Experimental Feasibility Test of Measurement-Device-Independent Quantum Key Distribution on Free-Space Channel

Hai-Lin Yong,[1,*] Chang Liu,[1] Dong-Dong Li,[1] Wen-Jie Zou,[2] Ji-Gang Ren,[1] Cheng-Zhi Peng,[1,†] and Jian-Wei Pan[1]

[1]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Shanghai 201315, China*

[2]*Department of Physics, Tsinghua University, Beijing 100084, China*

(Dated: July 19, 2013)

PACS numbers:

Quantum key distribution (QKD) [1] provides an approach to grow unconditional secure keys between two remote parties. In the past decade, various field-test QKD networks [2–5] with commercial terminals have been built worldwide. While the secure distance of conventional QKD systems based on fiber channel is limited due to photon loss, recent developments of free-space quantum communication [6–9] confirm the feasibility of satellite based global QKD network.

Nevertheless, the security of practical QKD systems is compromised because of detection loopholes [10, 11], until the concept of measurement-device-independent (MDI)-QKD [12, 13] is proposed. A crucial point of MDI-QKD is to replace the detection at the receiver side by a Bell state measurement (BSM) at a third untrusted party. To put MDI-QKD into practice [14–16], one has to implement BSM over a long distance, which is of great challenge.

Lying at the heart of BSM is the two-photon interference, which stems from the bosonic nature of photon and occurs when two photons are indistinguishable. To observe two-photon interference, one should keep the indistinguishability of the photon pair, that is, in the same frequency, temporal, spacial, and polarization mode [17]. These requirements become strict when the two photons travel a long distance. Great efforts have been devoted to realize the long-distance Bell state measurement (BSM). In 2005, a notable experiment with two 25-km-long fibers in the laboratory has been implemented [18], confirming the possibility of long distance BSM. However, the fiber based interference suffers from thermally induced fiber length fluctuations and is hard to be implemented out of laboratory. We note that a field test of fiber-optics implementation [19] has been done recently.

Here we report a realization of HOM interferometry with one arm being a free-space path, which can be regarded as a feasibility test of the free-space channel of MDI-QKD. In the past few years, great developments have been made in the free-space quantum communication for its capacity to realize satellite-ground global quantum communication, and the communication distance has been extended to a scale of 100 km [7, 8].

We note that, in the previous free-space quantum communication experiment [20, 21], quantum operation is performed at the transmitter, and then the photon is transmitted to the receiver. The main challenge there is to get a high collecting efficiency. Nevertheless, in our experiment the photon is firstly transmitted and the quantum operation (i.e. BSM or HOM interference) is performed at the receiver. This requires not only a high coupling efficiency, but also to keep the indistinguishability of the photon pair during the transmitting and receiving process.

The experimental setup of the free-space HOM interferometry is shown in Fig. 1. The photon pair source consists of a wavelength-stabilized single-longitudinal-mode pumping laser at 405 nm and a PPKTP crystal which is temperature stabilized at its degenerate working point. The temperature stabilization ensures that the photon pair generated in parametric down conversion (PDC) process is indistinguishable in frequency. The spectrum of photon pairs centers at 810 nm with the full-width at half-maximum (FWHM) of 1.2 nm.

The photon traveling in the fiber channel is coupled into a single mode fiber (SMF) cable of 170 m for time delay with a 0.5 dB total loss. In the free space channel, the other photon from the same pair is coupled in to a single mode fiber and transmitted in to the free space by the transmitting system and then collected in to a single mode fiber by the receiver system. In the transmitting system, the aperture of the telescope is 80 mm, and after adequate collimation and expansion process the photon beam is about 60 mm wide with about 23 μrad divergence angle. In the receiver system the aperture of the telescope is 127 mm and after the inverse processes in the transmitting system the photon is collected into a single mode fiber.

Because the wavefront of transmitted beam is disturbed by turbulence of the atmosphere, the direction of the photon beam fluctuates relative to the receiver system. Moreover, the transmitting and receiving system are also vibrating due to mechanical stress from the environment. As the diameter of the SMF is nearly 5 μm, any deviation would severely reduce the coupling efficiency. This requires that the receiver system matches the transmitting system with high precision to acquire a high coupling efficiency.

