CHIN. PHYS. LETT. Vol. 36, No. 7 (2019) 070301

Experimental Point-to-Multipoint Plug-and-Play Measurement-Device-Independent Quantum Key Distribution Network *

Guang-Zhao Tang(唐光召)**, Shi-Hai Sun(孙仕海)**, Chun-Yan Li(李春燕)
College of Science, National University of Defense Technology, Changsha 410073

(Received 21 January 2019)

Measurement-device-independent quantum key distribution (MDI-QKD) offers a practical way to realize a star-type quantum network. Previous experiments on MDI-QKD networks can only support the point-to-point communication. We experimentally demonstrate a plug-and-play MDI-QKD network which can support the point-to-multipoint communication among three users. Benefiting from the plug-and-play MDI-QKD architecture, the whole network is automatically stabilized in spectrum, polarization, arrival time, and phase reference. The users only need the encoding devices, which means that the hardware requirements are greatly reduced. Our experiment shows that it is feasible to establish a point-to-multipoint MDI-QKD network.

PACS: 03.67.Dd, 03.67.Hk, 89.70.Cf DOI: 10.1088/0256-307X/36/7/070301

The fundamental laws of quantum mechanics ensure the information-theoretical security of quantum key distribution (QKD) for remote users.[1,2] Until now, various QKD systems and networks have been demonstrated by tremendous experiments.[3−6] Most of the QKD networks[3−5] apply the trusted relays to form the point-to-point links between a quantum transmitter and a quantum receiver. To reduce the hardware requirement and to increase the scalability, the point-to-multipoint architecture[6] is suggested to share those expensive resources in QKD systems, especially single-photon detectors (SPDs). A critical shortcoming of these QKD networks is that the relays have to be assumed to be trustworthy. As soon as any one of the relays is dishonest, the security of the whole network will have failed. Moreover, a QKD network with trusted relays still suffers from various loopholes originating from the gap between the theoretical models and the practical devices. Among those loopholes, the detection-related loopholes are considered as the main source of attacks.[7−9]

The measurement-device-independent QKD (MDI-QKD)[10−20] can not only eliminate all security loopholes on detection, but also provide a perfect star-type network architecture. In MDI-QKD, the users send the independently prepared encoding states to an untrusted measurement site (Charlie). Charlie measures the signals received and reveals the Bell states obtained. Then, the users broadcast the intensity and basis settings to generate the final secure key. The architecture of a traditional MDI-QKD network is shown in Fig. 1(a). An experiment[20] has been designed to show the feasibility of the traditional MDI-QKD network. It randomly switches any two users to the untrusted measurement site every two hours. Therefore, it still belongs to the point-to-point links. On the other hand, it requires complicate stabilization systems to calibrate the spectrum, polarization, arrival time, and phase reference of signals. It may become difficult to implement when more users are added. The plug-and-play MDI-QKD network,[16] which is shown in Fig. 1(b), contains the potential to establish a self-stabilized MDI-QKD network, which can support the point-to-multipoint communication.

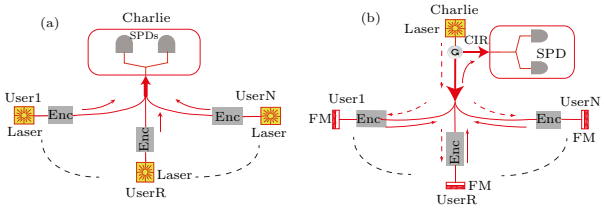

Fig. 1. MDI-QKD network. (a) The architecture of traditional MDI-QKD network. (b) The architecture of plug-and-play MDI-QKD network. Enc: encoder; Cir: circulator; FM: Faraday mirror.

In this study, we make a proof-of-principle demonstration of a self-stabilized plug-and-play MDI-QKD network which can support the point-to-multipoint communication. By encoding the signals launched by SynL1 and SynL3 subsequently, David can communicate with Alice and Bob simultaneously. The signal laser and SPDs are in the charge of Charlie. Alice, Bob, and David only need the encoding devices. Benefiting from the plug-and-play MDI-QKD architecture, the whole network is self-stabilized in spectrum, polarization, arrival time, and phase reference. Our network simplifies the stabilization systems and presents a practical way to realize a point-to-multipoint star-type MDI-QKD network.

