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

Rong Xue,[1] Xu Liu,[1] Hao Li,[2] Lixing You,[2] Yidong Huang,[1,3,4] and Wei Zhang[1,3,4,*]

[1] *Beijing National Research Center for Information Science and Technology (BNRist), Beijing Innovation Center for Future Chips, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China*

[2] *State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

[3] *Frontier Science Center for Quantum Information, Beijing 100084, China*

[4] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*

(Received 1 September 2021; revised 24 November 2021; accepted 7 January 2022; published 16 February 2022)

In measurement-device-independent quantum key distribution (MDI QKD), the setup of Bell state measurement (BSM) usually requires that the photons sent by different users should be frequency degenerate. It increases the complexity to implement MDI QKD since a complicated feedback system is usually required to calibrate photons' frequencies in different users. It also limits the development of MDI QKD networks since wavelength division multiplexing (WDM) technology is not compatible with this requirement. In this work, we propose a MDI QKD scheme of frequency-nondegenerate photons, in which the users send photons with different frequencies. It is based on a BSM setup with a frequency-domain beam splitter (FBS), which is realized by a phase modulator (PM). A proof-of-principle experiment is realized, showing 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 photons sent by the users. The results manifest that our scheme has great potential for simplifying the implementation and realizing MDI QKD networks combined with WDM.

DOI: 10.1103/PhysRevApplied.17.024045

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] generates secure keys between users based on the laws of quantum mechanics, which will play a role in future information security [4]. Since the BB84 protocol [5] was proposed, QKD has developed rapidly, especially in experimental implementation [3,6–8]. However, its security should be considered more carefully in practical systems with nonideal devices. As an example, it has been shown that single-photon detectors are vulnerable to eavesdroppers [4]. A measurement-device-independent quantum key distribution (MDI QKD) protocol [9] was proposed to overcome the problem introduced by nonideal detectors. Laboratory proof-of-principle experiments [10–12] and field tests [13–15] via optical fibers or free space have been achieved in recent years. Recently, MDI QKD has also developed towards integrated chips [16,17]. So far, the transmission distance of MDI QKD has been achieved over 404 km with ultralow-loss optical fiber [18], indicating that MDI QKD is suitable for long-distance applications. Additionally, it is easy to achieve a multiple-user MDI QKD in a star-topology network when all the users connect to the same measurement relay [14]. Thus, MDI QKD has attracted much attention as a promising way to realize QKD in practical systems in terms of security, practicability, and scalability.

However, the previous implementations of MDI QKD have some strict requirements on the photons sent by users. The basis of MDI QKD is the Bell state measurement (BSM) [19–22] at the relay node. Usually, the BSM setup is based on linear optics. The quantum-interference process in the BSM setup requires that photons sent by different users should be frequency degenerate. In previous MDI QKD experiments, an additional feedback control system is needed to calibrate and lock the laser wavelengths of different users [14,23,24], otherwise, the interference visibility will decrease as the wavelengths drift. The feedback system is quite complicated since different users are at different locations and additional optical paths and/or classical communication are required to send the laser lights and the feedback signals between users. It is notable that the laser wavelength calibration issue can be bypassed by some methods, such as the laser with its frequency locked to a molecular absorption line [11,25] or plug-and-play

[*] zwei@tsinghua.edu.cn

architecture [26,27]. Nevertheless, a simple way to realize wavelength calibration between independent sources is still vital and valuable in MDI QKD implementation. Moreover, as the number of users increases, the realization of the MDI QKD network is very crucial. The requirement of frequency-degenerate photons limits the development of the MDI QKD network based on wavelength division multiplexing (WDM).