For this purpose we applied a 100-Hz frequency ac-

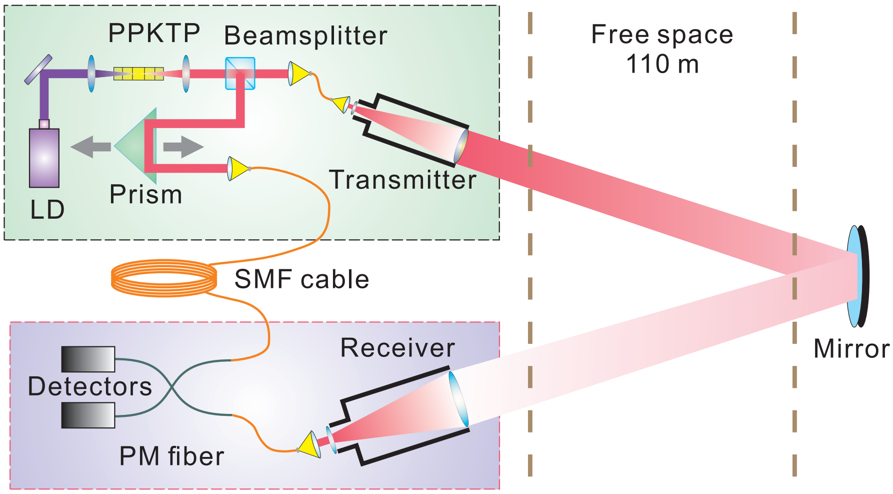

FIG. 1: (Color Online) Experimental setup. Signal photons and idle photons are generated through PDC process. After flying for 110 m free space to reach the flat mirror, one of each twin-photon pair is reflected back and coupled into the fiber of the receiver. At the same time, another photon is delayed in a SMF cable with same optical path length. Using a motorized linear translation stage, difference of optical length of the two channel is fine adjusted on the fiber link at the transmitter. The coincidence number varies to HOM dip while optical length difference vanishes.

quiring, pointing and tracking (APT) technique with 2 μrad accuracy. Two beacon lasers (650 nm and 532 nm) from the transmitting and receiving system respectively were utilized to track each other. The tracking technique guarantees the co-axis condition of the transmitter and receiver system, suppresses fluctuation from the environment and brings a high coupling efficiency.

A right-angle prism on a long-travel motorized linear translation stage is used to compensate the optic path length in the fiber channel, so that the twin-photon pairs from the fiber channel and the free space channel arrive at the beam splitter at the same time and are indistinguishable in temporal characteristics. The translation stage with a minimum step length of 2 μm is controlled by softwares on the computer. In the data acquisition process, the optic path length in the fiber channel is scanned by moving the translation stage. To improve the efficiency of the scan process, we utilize the current location of the dip to predict the next location of the dip and scan finely near the dip and coarsely far away from the dip. It takes 2 min to complete a scan process.

We have repeated the scanning process 25 times during 100 minutes. The averaged result is shown in Fig. 2. A clear dip after Gaussian fitting is observed with a visibility of 71% and a FWHM of 141.7 μm .

In Fig. 3, we show the time variation of the center of the dip. On the short-time scale, the position of the center fluctuates within 40 μm, which is mainly due to the tilt of fast steering mirror (FSM) during the tracking process, high-frequency disturbance of turbulence in the atmosphere and mechanical vibration from environment. On the long-time scale, the center of the dip drifts for about 70 μm with a deterministic direction. This is main-

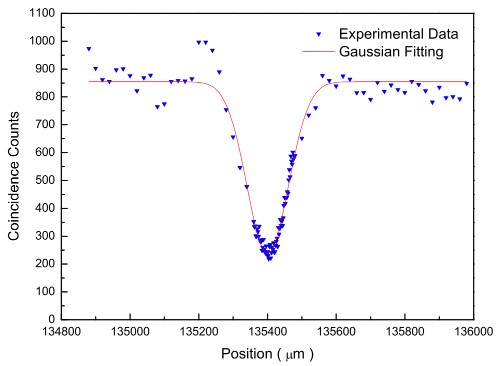

FIG. 2: (Color Online) HOM dip of coincidence counts. The triangle points represent the experiment data accumulated over 100 min by scanning the optic path length with a motorized translation stage repeatedly. The red solid line represents gaussian fitting of the experimental data.

ly due to thermally induced optic path length fluctuation in free space and fiber cable channel. We note that in the future applications the drift can be compensated in real time with a low-frequency closed-loop control system.

