye T., Ljunggren D. and Sundberg E., *Opt. Express*, 1999, 4: 383–387
43. Bethune D.-S. and Risk W.-P., *IEEE J. Quantum Electron.*, 2000, 36: 340–347
44. Bethune D.-S., Risk W.-P., *New J. Phys.*, 2000, 4: 42.1–42.15
45. Tomita A. and Nakamura K., *Opt. Lett.*, 2002, 27: 1827–1829
46. Yoshizawa A., Kaji R. and Tsuchida H., *Appl. Phys. Lett.*, 2004, 84: 3606–3608
47. Lacaíta A., Zappa F., Cova S. and Lovati P., *Appl. Opt.*, 1996, 35: 2986–2996
48. Marand C. and Townsend P.-D., *Opt. Lett.*, 1995, 20: 1695–1697
49. Inoue K., Waks E. and Yamamoto Y., *Phys. Rev. Lett.*, 2002, 89: 037902
50. Chen X., Zhou C., Wu G. and Zeng H., *Appl. Phys. Lett.*, 2004, 84: 2691
51. Chen X., Zhou C., Wu G. and Zeng H., *Appl. Phys. Lett.*, 2004, 85: 1648
52. Muller A., Herzog T., Huttner B., Tittel W., Zbinden H. and Gisin N., *Appl. Phys. Lett.*, 1997, 70: 793–795
53. Stucki D., Gisin N., Guinnard O., Ribordy G. and Zbinden H., *New J. Phys.*, 2002, 4: 41.1–41.8
54. Bergh R.-A., *Fiber optic and laser sensors X.*, In: Udd E. and Depaula R.P. (eds) *Proc. SPIE*, 1992, 1795: 126–134
55. Ribordy G., Gautier J.-D., Zbinden H. and Gisin N., *Appl. Opt.*, 1998, 37: 2272–2277
56. Lutkenhaus N., *Phys. Rev. A*, 2000, 61: 052304
57. Cova S., Ghioni M., Lacaíta A., Samori C. and Zappa F., *Appl. Opt.*, 1996, 35: 1956–1976
58. Brown R.-G.-W., Ridley K.-D. and Rarity J.-G., *Appl. Opt.*, 1986, 25: 4122–4126
59. Bennett C. and Brassard G., *Quantum cryptography: public key distribution and coin tossing*, in: *Proc. Int. Conf. Comput. Syst. Signal Process.*, Bangalore, 1984: 175–179
60. Bennett C., Bessette F., Brassard G., et al., *Experimental quantum cryptography*, *J. Cryptol.*, 1992, 5(3): 3–28
61. Hughes R., Nordholt J., Derkacs D., et al., *Practical free-space quantum key distribution over 10 km in daylight and at night*, *New J. Phys.*, 2002, 4: 43.1–43.14
62. Kurtsiefer C., Zarda P., Halder M., et al., *A step towards global key distribution*, *Nature*, 2002, 419(3): 450
63. Zbinden H., Gautier J.-D., Gisin N., et al., *Interferometry with Faraday mirrors for quantum cryptography*, *Electron. Lett.*, 1997, 33(7): 586–588
64. Zhou C., Wu G., Chen X., et al., *“Plug and play” quantum key distribution system with differential phase shift*, *Appl. Phys. Lett.*, 2003, 83(9): 1692–1694
65. Zhou C. and Zeng H., *Time-division single-photon Sagnac interferometer for quantum key distribution*, *Appl. Phys. Lett.*, 2003, 82(5): 832–834
66. Wu G., Zhou C. and Zeng H., *Time-division phase modulated single-photon interference in a Sagnac interferometer*, *Chin. Sci. Bull.*, 2003, 48(16): 1704–1708
67. <http://optics.org/articles/news/8/11/13/1>
68. <http://optics.org/articles/news/9/6/3/1>
69. Bennett C., *Quantum cryptography using any two nonorthogonal states*, *Phys. Rev. Lett.*, 1992, 68(21): 3121–3124
70. Martinelli M., *A universal compensator for polarization changes induced by birefringence on a retracing beam*, *Opt. Commun.*, 1989, 72: 341–344
71. Levine B.-F. and Bethea C.-G., *Single photon detection at 1.3 um using a gated avalanche photodiode*, *Appl. Phys. Lett.*, 1984, 44(5): 553–555
72. Ekert A.-K., *Phys. Rev. Lett.*, 1991, 67: 661
73. Ribordy G., Gautier J.-D., Gisin N., Guinnard O. and Zbinden H., *Electron. Lett.*, 1998, 34(22): 2116
74. Buttler W.-T., Torgerson J.-R. and Lamoreaux S.-K., *New, efficient and robust, fiber-based quantum key distribution schemes*, *Phys. Lett. A*, 2002, 299: 38–42
75. Slutsky B.-A., Rao R., Sun P. and Fainman Y., *Phys. Rev. A.*, 1998, 57(4): 2382
76. Boileau J.-C., Gottesman D., Laflamme R., et al., *Robust polarization-based quantum key distribution over a collective-noise channel*, *Phys. Rev. Lett.*, 2004, 92: 017901