We make a proof-of-principle experiment to demonstrate the feasibility of the plug-and-play MDI-QKD network. The experimental setup is shown in Fig. 2(a). Charlie controls a signal laser (1550 nm), three synchronization lasers (SynL,1310 nm), and four SPDs. The whole system is working at the repetition rate of 1 MHz. The homemade signal laser is internally modulated into a pulse train with a width of 2 ns (FWHM). We use an asymmetric Mach–Zehnder interferometer (AMZI) to separate the pulses of the signal laser into two time bins with 25 ns time delay. Alice, Bob, and David only have the modulation devices including PMs and AMs for encoding. For the X basis, the key bit is encoded into the relative phase, 0

*Supported by the National Natural Science Foundation of China under Grant Nos 11674397 and 61671455.
**Corresponding author. Email: tang130124@163.com; shsun1983@126.com
© 2019 Chinese Physical Society and IOP Publishing Ltd

or π, by PM1. For the Z basis, the key bit is encoded into the time bin, 0 or 1, by AM1. PM2 is used for the phase randomization. We use a sawtooth wave with a repetition rate of 15 kHz to make the global phase of each optical pulse randomize in the range of $[0, 2\pi]$.

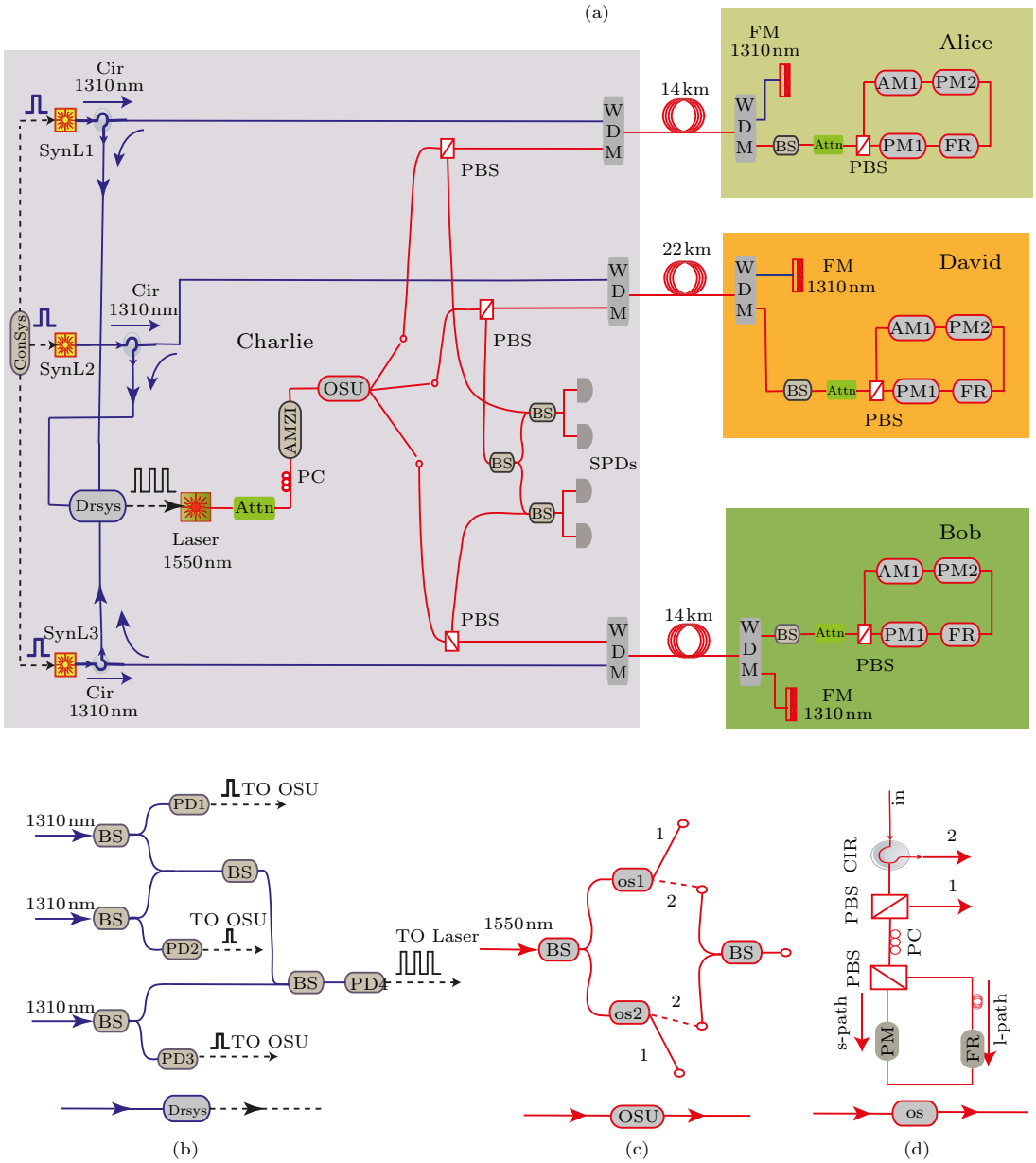

Fig. 2. (a) Experimental setup of the plug-and-play MDI-QKD network. Charlie controls all the lasers, including a signal laser (1550 nm) and three synchronization lasers (1310 nm). The optical switch unit is used to assign the signals. When the pulses of the SynLs are reflected back by the Faraday mirror (1310 nm), a homemade photoelectric detector (PD) is utilized to detect them and generate the driving clock for the signal laser. Alice, Bob, and David encode the signals and send them back to Charlie. Charlie uses four single-photon detectors (SPDs) to realize the Bell-state measurement. ConSys: control system; Drsys: driving system; SynL: synchronization laser; Attn: attenuator; PC: polarization controller; AMZI: asymmetric Mach-Zehnder interferometer; OSU: optical switch unit; WDM: wavelength division multiplexer; PM: phase modulator; AM: amplitude modulator; BS: beam splitter; PBS: polarizing beam splitter; CIR: circulator; FR: Faraday rotator; SPDs: single-photon detectors. (b) Schematic of the driving system. PD: photoelectric detector. (c) Schematic of the optical switch unit. (d) Schematic of the optical switch.[21]