Frequency is an intrinsic high-dimensional degree of freedom (DOF) of photons [28]. In recent years, the frequency transformation of single photons has developed rapidly, based on nonlinear optical processes [29] or electro-optic phase modulation [30,31], providing possible ways to realize quantum interference between photons of different frequencies. In this work, we propose that MDI QKD of frequency-nondegenerate photons could be realized through frequency transformation. We realize a frequency-domain beam splitter (FBS) based on one-stage phase modulation [30]. It could be used to realize the Hong-Ou-Mandel (HOM) interference [32] of frequency-nondegenerate photons, which is the basis of the BSM of frequency-nondegenerate photons. Then we demonstrate that it could support MDI QKD of frequency-nondegenerate photons by a proof-of-principle experiment. The results show that the BSM setup based on the FBS could select specific users to realize MDI QKD by adjusting the modulation frequency of the phase modulator (PM). It could be used as switching and routing functions in WDM networks. In addition, the visibility of HOM interference of frequency-nondegenerate photons can be used as an indicator of the wavelength difference drifting. According to the indicator, the modulation frequency of the PM could be controlled to match the wavelength difference dynamically. Since both the measurement of HOM interference and the control of the PM are placed at the relay node, the additional optical paths and/or classical communication for the laser wavelength calibration are not required. Hence, the implementation of MDI QKD could be highly simplified in this scheme.

II. SCHEME DESCRIPTION

A. BSM of frequency-nondegenerate photons based on a FBS

BSM is a useful operation in many photonic quantum-communication applications [33]. It is used to distinguish different Bell states, which are a set of maximum entangled two-photon quantum states with the form of

$$
\begin{aligned}
|\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\,|1\rangle \pm |1\rangle\,|0\rangle),\\
|\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle \pm |1\rangle\,|1\rangle),
\end{aligned}
\tag{1}
$$

where “0” and “1” denote two orthogonal polarization directions or two different time bins, respectively, if the information is encoded on photons’ polarization or arrival time. The BSM setup based on linear optics can distinguish two of the four Bell states at most [21]. In some applications, such as MDI QKD, a simplified BSM based on a 50:50 beam splitter (BS) is used, which can distinguish $|\Psi^-\rangle$ from the other three [20,22]. The basis of the BSM process is the two-photon interference at the 50:50 BS, which requires that the two photons should be indistinguishable, especially, they should be frequency degenerate. However, it has been demonstrated that the indistinguishability of probability amplitudes is crucial for the two-photon interference, not the indistinguishability of photons [34,35]. This leads to achieving the two-photon interference and the BSM in different ways. In this work, the BSM between frequency-nondegenerate photons is realized based on a FBS.

Different from a 50:50 BS, the input and output ports of a 50:50 FBS are two specific frequency channels, instead of spatial paths. The relation between the inputs and the outputs of a 50:50 FBS is the same as that of a 50:50 BS. If the frequencies of the two input photons match the FBS, the two-photon interference will occur between the two frequency channels. When the input photons are encoded in the DOF except frequency, such as time bin, the BSM of frequency-nondegenerate photons can be realized. The two photons would output from the FBS at the two frequency channels, respectively. Hence, $|\Psi^-\rangle$ could be distinguished by the coincidence events when the photons at the two frequency channels are separated by optical filters and detected by single-photon detectors, respectively. In this way, a simplified BSM of frequency-nondegenerate photons is realized.

In this work, the 50:50 FBS is realized by a broadband PM driven by a sinusoidal microwave signal with a modulation frequency of f_m [30]. It scatters photons from a specific frequency into many different frequency components. The interval between any adjacent frequency components is f_m. By setting a suitable modulation depth of the PM, a 50:50 FBS can be realized, whose input and output ports are both two specific frequency channels with an interval of f_m. The 50:50 FBS would introduce a loss of 2.2 dB since part of the photons would be scattered to frequency components outside the output frequency channels. It is noteworthy that a theoretically almost lossless FBS could be realized by a more complex scheme with two PMs and a pulse shaper [31], however, its setup is complicated with higher loss introduced by the devices. Thus, we select the FBS scheme with only one PM for simplification.

B. MDI QKD of frequency-nondegenerate photons

We propose that the MDI QKD network of frequency-nondegenerate photons can be realized based on the BSM

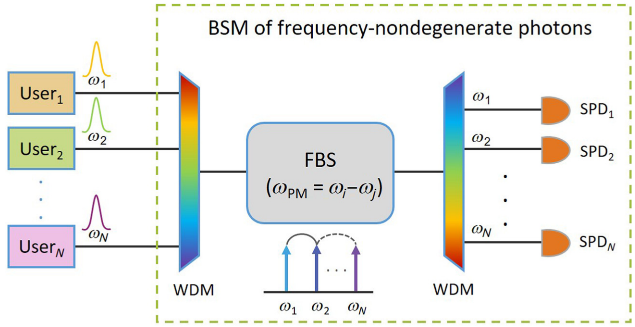

FIG. 1. Schematic of the MDI QKD network of frequency-nondegenerate photons. WDM, wavelength division multiplexing; FBS, frequency-domain beam splitter; PM, phase modulator; SPD, single-photon detector.