We show the visibility during the experiment in Fig. 4. The visibility is stable, which indicates that the indistinguishability of the photon pairs is maintained stably in the whole channel. The stability of the two-photon interference is essential for its future application in the long-distance quantum communication, especially for the MDI-QKD.

In conclusion, we have experimentally observed two-

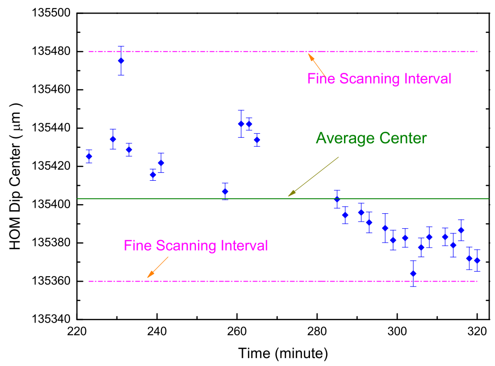

FIG. 3: (Color Online) The center of the dip over 100 min. The green solid line at 135403 μm represents the average of the center. The pink dash-dotted line represents the fine scanning interval in the experiment.

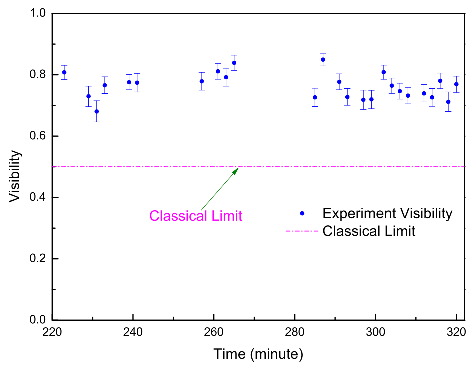

FIG. 4: (Color Online) The visibility of HOM dip during the experiment. The blue dotted line represents the experimental data. The pink dash-dotted line represents the classical limit.

photon interference with one arm being a 220 m free-space channel. Our results confirm the feasibility of constructing a MDI-QKD system on free-space links. We monitored the interferometry for 100 minutes. The indistinguishability of photon pairs is maintained in the whole channel and the visibility of the two-photon interference is 71%. Our experiment represents a feasibility test of the long-distance free-space HOM interferometry and marks the first step to realize Bell state measurement based quantum communication protocols in free space over a long distance.

* Electronic address: `hlyong@mail.ustc.edu.cn`

† Electronic address: `pcz@ustc.edu.cn`

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.
[2] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, et al., New Journal of Physics **11**, 075001 (????).
[3] T. Chen, H. Liang, Y. Liu, W. Cai, L. Ju, W. Liu, J. Wang, H. Yin, K. Chen, Z. Chen, et al., Optics Express **17**, 6540 (2009).
[4] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, et al., Opt. Exp. **19**, 10387 (2011).
[5] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, et al., New Journal of Physics **13**, 3001 (2011).
[6] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, et al., Phys. Rev. Lett. **94**, 150501 (2005).
[7] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, et al., Phys. Rev. Lett. **98**, 010504 (2007).
[8] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, et al., Nature Photonics **7**, 387 (2013).
[9] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Nature Photonics **7**, 382 (2013).
[10] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 073 (2007).
[11] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Communications **2**, 349 (2011).
[12] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[13] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[14] A. Rubenok, J. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Arxiv preprint arXiv:1204.0738 (2012).
[15] T. da Silva, D. Vitoreti, G. Xavier, G. Temporão, and J. von der Weid, Arxiv preprint arXiv:1207.6345 (2012).
[16] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, et al., Arxiv preprint arXiv:1209.6178 (2012).
[17] L. Mandel, Rev. Mod. Phys. **71**, S274 (1999).
[18] M. Halder, S. Tanzilli, H. de Riedmatten, A. Beveratos, H. Zbinden, and N. Gisin, Phys. Rev. A **71**, 042335 (2005).
[19] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, ArXiv e-prints (2013), 1304.2463.
[20] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, et al., Nature **488**, 185 (2012), ISSN 0028-0836.
[21] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, et al., Nature **489**, 269 (2012).