PHYSICAL REVIEW A **94**, 032326 (2016)

Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution

Guang-Zhao Tang,[1] Shi-Hai Sun,[1,*] Feihu Xu,[2,†] Huan Chen,[1] Chun-Yan Li,[1] and Lin-Mei Liang[1,3,‡]

[1]*College of Science, National University of Defense Technology, Changsha 410073, People's Republic of China*

[2]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*

[3]*State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, People's Republic of China*

(Received 9 June 2016; published 27 September 2016)

Measurement-device-independent quantum key distribution (MDI-QKD) is immune to all security loopholes on detection. Previous experiments on MDI-QKD required spatially separated signal lasers and complicated stabilization systems. In this paper, we perform a proof-of-principle experimental demonstration of plug-and-play MDI-QKD over an asymmetric channel setting with a single signal laser in which the whole system is automatically stabilized in spectrum, polarization, arrival time, and phase reference. Both the signal laser and the single-photon detectors are in the possession of a common server. A passive timing-calibration technique is applied to ensure the precise and stable overlap of signal pulses. The results pave the way for the realization of a quantum network in which the users only need the encoding devices.

DOI: 10.1103/PhysRevA.94.032326

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows the two legitimate parties, Alice and Bob, to share an information-theoretical secure key guaranteed by the laws of quantum physics. Despite tremendous experimental effort being made in the field [3–5], an important problem in current QKD implementations is the gap between its theory and its practice [6–10]. To close this gap, three main approaches have been developed. The first one is the security patch [11,12], but it is difficult to include all potential and unnoticed security loopholes. The second one is the device-independent QKD (DI-QKD) [13–15]. This approach is still challenging with current technology since it requires a loophole-free Bell test. The third approach is the measurement-device-independent QKD (MDI-QKD) [16], which removes all detection-related security loopholes. Such a loophole is arguably the most important issue identified in conventional QKD implementations [7–10]. Therefore, MDI-QKD is of great importance to promote the security of practical QKD systems. In addition, with current technology, MDI-QKD is suitable for both long-distance communication and metropolitan networks [17,18].

Achievements of MDI-QKD have been made in both theory [19–23] and experiment [17,24–30]. The experimental demonstration of MDI-QKD requires the indistinguishability of photons from Alice and Bob, mainly in three dimensions: spectrum, polarization, and timing. To solve this challenge, the active stabilization systems were normally utilized in previous experiments. For example, the feedback temperature-control units for the distributed feedback lasers [25,28] or frequency-locked lasers [24,27] were employed to match the spectral mode. The feedback temporal-control system was utilized to calibrate the arrival time of the signals [24,28]. The phase- (or polarization-) stabilization system was always essential in the time-bin phase-encoding (or polarization-encoding) scheme. Recently, many proposals and demonstrations have been made to mitigate the complexity in the implementations of MDI-QKD [18,31–33]. In particular, a promising scheme is the plug-and-play MDI-QKD [18,33], which greatly reduces the experimental complexity of mode matching and reference-frame alignment. But, since the signal laser source and single-photon detectors (SPDs) are in the charge of an untrusted server, plug-and-play MDI-QKD is vulnerable to source attacks [6,7,9]. Fortunately, with the security analysis reported in Ref. [18], plug-and-play MDI-QKD can be implemented even with a single untrusted source. However, so far, an experimental demonstration of plug-and-play MDI-QKD is still missing, except for a proof-of-concept test [33] with polarization encoding over a free space channel within a few meters. This proof-of-concept test is not in accordance with the plug-and-play architecture and still needs some stabilization measures.