setup with a 50:50 FBS, as illustrated in Fig. 1. Each user sends light pulses with weak coherent states at different frequencies. They are coupled together through a WDM device and transmitted to the relay node. The relay node uses a 50:50 FBS to perform BSM of frequency-nondegenerate photons between two users whose frequency difference matches the modulation frequency of the PM. The output photons with different frequencies are demultiplexed to the corresponding single-photon detectors for the BSM. In this manner, the MDI QKD protocol could be implemented between two arbitrary users.

To realize the MDI QKD, photons sent by the users should be encoded. In this work, the time-bin phase encoding method [10,36] is utilized, in which the states of $|0\rangle$ and $|1\rangle$ denote early and late time bins, respectively. The users send their photons in two unbiased orthogonal bases randomly. In the Z basis, bits of 0 and 1 are encoded on the states of $|0\rangle$ and $|1\rangle$, respectively. In the X basis, bits of 0 and 1 are encoded on the states of $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, respectively. The relay node receives the photons from users and performs BSM of frequency-nondegenerate photons. The relay node records the coincidence events projected on $|\Psi^-\rangle$ and announces them to the public. Then the users keep the bits corresponding to successful events, also in the same basis through key sifting. One of the two users should perform bit flip so that the two users could generate identical keys. According to the decoy-state method [37] and finite-key effect with statistical fluctuations [38], the key-rate formula is given by

$$R \geq Q_{11}^{Z}[1 - H(e_{11}^{X})] - Q_{\mu\nu}^{Z} f H(E_{\mu\nu}^{Z}), \tag{2}$$

where the second term contains the total gain in the Z basis ($Q_{\mu\nu}^{Z}$) and the total quantum bit error rate (QBER) in the Z basis ($E_{\mu\nu}^{Z}$), which could be measured directly in the experiment. The first term contains the gain when the two users send single photons in the Z basis (Q_{11}^{Z}) and the QBER when the two users send single photons in the X basis (e_{11}^{X}), which would be estimated according to the experimental results. $H(x)$ is the binary Shannon-entropy function and f is the error-correction efficiency. μ and ν are average photon numbers of the single-photon wave packets emitted by the two users.

Compared with the previous implementations of MDI QKD, the proposed scheme of frequency-nondegenerate photons has two advantages. First, according to the quantum-interference performance in the BSM setup, this scheme can actively match the modulation frequency of the PM and the frequency difference of the senders' photons at the relay node. It avoids the complicated feedback control system for the laser calibration between the two users, which are usually at two different places with a long distance. Second, the relay node could connect more than two users who send photons at different frequencies and select two of them to realize MDI QKD by controlling the modulation frequency of the PM. It provides a way to build a MDI QKD network based on WDM.

III. EXPERIMENTAL SETUP

We take a proof-of-principle experiment to show the feasibility of MDI QKD of frequency-nondegenerate photons. The setup is shown in Fig. 2.

All the users have the same setup, as shown in Fig. 2(a). The continuous wave (CW) laser (N7714A, Keysight Inc.) followed by an intensity modulator (IM) with a 40 dB extinction ratio is used to generate light pulses with a repetition frequency of 40 MHz and a FWHM of 100 ps. The IM is followed by a 90:10 BS and a power meter, which is not shown in Fig. 2(a), to monitor the output power of the IM. A variable optical delay line (VODL) and an