Our network can support communication for any two users. For example, if Alice wants to communicate with Bob, we can use SynL1 and SynL3 to generate the signals of Bob and Alice, which has been demonstrated in experiment.[18] Here we put emphasis on the point-to-multipoint communication among three users, namely, David communicates with Alice and Bob simultaneously. David needs to encode the signals launched by SynL1 and SynL3 independently. Alice and Bob need to encode the signals launched by SynL2. We use the setup shown in Fig. 2(b) to generate the driving clock of the signal laser and the optical switch unit. The synchronization pulses of SynL1 and SynL3 are sent from Charlie to Alice and Bob corre-

spondingly. After being reflected back by a Faraday mirror (1310 nm), they are detected by the photoelectric detectors (PD). The output of PD4 is used to drive the signal laser (1550 nm) to generate the signal pulses of David. Similarly, the synchronization pulses of SynL2 are sent from Charlie to David, reflected back by the Faraday mirror (1310 nm), and detected by the PDs. The output of PD4 is used to drive the signal laser (1550 nm) to generate the signal pulses of Alice and Bob.

Figure 2(c) shows the diagram of the optical switch unit (OSU), which is used to assign the signals to the correct users. We use the setup shown in Fig. 2(d) to serve as the optical switch (OS).[21] By modulating the relative phase shift (ϕ) between the two subsequent passages of the light (s-path and l-path) through the phase modulator, we can realize an arbitrary optical splitting ratio between output1 and output2. The extinction ratio can exceed 20 dB with an outstanding feature of stabilization.[21] We modulate ϕ to 0 (or π), the optical pulses output at output1 (or output2).

In our network, all users share the signal laser and the AMZI, which means that there is naturally no mismatch in spectral, in pulse waveform, and in phase-reference-frame at all. As to the polarization mode, the plug-and-play architecture can automatically compensate for the birefringence effects. The temporal mode difference between David and Alice, David and Bob can be expressed as

$$\begin{aligned}\Delta t^{\mathrm{AD}} &= (t_{1310}^{\mathrm{C}\rightleftarrows\mathrm{D}} + t_{1550}^{\mathrm{C}\rightleftarrows\mathrm{A}}) - (t_{1310}^{\mathrm{C}\rightleftarrows\mathrm{A}} + t_{1550}^{\mathrm{C}\rightleftarrows\mathrm{D}}) \\ &= \Delta t_0^{\mathrm{AD}} + (1/v_{1550} - 1/v_{1310})\Delta L^{\mathrm{AD}}, \quad (1) \\ \Delta t^{\mathrm{BD}} &= (t_{1310}^{\mathrm{C}\rightleftarrows\mathrm{D}} + t_{1550}^{\mathrm{C}\rightleftarrows\mathrm{B}}) - (t_{1310}^{\mathrm{C}\rightleftarrows\mathrm{B}} + t_{1550}^{\mathrm{C}\rightleftarrows\mathrm{D}}) \\ &= \Delta t_0^{\mathrm{BD}} + (1/v_{1550} - 1/v_{1310})\Delta L^{\mathrm{BD}}, \quad (2)\end{aligned}$$

