Hybrid High-Dimensional Quantum Key Distribution for a Composable Quantum Network

Fang-Xiang Wang,[1,2] Qi-Hang Lu,[1,2] Wei Chen,[1,2,*] Shuang Wang,[1,2] Haiyang Fu,[1,2] Yinjie Lu,[1,2] Penglei Hao,[1,2] Jia-Lin Chen,[1,2] Wenjing Ding,[1,2] Jianyu Ma,[1,2] De-Yong He,[1,2] Zhen-Qiang Yin,[1,2] Zheng Zhou,[1,2] Guang-Can Guo,[1,2] and Zheng-Fu Han[1,2]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

(Received 31 October 2022; revised 28 February 2023; accepted 14 April 2023; published 18 May 2023)

High-dimensional quantum key distribution (HD-QKD) possesses a higher noise-tolerance ability and secure key rate. In the work presented here, by developing a mapping method for multiple degrees of freedom (DOFs), we propose and implement a HD-QKD system with a quantum bit error rate as low as 0.57%. Our HD-QKD system can stably achieve high secure key rates and is composable, allowing one to build HD quantum networks compatible with multiple DOFs. The results indicate that the proposed scheme could bridge HD and two-dimensional terminals encoded in different DOFs and could support large-scale deployment of quantum networks with high performance. Our work significantly enhances the performance of HD-QKD and strengthens the practical applications of large-scale quantum networks in a hybrid way.

DOI: 10.1103/PhysRevApplied.19.054060

I. INTRODUCTION

Quantum key distribution (QKD) and quantum networks [1–7] enable users to transfer information securely by utilizing fundamental principles of quantum mechanics. They offer information-theoretic security to users who need to share private information [8–10], and play a key role in the networking of quantum nodes remotely [11–13]. Hence, quantum networks are a promising technology for the next generation of communication networks. QKD systems and quantum networks are commonly built using two-dimensional (2D) quantum states encoded in polarization (spin) [14], time bins, and phase [15]. So far, several encoding and decoding systems have been developed significantly for quantum networks [4–7]. Each of these systems has its own advantages, and networking of nodes with different degrees of freedom (DOFs) has rarely been considered. For example, time-bin (phase) [4,6] and polarization-based [7] quantum networks have been deployed on a large scale. However, these quantum networks cannot be interconnected, due to the differences between DOFs with different encodings. Additionally, the relatively low secure key rate is another obstacle to practical applications. Thus, issues of performance and compatible networking need to be addressed together, so that low-cost large-scale deployment of quantum networks could be accessible.

In order to improve the performance of QKD, researchers are pursuing new 2D protocols [16–18], as well as high-dimensional QKD (HD-QKD) systems that manipulate multiple dimensions of photon states [19,20]. Photons, the carriers of information, are particles that show wave-particle duality and possess multiple DOFs, such as the time-bin, spin, spatial, and frequency domains. As a result of encoding information in high-dimensional photon states, HD-QKD systems possess a much higher noise-tolerance ability and a much higher secure key rate [21–25]. HD-QKD systems usually prepare HD photon states either in a single DOF, such as that of the time domain [21] or of spatial modes [26], or in multiple DOFs [23,27–29]. In a single-DOF scenario, the fidelities of all HD states may be affected by the level of manipulation of the DOF and may suffer from a relatively high quantum bit error rate (QBER) [22,26]. In the second scenario, most multi-DOF schemes realize the preparation of HD states by utilizing DOF coupling, and the fidelity is limited by the levels of manipulation of all DOFs [28,30,31]. Additionally, these HD-QKD systems with DOFs with different encodings are compatible neither with each other nor with 2D-QKD terminals. These experimental difficulties limit the application of HD-QKD on a large scale.

*weich@ustc.edu.cn

In the work presented in this paper, we realize a hybrid HD-QKD system by simultaneously manipulating three DOFs (time bins, polarization, and spatial modes) of photons. The prepared HD state is in the form of a direct product of substates in different DOFs. By using a DOF-mapping method, the system decouples the preparation procedures of the HD quantum states in different DOFs and prevents the spread of experimental errors among the DOFs. Hence, we can manipulate HD photon states with high fidelity, and we implement an eight-dimensional (8D)-QKD system with a 0.57% average QBER for a 3-h running time. We also demonstrate the composability of the HD-QKD system, which allows us to connect it to QKD terminals encoded in different DOFs. Our experimental results show that an HD-QKD terminal can be used as both a backbone and an intermediary in building a general hybrid quantum network compatible with deployed quantum networks.