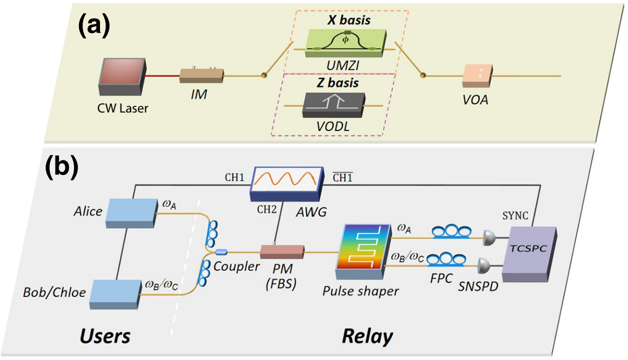

FIG. 2. Experimental setup for the MDI QKD of frequency-nondegenerate photons. (a) Setup of the users. (b) Setup of the experimental system. IM, intensity modulator; UMZI, unbalanced Mach-Zehnder interferometer; VODL, variable optical delay line; VOA, variable optical attenuator; FPC, fiber polarization controller; PM, phase modulator; FBS, frequency-domain beam splitter; AWG, arbitrary waveform generator; SNSPD, superconducting nanowire single-photon detector; TCSPC, time-correlated single-photon counting module.

unbalanced Mach-Zehnder interferometer (UMZI, mint-1x2-L-2.5 GHz, Kylia Inc.) with an arm length difference of 400 ps are used to emulate the time-bin phase encoding in the Z basis and X basis, respectively. By adjusting the VODL, light pulses are generated in the early or the late time bin with an interval of 400 ps. The states of $|0\rangle$ or $|1\rangle$ are generated after the light pulses are attenuated to the single-photon level by a variable optical attenuator (VOA). By tuning the voltage applied on the UMZI, the relative phase of its two arms is set to 0 or π. Hence, the states of $|+\rangle$ or $|-\rangle$ are generated after the light pulses are attenuated to the single-photon level by the VOA. To execute the decoy-state method, 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, by adjusting the attenuation of the VOA. The frequencies of the lasers in different users are different, therefore the photons received by the relay node are frequency nondegenerate from different users.

The setup of the experimental system is shown in Fig. 2(b). The photons with different frequencies sent by different users are combined by a coupler (a 50:50 fiber coupler, realizing the WDM function in a simple way). At the relay node, a PM (PM-5V5-40-PFA-PFA-UV, Eospace Inc.) is used as a 50:50 FBS. The output photons of the FBS are separated according to their frequencies by a multiport pulse shaper (Waveshaper 4000A, Finisar Inc.) and then detected by superconducting nanowire single-photon detectors (SNSPD, PHOTEC Inc.), respectively. The detection efficiency, the dark-count rate, and the average time jitter of the SNSPDs are approximately 50% at 1550 nm, approximately 100 cps, and approximately 80 ps, respectively. Then the detection events are recorded by a time-correlated single-photon counting module (TCSPC, HydraHarp 400, PicoQuant Inc.). We record the coincidence events projecting the states of photons onto $|\Psi^-\rangle$, when two detectors click in different time bins, specifically, one detector clicks in the early time bin and the other detector clicks in the late time bin or vice versa. In the setup, the modulation signals of the IMs at the users and the PM at the relay node, and the synchronized signal for the TCSPC are generated by an arbitrary waveform generator (AWG, M8195A, Keysight Inc.).

IV. EXPERIMENTAL RESULTS

To realize the MDI QKD of frequency-nondegenerate photons, the modulation frequency of the PM (f_m) at the relay node should match the frequency difference of the two users, which can be calibrated and locked according to the HOM interference of the photons sent by the two users. Before the experiment of MDI QKD, we demonstrate the feasibility of the calibration method firstly. In the experiment, the frequencies of the lasers in the two users are set at 193.09 and 193.11 THz, respectively, with a frequency difference of 20 GHz. In both users, the states of the photons are set at the same time bin ($|0\rangle$). The HOM interference of frequency-nondegenerate photons are measured under different f_m and the results are shown in Fig. 3. Figure 3(a) shows a typical result of coincidence measurement when $f_m = 20$ GHz. The horizontal axis (delay) is the relative time delay of the two users' photons arriving at the FBS. The time interval of coincidence peaks is 25 ns, corresponding to the period of the generated pulses. It can be seen that the coincidence peak at delay = 0 is much lower than other peaks, showing the effect of HOM interference. The visibility of HOM interference can be calculated by the coincidence peak at delay = 0 and the coincidence peaks at delay $\neq 0$ (the average counts are calculated from the eight peaks at delay $\neq 0$). The visibility in Fig. 3(a) is $48.5 \pm 1.4\%$, which is close to the theoretical upper limit of 50% for the Poisson distribution of photon numbers. The visibilities under different f_m are shown in Fig. 3(b). It can be seen that the visibility reaches the maximum under $f_m = 20$ GHz, which is the case that the f_m is equal to the frequency difference of the two users. The visibility decreases obviously when f_m changes. Hence, the visibility can be used as an indicator to show whether the f_m matches the frequency difference of the two users or not. In the implementations of MDI QKD, the wavelengths of lasers in the two users change slightly with time, consequently, their frequency difference always drifts. The measurement of HOM interference provides a way to monitor the difference between the f_m and the frequency difference of the two users. According to the visibility, the f_m could be controlled to match the frequency difference of the two users. 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 optical paths and/or classical communication for laser frequency calibration.