In this paper, we report a demonstration of plug-and-play MDI-QKD using time-bin phase encoding over an asymmetric channel setting in which the two channels from Alice and Bob to Charlie are 14- and 22-km standard optical fibers. The encoding optical pulses of Alice and Bob come from a single homemade laser held by Charlie, which ensures that no mismatch exists in both pulse waveform and optical spectrum. Thanks to the plug-and-play architecture [34], the polarization state is automatically calibrated and stabilized. The encoding optical pulses of Alice and Bob share the same reference frame. In the asymmetric channel setting, an experimental challenge is how to precisely match the timing of pulses, returned from Alice and Bob, respectively, over two mismatched channels. We developed a passive timing-calibration method by using two synchronization lasers (operating at 1310 nm) and multiplexing them with the signal laser (operating at 1550 nm) via wavelength division multiplexing (WDM).

*shsun@nudt.edu.cn
†fhxu@mit.edu
‡nmliang@nudt.edu.cn

II. EXPERIMENT

The experimental setup of plug-and-play MDI-QKD is illustrated in Fig. 1(a). We implement the time-bin phase-encoding scheme [17,24,25,28,29]. The signal laser source (1550 nm) and detectors are held by a common server (Charlie). The signal laser is internally modulated into a pulse train with a width of 2 ns (FWHM) at a 1-MHz repetition rate. An AMZI is utilized to separate the pulses into two time bins with a 20-ns time delay. Alice and Bob only have the modulation devices including PMs and AMs for encoding. The key bit in the X basis is encoded into the relative phase 0 or π by PM1, whereas the key bit in the Z basis is encoded into the time bin 0 or 1 by AM1. Figure 1(b) illustrates the structure of AM1 [35]. AM1 contains a normal PBS, a PBS with a 45° rotation from the optical axis, a phase modulator, and a Faraday rotator in which different optical intensities at the output port of the PBS are realized by modulating the relative phase between the long path (L) and the short path (S) [36]. PM2 is used for the active phase randomization, and AM2 is used to implement the decoy states.

The signal pulses travel through a single-mode fiber spool of 14 km (22 km) from Charlie to Alice (Bob). After being modulated by Alice and Bob, the pulses return to Charlie to interfere at the BS. A coincident detection at alternative time bins indicates a successful BSM. At the measurement site, the BSM is implemented with a polarization-maintaining BS and two commercial InGaAs SPDs (ID201) with an efficiency of 10% and a gate width of 2.5 ns. The dead time is 10 μs with a dark count rate of 6×10^{-6} per gate. A Bell state (singlet) is successfully postselected when a coincidence of two SPDs happens at alternative time bins. After Charlie announces the result of the partial BSM, Alice and Bob shift the raw key.

The crucial aspect in the experiment is the indistinguishability of signal pulses from Alice and Bob, mainly in three dimensions: spectrum, polarization, and timing. Errors would occur if any mismatch exists in these dimensions. In our system, Alice and Bob share the same signal laser, which guarantees no mismatch in the spectrum and in the pulse waveform. The active phase randomization is implemented to eliminate the partial-phase-randomization attack. In our proof-of-principle demonstration, a sawtooth wave with a repetition rate of 55 KHz (15 KHz) is applied to the PM2 of Alice (Bob) [37] to globally randomize the phase of each optical pulse in the range of $[0, 2\pi]$. Alice's and Bob's time bins come from the same AMZI, so they share the same phase reference frame. For the polarization mode, the plug-and-play architecture can automatically compensate for the birefringence effects [34].

In the asymmetric channel setting, the pulses of Alice and Bob travel different lengths of fibers. A challenge is to match the temporal mode. We use two additional SynLs (1310 nm) to calibrate the arrival time. The whole system is synchronized in the following manner: The SynL pulses are sent from Charlie to Alice (Bob), reflected back by a Faraday mirror (1310 nm), and detected by a PD. The output of the PD is used to drive the signal laser (1550 nm) to generate the signal pulses of Bob (Alice). The temporal mode difference between Alice and Bob can be expressed as

$$\begin{aligned}\Delta t &= \left(t^{1310}_{C\rightleftarrows B} + t^{1550}_{C\rightleftarrows A}\right) - \left(t^{1310}_{C\rightleftarrows A} + t^{1550}_{C\rightleftarrows B}\right) \\ &= \Delta t_0 + (1/v_{1550} - 1/v_{1310})\Delta L, \end{aligned} \quad (1)$$