II. HYBRID HD QUANTUM NETWORK

Quantum networks with different encoding schemes coexist side by side. Because of the orthogonality of different DOFs and the differences between different physical implementations, it is impossible to compatibly connect different QKD terminals and quantum networks together. This increases the cost of building a general quantum network and prevents secure communication between terminals using DOFs with different encodings. HD-QKD utilizes multiple DOFs of photons simultaneously and offers the potential to bridge the gap between terminals and networks with different DOFs. However, how to bridge this gap is still an open question.

A. The general scheme

Here, we propose a high-performance hybrid HD-QKD scheme. It is composable so that it can be adapted to QKD terminals and quantum networks encoded in different DOFs. The encoding (and decoding) procedures for the state spaces in different DOFs are designed to be independent. That is, the HD quantum state is proposed to be in the form of a direct product of different DOFs,

$$|\text{state}\rangle = \mathcal{U}_{\text{DOF}n} \cdots \bigotimes \mathcal{U}_{\text{DOF2}} \bigotimes \mathcal{U}_{\text{DOF1}} |\text{initial}\rangle. \quad (1)$$

If we adopt the decoy-state [9,10] BB84 protocol for both 2D [1] and HD [19] systems with two mutually unbiased bases (MUBs), the orthogonal nature of the state spaces in different DOFs makes it convenient to realize a composable HD-QKD system.

As shown in Fig. 1(a), a HD-QKD transmitter encoded in three DOFs (time, spatial, and spin domains) according to Eq. (1) is able to be connected to different QKD receivers. It can be connected to a HD receiver directly. When the state space of the receiver is in a subspace, such as in a sub-HD (larger than 2D) or 2D space, the HD transmitter closes the modulation of the subspaces

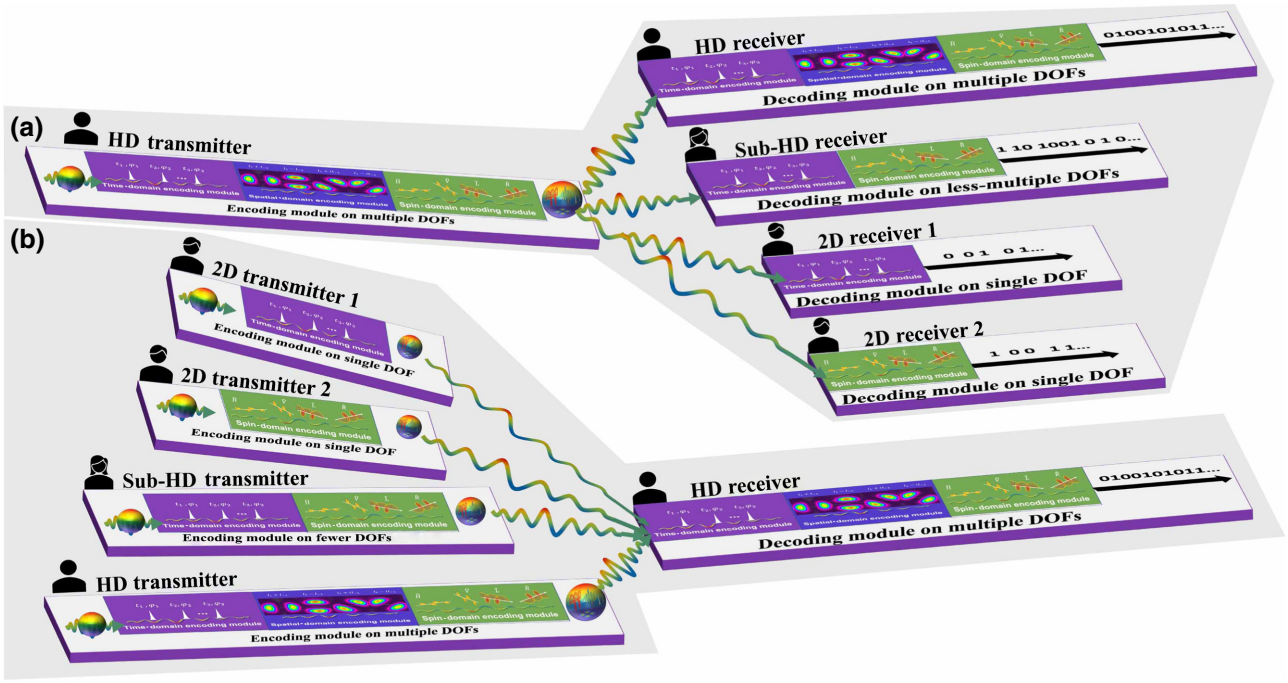

FIG. 1. Concept of a hybrid HD-QKD system that is composable with different QKD terminals. (a) The HD-QKD transmitter is composable so that it can be connected to a corresponding HD-QKD receiver directly or to a sub-HD or 2D-QKD receiver by closing the state spaces in several DOFs. (b) A composable HD-QKD receiver can be adapted to different QKD transmitters in a similar way.