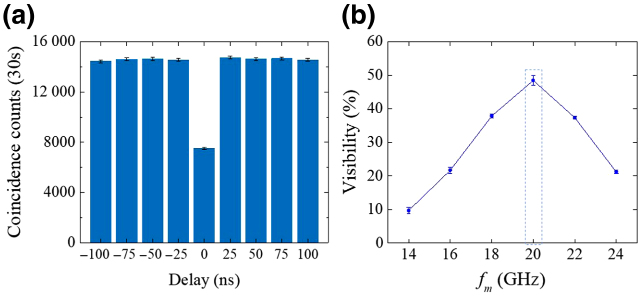

FIG. 3. The results of HOM interference of frequency-nondegenerate photons. (a) A typical coincidence result under $f_m = 20$ GHz, which matches the frequency difference of the two users, showing a visibility of $48.5 \pm 1.4\%$ without subtracting the accidental coincidence counts from the coincidence counts. (b) The measured visibilities under different f_m, showing that the visibility reduces when the f_m deviates from the frequency difference of the two lasers.

Then we take the experiment of the MDI QKD of frequency-nondegenerate photons. The frequencies of the lasers in the two users are 193.11 and 193.09 THz, respectively, corresponding to Alice and Bob. The f_m is set at 20 GHz, matching the frequency difference of the two users. Both users prepare photons with weak coherent states in the Z basis and X basis and send them to the relay node. The relay node performs BSM of frequency-nondegenerate photons and records the coincidence events projecting the states of photons onto $|\Psi^-\rangle$. The total gains and the total QBERs are obtained from these coincidence events. We calculate the total QBER from $E_{\mu\nu}^{X,Z} = N_{\text{error}}/(N_{\text{error}} + N_{\text{correct}})$, where $E_{\mu\nu}^{X,Z}$ is the error probability in the Z basis or X basis when the average photon numbers of the two users are μ and ν, N_{correct} (N_{error}) is the number of correct (error) coincidence events when the coincidence events correspond to the projection on $|\Psi^-\rangle$ and the encoded bits of the two users are different (identical). The results of the total gains and the total QBERs are listed in Table I. These performances support the MDI QKD implementation with a secure key rate of 7.66×10^{-7} bit/s/pulse, which is calculated according to Eq. (2). The result shows that the MDI QKD scheme of frequency-nondegenerate photons is feasible when the f_m matches the frequency difference of the two users.

As shown in Fig. 1, when multiple users of different photon frequencies connect to the relay node, two specific users could be selected to perform MDI QKD by controlling the f_m to match their frequency difference. To show the user selection function of the relay node, we change the laser frequency of one user and adjust the f_m to match the frequency difference of the two users, then measure the MDI QKD performance again. In the experiment, the laser frequencies of the two users are 193.11 and 193.135 THz, respectively, corresponding to Alice and Chloe. The f_m is set at 25 GHz. The measured total gains and the total QBERs are listed in Table II, generating a secure key rate of 5.13×10^{-7} bit/s/pulse. The user selection function has the potential for realizing frequency-domain switching and routing in a WDM MDI QKD network.

TABLE I. The total gains ($Q_{\mu_A\mu_B}^{X,Z}$) and the total QBERs ($E_{\mu_A\mu_B}^{X,Z}$) under different average photon numbers of Alice (μ_A) and Bob (μ_B) when the frequency difference of the two lasers and the f_m are both 20 GHz.