where $\Delta t_0^{\mathrm{AD(BD)}} = (1/v_{1550} - 1/v_{1310})(L_0^{\mathrm{C}\rightleftarrows\mathrm{D}} - L_0^{\mathrm{C}\rightleftarrows\mathrm{A(B)}})$, and $\Delta L^{\mathrm{A(B)D}} = \Delta L^{\mathrm{C}\rightleftarrows\mathrm{D}} - \Delta L^{\mathrm{C}\rightleftarrows\mathrm{A(B)}}$, $L^{\mathrm{C}\rightarrow\mathrm{A(B,D)}}$ represents the fiber length between Charlie and Alice (Bob, David), and $\Delta L = \alpha_{\mathrm{T}} L^0 \Delta T$ with $\alpha_{\mathrm{T}} = 5.4 \times 10^{-7}/^{\circ}\mathrm{C}$ being the thermal expansion coefficient of fiber, and ΔT representing the change of temperature. The second part of Eqs. (1) and (2) are negligible.[18] Therefore, the arrival time differences of signals between David and Alice, David and Bob are constants, which can be compensated by adjusting the time delay between the SynLs with high-resolution (10 ps) delay chips.

Our network is automatically stabilized in spectrum, polarization, arrival time, and phase reference, while the previous experiment[20] needs the polarization stabilization system, the phase stabilization system, and the wavelength calibration system to realize the high quality Hong–Ou–Mandel (HOM) interference. Thus the stabilization systems are greatly simplified in our experiment.

At the measurement site, four commercial InGaAs SPDs (two id201 of id Quantique; two single-photon detectors of QuantumCTek) are used to record the coincidences. For SPDs of id201, we chose the efficiency to be 10% with a gate width of 2.5 ns. The dead time is 10 μs with a dark count rate of 6×10^{-6} per gate. As to the SPDs of QuantumCTek, we adjust the parameters (efficiency, gate width, and dead time) to make the performance in accordance with that of the SPDs of id201.

We modulate the signal pulses of Alice and David (Bob and David) into three different intensities, namely, signal state intensity ($\mu = 0.3$ for Alice and David, $\mu = 0.4$ for Bob and David), decoy state intensity ($\nu = 0.1$) and vacuum state intensity ($\omega = 0.01$). The experimental gains are listed in Tables 1 and 3, and the quantum bit error rates (QBER) are listed in Tables 2 and 4. The QBERs of Z-basis are due to the extinction ratio of AM1 and the background counts (Rayleigh backscattering), while in X-basis, the vacuum and multiphoton components of weak coherent states cause accidental coincidences which introduce a typical error rate of 25%.

Table 1. Experimental values of gains $Q_{I_{\mathrm{A}}I_{\mathrm{D}}}^{Z(X)}(10^{-5})$. Here I_{A} and I_{D} are the optical intensities of Alice and David.

	Z-basis			X-basis		
	I_{A}					
I_{D}	μ	ν	ω	μ	ν	ω
μ	0.892	0.2971	0.04314	1.372	0.9287	0.7347
ν	0.2894	0.0993	0.0143	0.6725	0.2706	0.1068
ω	0.0413	0.0134	0.0015	0.325	0.0535	0.00455

Table 2. Experimental values of QBERs. Here I_{A} and I_{D} are the optical intensities of Alice and David.

	Z-basis			X-basis		
	I_{A}					
I_{D}	μ	ν	ω	μ	ν	ω
μ	0.0138	0.0310	0.1730	0.267	0.3626	0.4740
ν	0.0233	0.0329	0.1556	0.2905	0.2954	0.4128
ω	0.1014	0.1011	0.1222	0.4439	0.3885	0.3878

Table 3. Experimental values of gains $Q_{I_{\mathrm{B}}I_{\mathrm{D}}}^{Z(X)}$ (10^{-5}). Here I_{B} and I_{D} are the optical intensities of Bob and David.

	Z-basis			X-basis		
	I_{B}					
I_{D}	μ	ν	ω	μ	ν	ω
μ	1.242	0.3605	0.0572	1.925	1.037	1.139
ν	0.3742	0.1314	0.0195	0.7739	0.2592	0.1315
ω	0.0527	0.0171	0.0023	0.428	0.0757	0.0090

Table 4. Experimental values of QBERs. Here I_{B} and I_{D} are the optical intensities of Bob and David.

