Measurement-Device-Independent Quantum Key Distribution of Frequency-Nondegenerate Photons

Rong Xue[1], Xu Liu[1], Yidong Huang[1,2], and Wei Zhang[1,2,*]
[1]*Frontier Science Center for Quantum Information, Beijing National Research Center for Information Science and Technology (BNRist), Department of Electronic Engineering, Tsinghua University, Beijing 100084, China*
[2]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
**zwei@tsinghua.edu.cn*

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) of frequency-nondegenerate photons was proposed and demonstrated based on a frequency-domain beam splitter, which simplified the implementation of MDI-QKD and provided network functions on the relay node.

1. Introduction

Measurement-device-independent quantum key distribution (MDI-QKD) [1] guarantees unconditional security in practical systems by entrusting detection to an untrusted relay. However, due to the limitation of the Bell state measurement (BSM) based on linear optics, the photons sent by different users should be frequency-degenerate, which increases the complexity to realize MDI-QKD and limits the development of MDI-QKD networks based on wavelength division multiplexing (WDM). By applying the frequency-domain beam splitter (FBS) [2] to BSM, we proposed the scheme of the MDI-QKD network of frequency-nondegenerate photons and demonstrated the MDI-QKD of frequency-nondegenerate photons. The users' frequency difference can be monitored and actively matched at the relay node, thus an additional feedback system for the laser wavelength calibration is not required.

2. The Scheme

The scheme of the MDI-QKD network of frequency-nondegenerate photons is illustrated in Fig. 1 (a). The users send photons of different frequencies coupled together through a WDM device, and the relay node executes the BSM of frequency-nondegenerate photons, which is realized by a 50:50 FBS based on a phase modulator (PM) [2]. The input and output ports of the FBS are two specific frequency channels. The BSM of frequency-nondegenerate photons between two users is realized when the modulation frequency of the PM matches the frequency difference of the users. Then the photons at two frequency channels are separated by optical filters and detected by single-photon detectors, respectively.

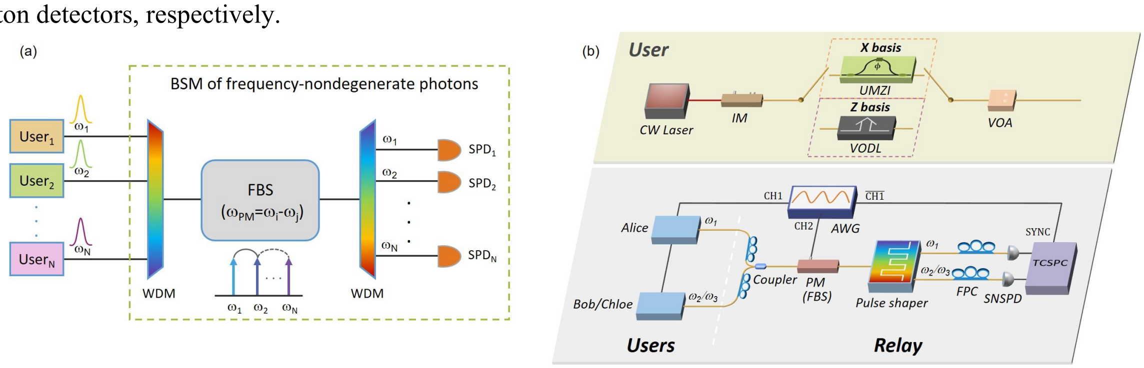

Fig. 1 (a). The scheme of the MDI-QKD network of frequency-nondegenerate photons. (b). Experimental setup for the MDI-QKD of frequency-nondegenerate photons. FPC, fiber polarization controller; AWG, arbitrary waveform generator; SNSPD, superconducting nanowire single-photon detector; TCSPC, time-correlated single-photon counting module.