	μ_A/μ_B	0.4	0.04	0
$Q_{\mu_A\mu_B}^X$	0.4	4.31×10^{-6}	1.25×10^{-6}	9.48×10^{-7}
	0.04	1.23×10^{-6}	3.21×10^{-8}	8.65×10^{-9}
	0	9.40×10^{-7}	8.13×10^{-9}	0
$E_{\mu_A\mu_B}^X$	0.4	25.35%	41.22%	50.42%
	0.04	42.93%	24.03%	46.99%
	0	48.42%	57.69%	0
$Q_{\mu_A\mu_B}^Z$	0.4	1.17×10^{-6}	1.13×10^{-7}	2.07×10^{-8}
	0.04	1.13×10^{-7}	2.29×10^{-8}	4.17×10^{-10}
	0	9.79×10^{-9}	4.17×10^{-10}	0
$E_{\mu_A\mu_B}^Z$	0.4	0.56%	2.03%	50.63%
	0.04	2.77%	1.36%	50.00%
	0	68.09%	50.00%	0

TABLE II. The total gains ($Q_{\mu_A\mu_C}^{X,Z}$) and the total QBERs ($E_{\mu_A\mu_C}^{X,Z}$) under different average photon numbers of Alice (μ_A) and Chloe (μ_C) when the frequency difference of the two lasers and the f_m are both 25 GHz.

	μ_A/μ_C	0.4	0.04	0
$Q_{\mu_A\mu_C}^X$	0.4	3.99×10^{-6}	1.36×10^{-6}	1.13×10^{-6}
	0.04	1.18×10^{-6}	3.19×10^{-8}	6.56×10^{-9}
	0	9.10×10^{-7}	8.96×10^{-9}	0
$E_{\mu_A\mu_C}^X$	0.4	25.83%	43.21%	51.85%
	0.04	42.83%	25.10%	50.79%
	0	47.58%	52.33%	0
$Q_{\mu_A\mu_C}^Z$	0.4	2.15×10^{-6}	2.27×10^{-7}	1.44×10^{-8}
	0.04	2.14×10^{-7}	1.90×10^{-8}	4.17×10^{-10}
	0	8.75×10^{-9}	4.17×10^{-10}	0
$E_{\mu_A\mu_C}^Z$	0.4	1.10%	3.76%	53.62%
	0.04	3.41%	1.42%	50.00%
	0	73.81%	50.00%	0

V. DISCUSSION

The secure key rates generated in the experiment are in the magnitude of 10^{-7} bit/s/pulse. It is mainly due to the system losses in the setup. For the photons sent by a specific user, the total loss is about 16.5 dB, including the insertion losses of the optical devices [the FPC before the coupler (0.3 dB), the coupler (3 dB), the PM (3.5 dB), and the pulse shaper (4.5 dB)], the theoretical loss of the FBS (2.2 dB), and the collection loss by the limited detection efficiency of detectors (3 dB). According to some typical implementations of MDI QKD [23,24,39], the key rates are in the magnitude of 10^{-8}–10^{-6} bit/s/pulse when the single side loss is at the same level as that of ours. Hence, the performance of our experiment is comparable with them. Considering the practical applications of the MDI QKD scheme of frequency-nondegenerate photons, the system loss should be highly reduced to support long-distance transmission. It could be expected that the loss introduced by the coupler and the pulse shaper could be further reduced by replacing them with some low-loss WDM components, such as fiber Bragg gratings (FBGs) [40,41]. The efficiency of the detector could be improved according to the recent progress of SNSPD [42]. The insertion loss of the PM also has space to reduce, if the technology of PM could be improved [43].

The experiment shows that multiple users with different photon frequencies can connect to the same relay node and two specific users can be selected by controlling the modulation frequency of the PM. In this way, a WDM MDI QKD network with switching and routing functions is realized. The user number of such a network is limited by two parameters. The first one is the user's frequency channel bandwidth. It could be designed according to the optical filter technology of the relay node, which is used to combine and separate photons from different users. A bandwidth of 12.5 GHz (0.1 nm) could be expected through mature technologies, such as FBGs. The second one is the modulation bandwidth of the PM. Recently, PMs with bandwidths over 100 GHz are reported [44,45]. Therefore, this scheme has the potential to support a fully connected network with over nine users, which have different photon frequencies. The user number could be even larger if the network topology is not fully connected and some users could have the same photon frequency.