	Z-basis			X-basis		
	I_{B}					
I_{D}	μ	ν	ω	μ	ν	ω
μ	0.0151	0.0384	0.1628	0.277	0.339	0.462
ν	0.0287	0.0450	0.1569	0.294	0.286	0.388
ω	0.1412	0.1422	0.1957	0.460	0.382	0.420

In the asymptotic case, the secure key rate is given by[10,22]

$$R \geq q\{Q_{\mu\mu,11}^{Z,L}[1 - H(e_{11}^{X,U})] - Q_{\mu\mu}^{Z} f H(E_{\mu\mu}^{Z})\}, \quad (3)$$

where q is the proportion of pulses when both Alice and Bob send out signal states in the Z basis, $Q_{\mu\mu}^{Z}$ and $E_{\mu\mu}^{Z}$ are the overall gain and error rate when Alice and Bob send the signal states in the Z basis, and they can be directly measured from the experiment: $Q_{\mu\mu,11}^{Z,L} = \mu^2 e^{-2\mu} Y_{11}^{Z,L}$, where $Y_{11}^{Z,L}$ is a lower bound of

the yield of single photon states in the Z basis, $e_{11}^{X,U}$ is an upper bound of the QBER of the single photon states in the X basis, $f = 1.16$ is the error correction efficiency, and $H(e) = -e\log_2 e - (1-e)\log_2(1-e)$ is the binary Shannon entropy function.

Here $Y_{11}^{Z,L}$ and $e_{11}^{X,U}$ can be estimated using an analytical method with two decoy states according to Ref. [22], and $Y_{11}^{Z,L}$ is given by

$$\begin{aligned} Y_{11}^{Z,L} =& [(\mu_a^2 - \omega_a^2)(\mu_b - \omega_b)Q_{M1}^Z - (\nu_a^2 - \omega_a^2)(\nu_b \\ & - \omega_b)Q_{M2}^Z]/[(\mu_a - \omega_a)(\mu_b - \omega_b)(\nu_a \\ & - \omega_a)(\nu_b - \omega_b)(\mu_a - \nu_a)], \end{aligned} \tag{4}$$

where $Q_{M1}^Z = Q_{\nu_a\nu_b}^Z e^{(\nu_a+\nu_b)} + Q_{\omega_a\omega_b}^Z e^{(\omega_a+\omega_b)} - Q_{\nu_a\omega_b}^Z e^{(\nu_a+\omega_b)} - Q_{\omega_a\nu_b}^Z e^{(\omega_a+\nu_b)}$, and $Q_{M2}^Z = Q_{\mu_a\mu_b}^Z e^{(\mu_a+\mu_b)} + Q_{\omega_a\omega_b}^Z e^{(\omega_a+\omega_b)} - Q_{\mu_a\omega_b}^Z e^{(\mu_a+\omega_b)} - Q_{\omega_a\mu_b}^Z e^{(\omega_a+\mu_b)}$.

We can obtain $e_{11}^{X,U}$ as follows:

$$\begin{aligned} e_{11}^{X,U} =& \frac{1}{(\nu_a - \omega_a)(\nu_b - \omega_b)Y_{11}^{X,L}} \\ & \cdot [Q_{\nu_a\nu_b}^X E_{\nu_a\nu_b}^X e^{(\nu_a+\nu_b)} + Q_{\omega_a\omega_b}^X E_{\omega_a\omega_b}^X e^{(\omega_a+\omega_b)} \\ & - Q_{\nu_a\omega_b}^X E_{\nu_a\omega_b}^X e^{(\nu_a+\omega_b)} - Q_{\omega_a\nu_b}^X E_{\omega_a\nu_b}^X e^{(\omega_a+\nu_b)}], \end{aligned} \tag{5}$$

where $Y_{11}^{X,L}$ can be achieved with a similar method for $Y_{11}^{Z,L}$.

The parameters we estimated are listed in Tables 5 and 6.

Table 5. Parameters estimated in the process of secure key rate estimation: $Q_{M1(2),A}^{Z(X)}$ (10^{-5}), and $Y_{11,A}^{Z(X),L}$ (10^{-4}).

	$Q_{M1}^{Z(X)}$	$Q_{M2}^{Z(X)}$	$Y_{11}^{Z(X),L}$
Z-basis	0.0919	1.512	0.734
X-basis	0.1563	1.060	2.275

Table 6. Parameters estimated in the process of secure key rate estimation: $Q_{M1(2),B}^{Z(X)}$ (10^{-5}), and $Y_{11,B}^{Z(X),L}$ (10^{-4}).