3. The Experiment

As shown in Fig. 1 (b), the continuous wave (CW) laser followed by an intensity modulator (IM) is used to generate light pulses with a repetition frequency of 40 MHz and a full width at half maximum of 100 ps. The time-bin phase-encoding [3] is emulated in the Z basis and X basis by a variable optical delay line (VODL) and an unbalanced Mach-Zehnder interferometer (UMZI), respectively. The decoy-state method [4] is realized by adjusting the attenuation of the variable optical attenuator (VOA). The average photon number of the pulses is set to 0.4, 0.04, and 0 to generate the signal state, decoy state, and vacuum state, respectively. The relay node performs BSM of frequency-nondegenerate photons between two users whose frequency difference matches the f_m. We record the coincidence events projected on $|\Psi^{-}\rangle$, when two detectors click in different time-bins. We took the experiments of the MDI-QKD of frequency-nondegenerate photons in two cases, showing the user selection function of the relay node. In the first case, the frequencies of the two lasers are set to 193.11 THz and 193.09 THz, respectively, corresponding to user Alice and Bob, and the f_m is set to 20 GHz. In the second case, the frequencies of the two lasers are set to 193.11 THz and 193.135 THz, respectively, corresponding to user Alice and Chloe, and the f_m is set to 25 GHz. Secure key rates of 7.66×10^{-7} bit/s/pulse and 5.13×10^{-7} bit/s/pulse are generated in the two cases, respectively.

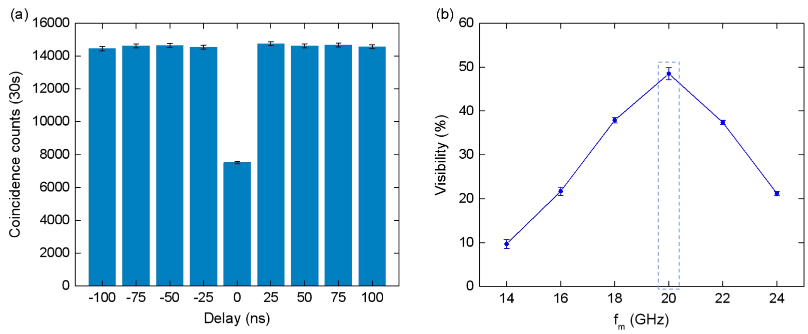

Fig. 2. The results of HOM interference of frequency-nondegenerate photons. (a) A typical coincidence result under f_m = 20 GHz, which matches the frequency difference of the two users. (b) The visibilities under different f_m.

Then we demonstrated the feasibility of the calibration function when the frequency difference of the lasers in the two users is fixed at 20 GHz yet the f_m is changed. The states of the photons in the two users are set at the same time-bin. The Hong-Ou-Mandel (HOM) interference [5] of frequency-nondegenerate photons are measured under different f_m. Fig. 2 (a) shows a typical result when f_m = 20 GHz, showing the effect of HOM interference of frequency-nondegenerate photons. The visibility when the f_m matches the frequency difference of the two users is 48.5 ± 1.4% in Fig. 2 (a). The visibilities under different f_m are shown in Fig. 2 (b). It can be seen that the visibility can be used as an indicator of wavelength difference drifting, and the f_m can be controlled to match the frequency difference of the two users dynamically according to the visibility. All the measurement and the control of the f_m are realized at the relay node, therefore this MDI-QKD scheme does not need additional feedback systems for laser wavelength calibration.

4. Conclusion

We demonstrated the MDI-QKD of frequency-nondegenerate photons based on an FBS. The results showed that the BSM of frequency-nondegenerate photons could select specific users to realize MDI-QKD by adjusting the modulation frequency of the PM to match the frequency difference of the users. It could be used as frequency-domain switching and routing functions in WDM networks. The visibility of HOM interference of frequency-nondegenerate photons can be used as an indicator to solve the laser wavelength drifting problem. Since it is easy to expand point-to-point MDI-QKD to a star-topology network, our scheme can be expanded to MDI-QKD networks combined with WDM and has great potential to be applied to other quantum network applications.

5. Acknowledgments

We acknowledge the support of National Key R&D Program of China (2017YFA0303704), Beijing Natural Science Foundation (BNSF) (Z180012), National Natural Science Foundation of China (NSFC) (61875101, 91750206), and the Tsinghua University Initiative Scientific Research Program.

6. References

[1] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **108**(13), 130503 (2012).
[2] P. Imany, O. D. Odele, M. S. Alshaykh, H.-H. Lu, D. E. Leaird, and A. M. Weiner, "Frequency-domain Hong–Ou–Mandel interference with linear optics," Opt. Lett. **43**(12), 2760 (2018).
[3] 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, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental Measurement-Device-Independent Quantum Key Distribution," Phys. Rev. Lett. **111**(13), 130502 (2013).
[4] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
[5] C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," Phys. Rev. Lett. **59**(18), 2044–2046 (1987).