where $\Delta t_0 = (1/v_{1550} - 1/v_{1310})(L^0_{C\rightleftarrows B} - L^0_{C\rightleftarrows A})$ and $\Delta L = \Delta L_{C\rightleftarrows B} - \Delta L_{C\rightleftarrows A}$. $L_{C\rightarrow B}$ represents the fiber length between Charlie and Bob. $\Delta L = \alpha_T L^0 \Delta T$, where $\alpha_T = 5.4 \times 10^{-7}/°\mathrm{C}$ is the thermal expansion coefficient of the fiber and ΔT represents the change in temperature. The second term in Eq. (1) is negligible since it only induces 0.14 ps with a 10 °C temperature change [38]. Therefore, the arrival time difference of signals between Alice and Bob is a constant which can be compensated by adjusting the time delay between two SynLs with a delay chip. The temporal mode mismatch depends on the resolution of the delay chip (10 ps) which is much smaller than the width of the signal pulse (2 ns). This ensures a high-visibility interference.

TABLE I. Experimental values of gains $Q^{Z(X)}_{I_A I_B}(\times 10^{-4})$. I_A and I_B are the optical intensities of Alice and Bob.

	Z basis			X basis		
	μ	ν	ω	μ	ν	ω
		I_A			I_B	
μ	1.819	0.547	0.125	9.018	4.347	3.408
ν	0.624	0.217	0.0378	4.316	0.925	0.323
ω	0.130	0.0386	0.0050	5.207	0.323	0.0115

III. RESULTS

In our demonstration, the optical pulses are modulated into three different intensities according to the decoy state method [39], namely, signal state intensity ($\mu = 0.4$), decoy state intensity ($\nu = 0.1$), and vacuum state intensity ($\omega = 0.01$). The optical intensities of a certain basis are put into nine pairs. The experimental gains and quantum bit error rates (QBERs) for different intensity combinations are listed in Tables I and II. The QBERs of the Z basis are due to the extinction ratio of AM1 and the background counts (Rayleigh backscattering and detectors' dark counts). In the ideal case, the QBERs of the Z basis should be 0. Whereas, in the X basis, the vacuum and multiphoton components of weak coherent states cause

TABLE II. Experimental values of QBERs. Error bars represent one standard deviation.

	Z basis			X basis		
	μ	ν	ω	μ	ν	ω
		I_A			I_B	
μ	0.0188 ±0.001	0.0378 ±0.004	0.136 ±0.009	0.269 ±0.007	0.341 ±0.007	0.483 ±0.009
ν	0.0356 ±0.003	0.0450 ±0.003	0.133 ±0.013	0.351 ±0.008	0.278 ±0.012	0.428 ±0.012
ω	0.151 ±0.005	0.133 ±0.01	0.194 ±0.04	0.484 ±0.008	0.432 ±0.015	0.368 ±0.052