	$Q_{M1}^{Z(X)}$	$Q_{M2}^{Z(X)}$	$Y_{11}^{Z(X),L}$
Z-basis	0.1219	1.690	1.650
X-basis	0.0945	1.932	1.136

About 1.2×10^{11} signal pulses are sent out in our experiment. We chose $q = \frac{1}{36}$ for the three optical intensity states which are prepared with the same probability. Therefore, we obtain that $Y_{11,AD}^{Z,L} = 7.34 \times 10^{-5}$ and $e_{11,AD}^{X,U} = 14.65\%$, $Y_{11,BD}^{Z,L} = 1.65 \times 10^{-4}$ and $e_{11,BD}^{X,U} = 5.54\%$. The secure key rate for Alice and David can reach 1×10^{-8} bits per pulse, and the secure key rate for Bob and David is 1.83×10^{-7} bits per pulse.

We remark that, according to the security analysis in Ref. [21] the energy and arrival time of signal pulses should be monitored precisely to acquire the certain information about the photon-number distribution and the timing mode in plug-and-play MDI-QKD network. In our proof-of-principle demonstration, however, we cut down the energy of signal pulses to reduce the Rayleigh backscattering (RBS). The intensity detector cannot monitor the energy of signal pulses successfully with such a low pulse energy level. However, it does not affect the feasibility of our plug-and-play MDI-QKD network, since we can adopt the scheme of pulse trains to reduce the RBS.[23] The reduction of the RBS is demonstrated with an arbitrary waveform generator (Tektronix AWG7082C) worked at 1 MHz repetition rate in gated mode. Another waveform generator (KEYSIGHT 33250A) is used to offer the gate signals (5 kHz with a width of 5 μs). The background counts can reach 10^{-6} per gate.

On the other hand, the performance can be significantly improved by optimizing the parameters and applying the high-speed SPDs. It has been demonstrated that the transmission distance and secure key rate are substantially improved using the superconducting nanowire single photon detectors (SNSPD) with an efficiency over 40%.[14]

In conclusion, we have made a proof-of-principle demonstration of a self-stabilized plug-and-play MDI-QKD network over an asymmetric channel setting. In our network, David can communicate with Alice and Bob simultaneously by encoding the signals launched by SynL1 and SynL3 subsequently. Our experiment presents a practical way to realize a star-type MDI-QKD network which greatly reduces the hardware requirements for users.

References

[1] Bennett C H and Brassard G 1984 *Int. Conf. Comput. Syst. Signal Process* (Bangalore India) (New York: IEEE) p 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Peev M et al 2009 *New J. Phys.* **11** 075001
[4] Chen T Y et al 2010 *Opt. Express* **18** 27217
[5] Sasaki M et al 2011 *Opt. Express* **19** 10387
[6] Fröhlich B et al 2013 *Nature* **501** 69
[7] Xu F et al 2010 *New J. Phys.* **12** 113026
[8] Lydersen L et al 2010 *Nat. Photon.* **4** 686
[9] Sun S H et al 2011 *Phys. Rev. A* **83** 062331
[10] Lo H K et al 2012 *Phys. Rev. Lett.* **108** 130503
[11] Rubenok A et al 2013 *Phys. Rev. Lett.* **111** 130501
[12] Liu Y et al 2013 *Phys. Rev. Lett.* **111** 130502
[13] Tang Z Y et al 2014 *Phys. Rev. Lett.* **112** 190503
[14] Tang Y L et al 2014 *Phys. Rev. Lett.* **113** 190501
[15] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
[16] Xu F 2015 *Phys. Rev. A* **92** 012333
[17] Comandar L C, Lucamarini M, Fröhlich B, Dynes J F et al 2016 *Nat. Photon.* **10** 312
[18] Tang G Z, Sun S H, Xu F, Chen H, Li C Y and Liang L M 2016 *Phys. Rev. A* **94** 032326
[19] Tang G Z, Sun S H, Chen H, Li C Y and Liang L M 2016 *Chin. Phys. Lett.* **33** 120301
[20] Tang Y L, Yin H L, Zhao Q, Liu H et al 2016 *Phys. Rev. X* **6** 011024
[21] Lucio-Martinez I, Chan P, Mo X, Hosier S and Tittel W 2009 *New J. Phys.* **11** 095001
[22] Xu F, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007
[23] Sun S H, Ma H Q, Han J J, Liang L M and Li C Z 2010 *Opt. Lett.* **35** 1203