VI. CONCLUSION

In conclusion, we propose and experimentally demonstrate a MDI QKD scheme of frequency-nondegenerate photons, in which the photons sent by different users have different frequencies. Its feasibility is demonstrated by a proof-of-principle experiment, in which a PM is used as a FBS to realize the BSM of frequency-nondegenerate photons. The experimental results show that the BSM of frequency-nondegenerate photons could select specific users to realize MDI QKD, if the modulation frequency of the PM is adjusted to match the frequency difference of the two users. The visibility of HOM interference of frequency-nondegenerate photons can be used as an indicator of the modulation frequency adjustment. It provides a convenient way to handle the issue introduced by the laser wavelength drifting at the users. Moreover, the experiment also shows that frequency transformation can be applied to MDI QKD, improving the flexibility of its implementation. Switching and routing functions of WDM MDI QKD networks can be realized by the BSM based on a FBS at the relay node. For the outlook, the BSM of frequency-nondegenerate photons also has great potential for other quantum network scenarios, such as quantum teleportation [46] and quantum swapping [47].

ACKNOWLEDGMENTS

We acknowledge the support of National Key R&D Program of China (Contract No. 2017YFA0303704), Beijing Natural Science Foundation (BNSF) (Contract No. Z180012), National Natural Science Foundation of China (NSFC) (Contracts No. 61875101 and No. 91750206), Beijing Academy of Quantum Information Sciences (Contract No. Y18G26), and the Tsinghua University Initiative Scientific Research Program.

[1] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, Quantum cryptography, Contemp. Phys. **36**, 149 (1995).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[3] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[5] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[6] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, Npj Quantum Inf. **2**, 16025 (2016).

[7] S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, S.-F. Liu, Z. Zhou, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, Practical gigahertz quantum key distribution robust against channel disturbance, Opt. Lett. **43**, 2030 (2018).

[8] Z. Yuan, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, A. J. Shields, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, and J. F. Dynes, 10-Mb/s quantum key distribution, J. Lightwave Technol. **36**, 3427 (2018).

[9] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[10] 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**, 130502 (2013).

[11] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution robust against environmental disturbances, Optica **4**, 1016 (2017).

[12] D. Lee, S. Hong, Y.-W. Cho, H.-T. Lim, S.-W. Han, H. Jung, S. Moon, K. J. Lee, and Y.-S. Kim, Reference-frame-independent, measurement-device-Independent quantum key distribution using fewer quantum states, Opt. Lett. **45**, 2624 (2020).

[13] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan, Field test of measurement-device-Independent quantum key distribution, IEEE J. Select. Topics Quantum Electron **21**, 116 (2015).

[14] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over Untrustful Metropolitan Network, Phys. Rev. X **6**, 011024 (2016).

[15] Y. Cao, *et al.*, Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **125**, 260503 (2020).

[16] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Chip-based measurement-device-Independent quantum key distribution, Optica **7**, 238 (2020).

[17] L. Cao, *et al.*, Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems, Phys. Rev. Appl. **14**, 011001 (2020).

[18] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over a 404 Km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[19] H. Weinfurter, Experimental bell-state analysis, Europhys. Lett. **25**, 559 (1994).

[20] S. L. Braunstein and A. Mann, Measurement of the bell operator and quantum teleportation, Phys. Rev. A **51**, R1727 (1995).

[21] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Dense Coding in Experimental Quantum Communication, Phys. Rev. Lett. **76**, 4656 (1996).

[22] F. Zhu, W. Zhang, and Y. Huang, Fiber-based frequency-degenerate polarization entangled photon pair sources for information encoding, Opt. Express **24**, 25619 (2016).

[23] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over 200 Km, Phys. Rev. Lett. **113**, 190501 (2014).

[24] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, A cost-effective measurement-device-Independent quantum key distribution system for quantum networks, Quantum Sci. Technol. **2**, 04LT01 (2017).

[25] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phase-Reference-Free Experiment of Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **115**, 160502 (2015).

[26] Y. Choi, O. Kwon, M. Woo, K. Oh, S.-W. Han, Y.-S. Kim, and S. Moon, Plug-and-play measurement-device-Independent quantum key distribution, Phys. Rev. A **93**, 032319 (2016).