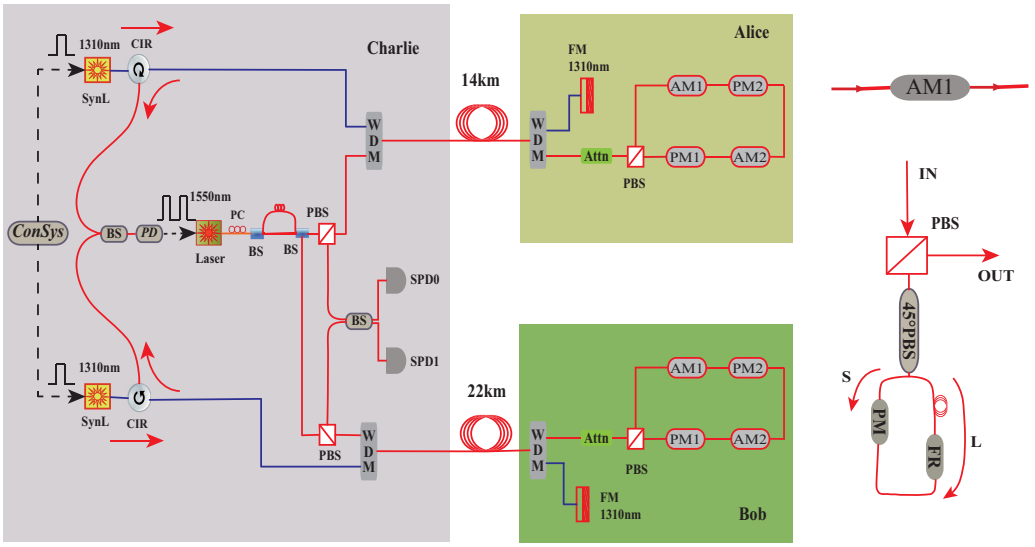

FIG. 1. (a) Experimental setup of the plug-and-play MDI-QKD. The synchronization optical pulses (1310 nm) are sent out by Charlie. They travel to Alice (Bob) and are reflected back by a Faraday mirror (1310 nm). A homemade photoelectric detector (PD) is utilized to detect them and output the system clock. Then, the signal laser (1550 nm) generates the optical pulses of Bob (Alice). The time bins are generated by an asymmetric Mach-Zehnder interferometer (AMZI) in Charlie. The clients (Alice and Bob) receive the time-bin pulses and encode the bits. Then, the signals are reflected back to Charlie for the partial Bell state measurement (BSM). ConSys: control system; SynL: synchronization laser; CIR: circulator; BS: beam splitter; PC: polarization controller; WDM: wavelength division multiplexer; Attn: attenuator; FM: Faraday mirror; SPD. (b) Schematic of the amplitude modulator (AM1): PBS: polarizing beam splitter; 45° PBS: polarizing beam splitter with 45° from the optical axis; PM: phase modulator; FR: Faraday rotator.

accidental coincidences which introduce an error rate of 50%. Thus, the error rate of the X basis has an expected value of 25%.

The secure key is extracted from the data when both Alice and Bob encode their bits using signal states (μ) in the Z basis. The rest of the data are applied to estimate the parameters used in the secure key rate calculation. In the asymptotic case, the secure key rate is given by [16]

$$R \geqslant q\{Q^{Z,L}_{\mu\mu,11}[1 - H(e^{X,U}_{11})] - Q^{Z}_{\mu\mu} f H(E^{Z}_{\mu\mu})\}, \qquad (2)$$

where q, $Q^{Z}_{\mu\mu}$, and $E^{Z}_{\mu\mu}$ are the possibility, overall gain, and QBER when Alice and Bob send the signal states in the Z basis. $Q^{Z,L}_{\mu\mu,11} = \mu^2 e^{-2\mu} Y^{Z,L}_{11}$, where $Y^{Z,L}_{11}$ is a lower bound of the yield of single-photon states in the Z basis; $e^{X,U}_{11}$ is an upper bound of the QBER of the single-photon states in the X basis; $Y^{Z,L}_{11}$ and $e^{X,U}_{11}$ can be estimated from the decoy state method; f is the error correction efficiency; H is the binary Shannon entropy function. A total number of $N = 6.14 \times 10^{10}$ pulses is sent out in the experiment. We take the values $q = \frac{1}{18}$ and $f = 1.16$ in our calculation. By using the analytical bounds derived in Ref. [39], we obtain that $Y^{Z,L}_{11} = 2.2 \times 10^{-3}$ and $e^{X,U}_{\mu\mu,11} = 5.07\%$ (see the Appendix). Finally, a secure key rate of $R = 4.7 \times 10^{-6}$ bits per pulse is demonstrated.

