Experimental asymmetric Plug-and-Play Measurement-device-independent quantum key distribution

Guang-Zhao Tang,[1] Shi-Hai Sun,[1] Fei-Hu 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*

Measurement-device-independent quantum key distribution (MDI-QKD) is immune to all loopholes on detection. Several experiments have been made recently, which require the complicated stabilization systems. Here, we make a proof-of-principle demonstration of self-stabilized asymmetric plug-and-play MDI-QKD [1]. The whole system is automatically stabilized in spectral, in polarization, in arrival time, and in phase reference. The signal laser and 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.

In MDI-QKD protocol, the signals of clients are sent to an untrusted common server for the Bell-state measurement (BSM). Since most of the identified security loopholes are sited on the detection part, MDI-QKD is of great importance to promote the security of practical QKD systems. Achievements of MDI-QKD have been made both in theory [2–4] and in experiment [5–10]. The experimental demonstration of MDI-QKD requires the indistinguishablity of photons from Alice and Bob, mainly in three dimensions: spectral, polarization, and timing. To fulfil these requirements, the active stabilization systems (the temperature control units, the feedback temporal control system, and the phase (polarization) stabilization system) are commonly applied in experiments. Obviously, it is difficult to realize a quantum network with these complex active stabilization systems. Fortunately, the proposal of plug-and-play MDI-QKD [11, 12] greatly reduce the complexity of mode match and reference frame alignment. However, the experimental demonstration of plug-and-play MDI-QKD is still missing.

Here, we report a proof-of-principle demonstration of asymmetric plug-and-play MDI-QKD over 36km optical fiber [1]. The optical pulses of Alice and Bob come from a homemade signal laser which is in the charge of Charlie. There is no mismatch both in pulse waveform and in optical spectral at all. Due to the architecture of plug-and-play system, the polarization state is automatically calibrated and stabilized. Furthermore, the phase stabilization system is eliminated, since the time bins of Alice and Bob are generated by the same Mach-Zehnder interferometer (MZI). A passive timing calibration method is developed to ensure the precise and stable interference of signal pulses from Alice and Bob.

The experimental setup of plug-and-play MDI-QKD is illustrated in Fig 1(a) [1]. The signal laser source (1550nm) and detectors are both in the charge of a common server (Charlie). The signal laser is internally modulated into a pulse train with a width of 2ns and 1MHz repetition rate. An asymmetric Mach-Zehnder interferometer (AMZI) is utilized to separate the pulses into two time bins with 20ns time delay. The clients (Alice and Bob) only have the modulation devices. Two phase modulators (PMs) and two amplitude modulators (AMs) are used by each client. For the X basis, the key bit is encoded into the relative phase, 0 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, and AM2 is used to modulate the decoy states. We use the setting of Fig 1(b) to serve as an amplitude modulator (AM1) [14].

In our system, the clients, Alice and Bob, share one signal laser. Thus, there is naturally no mismatch in spectral and in pulse waveform at all. But, the active phase randomization is required to eliminate the partial-phase-randomization attack. In our proof-of-principle demonstration, a sawtooth wave with a repetition rate of 55KHz (15KHz) is applied to PM2 of Alice (Bob), to make the global phase of each optical pulse randomize in the range of [0,2π]. The time bins of clients come from the same AMZI. Thus, Alice and Bob share the same phase reference frame. For the polarization mode, the plug-and-play architecture can automatically compensate for the birefringence effects.

For the temporal mode, two synchronization lasers (SynL,1310nm) are used to calibrate the arrival time of signal pulses. The whole system is synchronized in the following manner: the SynL pulses are sent from Charlie to Alice (Bob). With the help of a Faraday mirror (1310nm), they travel back to Charlie, and are detected by a photoelectric detector (PD). The output of PD is used to drive the signal laser (1550nm) to generate the signal pulses of Bob (Alice). The temporal mode difference between Alice and Bob can be expressed as:

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

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

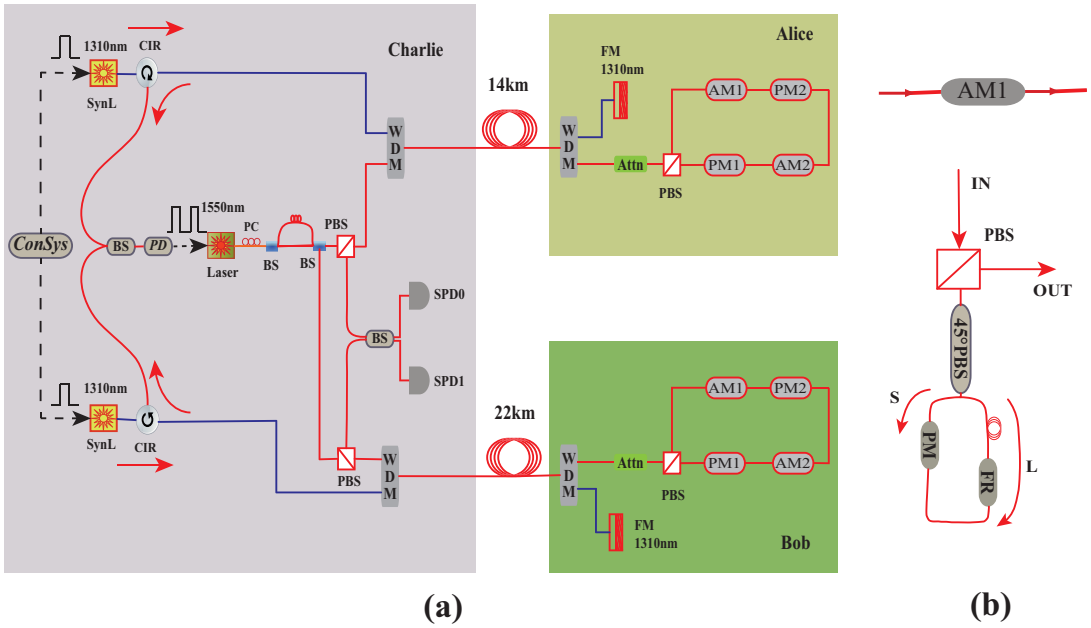

FIG. 1. (a) Experimental setup of the plug-and-play MDI-QKD. ConSys, control system; SynL, synchronization laser; CIR, circulator; BS, beam splitter; PC, polarization controller; WDM, wavelength division multiplexer; Attn, attenuator; FM, Faraday mirror; SPD, single-photon detector. (b) Schematic of the amplitude modulator (AM1): PBS, polarizing beam splitter; 45^0 PBS, polarizing beam splitter with 45^0 from the optical axis; PM, phase modulator; FR, Faraday rotator.

length between Charlie and Bob. $\Delta L = \alpha_T L^0 \Delta T$, where $\alpha_T = 5.4 \times 10^{-7}/^\circ C$ is the thermal expansion coefficient of fiber, and ΔT represents the change of temperature. The second part of Eq. (1) is negligible. 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.

At the measurement site, the partial BSM is implemented with a polarization-maintaining beam splitter (BS) and two commercial InGaAs SPDs (id201) with an efficiency of 10% and a gate width of 2.5ns. The dead time is 10μs with a dark count rate of 6×10^{-6} per gate. In our demonstration, the optical pulses are modulated into three different intensities according to the decoy state method [13], namely the signal state intensity ($\mu = 0.4$), the decoy state intensity ($\nu = 0.1$), and the vacuum state intensity ($\omega = 0.01$). The overall gains and quantum bit error rate (QBER) are listed in Table I and Table II.

We evaluate the secure key rate using an analytical method with two decoy states [13]. The secure key rate is given by [2]

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

where q, $Q^Z_{\mu\mu}$, and $E^Z_{\mu\mu}$ are the possibility, overall gain, and error rate 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. f is the error correction efficiency. $H(e) = -elog_2e-(1-e)log_2(1-e)$ is the binary Shannon entropy function. A total number of $N = 6.14\times 10^{10}$ pulses are sent out in the experiment. We take the value $q = \frac{1}{18}$ and $f = 1.16$ in our calculation. Thus, we

TABLE I. Experimental values of QBERs. I_A and I_B are the optical intensities of Alice and Bob. Errors shown represent standard deviation.

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

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

	Z-basis			X-basis		
	I_A					
I_B	μ	ν	ω	μ	ν	ω
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

get a lower bound of the yield $Y_{11}^{Z,L} = 2.2 \times 10^{-3}$, and an upper bound of the error rate $e_{\mu\mu,11}^{X,U} = 5.07\%$. We can estimate a secure rate of 4.7×10^{-6} bits per detection gate.

In conclusion, we have made a proof-of-principle demonstration of self-stabilized asymmetric plug-and-play MDI-QKD [1]. The homemade laser sources and expensive detectors are provided by a common server. The spectral and polarization state of signals are automatically indistinguishable. The passive time calibration technique ensures a precise and stable interference of photons from two remote parties. The phase reference frame is naturally aligned. The techniques used in our demonstration greatly promote the practicability of MDI-QKD and pave the way for a MDI quantum network.

[1] G. Z. Tang, S. H. Sun, F. Xu, H. Chen, C. Y. Li, and L. M. Liang, *Phys. Rev. A* **94**, 032326 (2016).
[2] H. K. Lo, M. Curty, B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012).
[3] F. Xu, H. Xu, H. K. Lo, *Phys. Rev. A* **89**, 052333 (2014).
[4] Q. Wang, X. B. Wang, *Sci. Rep.* **4**, 4612 (2014).
[5] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel, *Phys. Rev. Lett.* **111**, 130501 (2013).
[6] Y. Liu, T. Y. Chen, L. J. Wang, H. Liang, G. L. Shentu, J. Wang, *et al. Phys. Rev. Lett.* **111**, 130502 (2013).
[7] Z. Y. Tang, Z. F. Liao, F. H. Xu, B. Qi, L. Qian, and H. K. Lo, *Phys. Rev. Lett.* **112**, 190503 (2014).
[8] Y. L. Tang, H. L. Hua, S. J. Chen, Y. Liu, W. J. Zhang, X. Jiang, *et al. Phys. Rev. Lett.* **113**, 190501 (2014).
[9] 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).
[10] C. Wang, X. T. Song, Z. Q. Yin, S. Wang, W. Chen, C. M. Zhang, G. C. Guo, Z. F. Han, *Phys. Rev. Lett.*, **115**, 160502 (2015).
[11] F. Xu, *Phys. Rev. A*, **92**, 012333 (2015).
[12] Y. Choi, O. Kwon, M. Woo, K. Oh, S. W. Han, Y. S. Kim, S. Moon, *Phys. Rev. A*, **93**, 032319 (2016).
[13] F. Xu, M. Curty, B. Qi, H. K. Lo. *New J. Phys.*, **15**, 113007 (2013).
[14] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, W. Tittel, *New J. Phys.*, **11**, 095001 (2009).