[27] C. H. Park, M. K. Woo, B. K. Park, M. S. Lee, Y.-S. Kim, Y.-W. Cho, S. Kim, S.-W. Han, and S. Moon, Practical plug-and-play measurement-device-Independent quantum key distribution with polarization division multiplexing, IEEE Access **6**, 58587 (2018).

[28] M. Bloch, S. W. McLaughlin, J.-M. Merolla, and F. Patois, Frequency-coded quantum key distribution, Opt. Lett. **32**, 301 (2007).

[29] T. Kobayashi, R. Ikuta, S. Yasui, S. Miki, T. Yamashita, H. Terai, T. Yamamoto, M. Koashi, and N. Imoto, Frequency-domain hong–ou–Mandel interference, Nat. Photonics **10**, 441 (2016).

[30] 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**, 2760 (2018).

[31] H.-H. Lu, J. M. Lukens, N. A. Peters, O. D. Odele, D. E. Leaird, A. M. Weiner, and P. Lougovski, Electro-Optic Frequency Beam Splitters and Tritters for High-Fidelity Photonic Quantum Information Processing, Phys. Rev. Lett. **120**, 030502 (2018).

[32] C. K. Hong, Z. Y. Ou, and L. Mandel, Measurement of Subpicosecond Time Intervals between Two Photons by Interference, Phys. Rev. Lett. **59**, 2044 (1987).

[33] N. Gisin and R. Thew, Quantum communication, Nat. Photonics **1**, 165 (2007).

[34] T. B. Pittman, D. V. Strekalov, A. Migdall, M. H. Rubin, A. V. Sergienko, and Y. H. Shih, Can Two-Photon Interference Be Considered the Interference of Two Photons?, Phys. Rev. Lett. **77**, 1917 (1996).

[35] Y.-S. Kim, O. Slattery, P. S. Kuo, and X. Tang, Conditions for two-photon interference with coherent pulses, Phys. Rev. A **87**, 063843 (2013).

[36] X. Ma and M. Razavi, Alternative schemes for measurement-device-Independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[37] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[38] X. Ma, C.-H. F. Fung, and M. Razavi, Statistical fluctuation analysis for measurement-device-Independent quantum key distribution, Phys. Rev. A **86**, 052305 (2012).

[39] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics, Phys. Rev. X **10**, 031030 (2020).

[40] P. Lu, S. J. Mihailov, D. Coulas, H. Ding, and X. Bao, Low-loss random fiber gratings made with an fs-IR laser for distributed fiber sensing, J. Lightwave Technol. **37**, 4697 (2019).

[41] C. Reimer, S. Sciara, P. Roztocki, M. Islam, L. Romero Cortés, Y. Zhang, B. Fischer, S. Loranger, R. Kashyap, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, W. J. Munro, J. Azaña, M. Kues, and R. Morandotti, High-dimensional one-way quantum processing implemented on d-level cluster states, Nat. Phys. **15**, 148 (2019).

[42] G.-Z. Xu, W.-J. Zhang, L.-X. You, J.-M. Xiong, X.-Q. Sun, H. Huang, X. Ou, Y.-M. Pan, C.-L. Lv, H. Li, Z. Wang, and X.-M. Xie, Superconducting microstrip single-photon detector with system detection efficiency over 90% at 1550 nm, Photon. Res. **9**, 958 (2021).

[43] Phase Modulators, https://www.eospace.com/phase-modulator.

[44] C. Wang, M. Zhang, X. Chen, M. Bertrand, A. Shams-Ansari, S. Chandrasekhar, P. Winzer, and M. Lončar, Integrated lithium niobate electro-optic modulators operating at CMOS-compatible voltages, Nature **562**, 101 (2018).

[45] A. J. Mercante, S. Shi, P. Yao, L. Xie, R. M. Weikle, and D. W. Prather, Thin film lithium niobate electro-optic modulator with terahertz operating bandwidth, Opt. Express **26**, 14810 (2018).

[46] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation, Nature **390**, 575 (1997).

[47] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental Entanglement Swapping: Entangling Photons That Never Interacted, Phys. Rev. Lett. **80**, 3891 (1998).