IV. CONCLUSION AND DISCUSSION

We discuss the limitations of our proof-of-principle experiment and possible solutions. First, the plug-and-play MDI-QKD is vulnerable to various source attacks [6,7,9] since the signal source is totally controlled by an untrusted server. By keeping a few assumptions including the single-mode assumption, the phase-randomization assumption, and the trust of the monitoring devices, a complete security analysis for plug-and-play MDI-QKD was derived in Ref. [18]. It shows that, with careful source monitoring, we can rigorously derive a lower bound of the secure key generation rate even with an unknown and untrusted source. According to the security analysis in Ref. [18], the energy and arrival time of each signal pulse should be monitored precisely to acquire the certain information about the photon-number distribution and the timing mode. In our demonstration, however, we cut down the energy of signal pulses to reduce the Rayleigh backscattering, which leads to the fact that that the intensity detector cannot monitor such weak energy. Hence, the monitor unit was not implemented. This can be improved by using the scheme of pulse trains as demonstrated in conventional plug-and-play QKDs [34,40]. Second, in our implementation, the parameters were not optimized, and the secure key rate was only calculated in the asymptotic case. A full parameter optimization and the finite key effect can be considered by using the theory in Ref. [22]. Lastly, the secure key generation rate can be significantly improved by increasing the repetition rate and the detector efficiency [28].

In conclusion, we have performed a proof-of-principle demonstration of self-stabilized asymmetric plug-and-play MDI-QKD over a 36-km fiber. The homemade laser sources and expensive detectors are provided by a common server. The polarization and phase can be automatically calibrated and stabilized. The passive time-calibration technique ensures

a precise and stable interference of photons from two remote parties. The techniques demonstrated in our experiment greatly improve the practicability of MDI-QKD and pave the way for a MDI quantum network with an untrusted network server.

ACKNOWLEDGMENTS

We thank V. Makarov for the helpful discussions. This work is supported by the National Natural Science Foundation of China, Grants No. 11304391, No. 11674397, and No. 61671455. L.-M.L. is supported by the Program for New Century Excellent Talents (NCET). F. X. thanks NSERC PDF for the support.

APPENDIX: SECURE KEY RATE ESTIMATION

The secure key rate is calculated with an analytical method with two decoy states according to Ref. [39]. $Y_{11}^{Z,L}$ is given by

$$Y_{11}^{Z,L}=\frac{(\mu_a^2-\omega_a^2)(\mu_b-\omega_b)Q_Z^{M1}-(\nu_a^2-\omega_a^2)(\nu_b-\omega_b)Q_Z^{M2}}{(\mu_a-\omega_a)(\mu_b-\omega_b)(\nu_a-\omega_a)(\nu_b-\omega_b)(\mu_a-\nu_a)}, \tag{A1}$$

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

TABLE III. Parameters estimated in the process of secure key rate estimation. $Q_\lambda^{M1(2)}(10^{-4})$, $Y_{11}^{\lambda,L}(10^{-3})$ with $\lambda\in\{X,Z\}$.

	Q_λ^{M1}	Q_λ^{M2}	$Y_{11}^{\lambda,L}$
Z	0.1846	3.668	2.219
X	0.4353	10.016	4.40

$e_{11}^{X,U}$ is

$$\begin{aligned}e_{11}^{X,U}=&\frac{1}{(\nu_a-\omega_a)(\nu_b-\omega_b)Y_{11}^{X,L}}\\&\times\left[Q_X^{\nu_a\nu_b}E_X^{\nu_a\nu_b}e^{(\nu_a+\nu_b)}+Q_X^{\omega_a\omega_b}E_X^{\omega_a\omega_b}e^{(\omega_a+\omega_b)}\right.\\&\left.-Q_X^{\nu_a\omega_b}E_X^{\nu_a\omega_b}e^{(\nu_a+\omega_b)}-Q_X^{\omega_a\nu_b}E_X^{\omega_a\nu_b}e^{(\omega_a+\nu_b)}\right],\end{aligned} \tag{A2}$$

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

By using the above equations, we estimate the parameters listed in Table III. In the secure key calculation, we assume an error correction code with $f=1.16$ and choose $q=\frac{1}{18}$, which is due to the fact that the three optical intensity states are prepared with the same probability.

[1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **92**, 201104 (2008).
[4] Y. Liu, T. Y. Chen, J. Wang, W. Q. Cai, X. Wan, and L. K. Chen *et al.*, Opt. Express **18**, 8587 (2010).
[5] S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, G. C. Guo, and Z. F. Han, Opt. Lett. **37**, 1008 (2012).
[6] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[7] F. Xu, B. Qi, and H. K. Lo, New J. Phys. **12**, 113026 (2010).
[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[9] S. H. Sun, M. S. Jiang, and L. M. Liang, Phys. Rev. A **83**, 062331 (2011).
[10] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).
[11] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).
[12] T. F. da Silva, G. B. Xavier, G. P. Termorao, and J. P. von der Weid, Opt. Express **20**, 18911 (2012).
[13] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[14] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[15] M. Curty and T. Moroder, Phys. Rev. A **84**, 010304(R) (2011).
[16] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[17] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, and M.-Q. Huang *et al.*, Phys. Rev. X **6**, 011024 (2016).
[18] F. Xu, Phys. Rev. A **92**, 012333 (2015).
[19] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).
[20] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A **89**, 052333 (2014).
[21] Q. Wang and X. B. Wang, Sci. Rep. **4**, 04612 (2014).
[22] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[23] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, Nat. Photonics. **9**, 772 (2015).
[24] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).
[25] Y. Liu, T. Y. Chen, L. J. Wang, H. Liang, G. L. Shentu, and J. Wang *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
[26] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporao, J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).
[27] Z. Y. Tang, Z. F. Liao, F. H. Xu, B. Qi, L. Qian, and H. K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).
[28] Y. L. Tang, H. L. Yin, S. J. Chen, Y. Liu, W. J. Zhang, and X. Jiang *et al.*, Phys. Rev. Lett. **113**, 190501 (2014).
[29] C. Wang, X. T. Song, Z. Q. Yin, S. Wang, W. Chen, C. M. Zhang, G. C. Guo, and Z. F. Han, Phys. Rev. Lett. **115**, 160502 (2015).
[30] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Nat. Photonics **10**, 312 (2016).

[31] P. González, L. Rebón, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira, Phys. Rev. A **92**, 022337 (2015).
[32] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **92**, 012319 (2015).
[33] Y. Choi, O. Kwon, M. Woo, K. Oh, S. W. Han, Y. S. Kim, and S. Moon, Phys. Rev. A **93**, 032319 (2016).
[34] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[35] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, New J. Phys. **11**, 095001 (2009).
[36] In the experiment, we only have two traditional amplitude modulators without the bias control circuits. Thus, we use the settings of Fig. 1(b) to serve as amplitude modulators. This kind of amplitude modulator features an outstanding stability which has been demonstrated in Ref. [35]. To be honest, this method would bring in an additional optical pulse at the input port of the PBS, which would cause the leakage of bit information. But it does not matter since we can eliminate this problem simply by replacing it with a traditional AM.
[37] In our demonstration, for simplicity, we take advantage of the simplest active phase-randomization method. The phase is not uniformly distributed in the range of $[0,2\pi]$. But it does not affect the feasibility of our demonstration since the effective phase-randomization technique has been demonstrated in several experiments.
[38] Drift in the fiber length is affected by the temperature change and the mechanical vibration. In the experiment, the mechanical vibration plays a less important role than the temperature change. Therefore, we only take the effect of temperature change into consideration.
[39] F. Xu, M. Curty, B. Qi, and H. K. Lo, New J. Phys. **15**, 113007 (2013).
[40] S. H. Sun, H. Q. Ma, J. J. Han, L. M. Liang, and C. Z. Li, Opt. Lett. **35**, 1203 (2010).