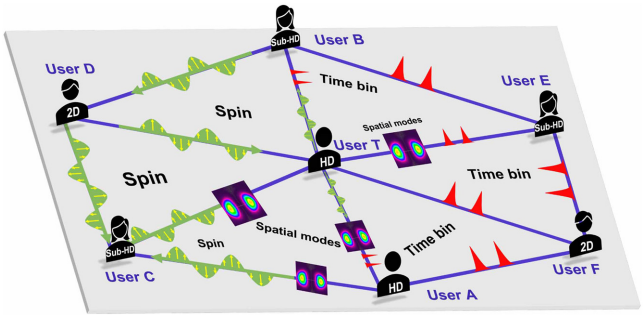

FIG. 2. Concept of composable quantum network. The HD and sub-HD QKD terminals act as important intermediaries for building a general quantum network compatible with different encoding systems.

in particular DOFs to build a compatible connection. For example, when the state space of the receiver is in a subspace of DOFs of time and spin, the HD transmitter closes the state modulation in the DOF of spatial modes to build a QKD connection to a sub-HD receiver (where the state space is larger than two dimensions). For a HD receiver, following Eq. (1), connections to different transmitters are realized in the same way [see Fig. 1(b)].

By using the strategies proposed in Fig. 1, we are able to build a general quantum network that is compatible with QKD terminals encoded in different DOFs. An example of a general quantum network is shown in Fig. 2. A HD-QKD terminal (user A, with three DOFs and eight dimensions) can either establish a high-noise-tolerance and high-secure-key-rate quantum link with another HD-QKD terminal (user T) or communicate with a sub-HD terminal (user C, with two DOFs and four dimensions) or a 2D terminal (user F, with one DOF and two dimensions). This HD-QKD terminal can also act as a trusted repeater to establish a secure quantum link between user C (encoded in the DOFs of spin and spatial modes) and user F (encoded in the DOF of time bins), who cannot communicate with each other directly, due to the encoding gap (see Sec. IV for further discussion).

B. DOF-mapping method

In order to realize a hybrid quantum network scheme, the modulation procedure needs to be divided into independent modules according to the DOFs. These modules should be stable enough to manipulate and easy to switch (i.e., open or close). A DOF-mapping method makes it possible to bypass difficulties of modulation in one DOF by the use of mature technologies in another one, and hence to realize high-quality manipulation of HD quantum states [23]. We design a sophisticated setup here to implement DOF mapping among the time, spin, and spatial-mode domains.

1. Path selection

Figure 3(a) shows the structure of a fiber-based Sagnac interferometer, which is immune to feedback and has good performance [32,33]. When a phase modulator (PM) is inserted into the Sagnac loop asymmetrically, the Sagnac interferometer performs active path selection with different modulation voltages (or phases). As shown in the figure, the photon states of the forward and backward loops go through the PM at different times and hence experience phases φ_f and φ_b, respectively. The output amplitudes for paths 1 and 2 are then determined by the phase difference $\Delta\phi = \varphi_f - \varphi_b$. Then, DOF mapping can be achieved by rational utilization of these paths.

2. Time-domain encoding module

By cascading an asymmetric Mach-Zehnder interferometer after the Sagnac interferometer, two sets of 2D MUBs in the DOF of the time domain are prepared according to Fig. 3(b). When the phase difference of PM1, $\Delta\varphi = \varphi_f - \varphi_b$, equals 0 or π, the photon state goes via path 1 (the short arm) or path 2 only and is output, correspondingly, from the AMZI as $|t_1\rangle$ or $|t_2\rangle$. When $\Delta\varphi = \pi/2$ and the phase of PM2 is set to 0 or π, the output state from the AMZI becomes $|t_1\rangle \pm |t_2\rangle$. We define $\{|\psi_t\rangle\} \in \{|t_1\rangle, |t_2\rangle\}$ and $\{|\xi_t\rangle\} \in \{|t_1\rangle \pm |t_2\rangle\}$ as the first and second sets, respectively, of MUBs in the DOF of time bins.

3. Spatial-domain encoding module

When the AMZI is replaced with symmetric paths and a polarizing beam splitter, the Sagnac-MZI structure is able to map path selection into polarization selection and then into spatial modes [Fig. 3(c)]. In this structure, when $\Delta\varphi = 0$, the photon output from the PBS is linearly polarized ($|H\rangle$, aligned with the slow axis). When $\Delta\varphi = \pi$, the corresponding polarization becomes $|V\rangle$ (aligned with the fast axis). The orthogonal linear polarization states are then coupled to free space, where the path consists of a q-plate, a half-wave plate (HWP), and a free-space PBS. The operator of a q-plate is

$$\hat{\mathcal{Q}} = \cos(\theta/2)\hat{\mathbf{I}} + i\sin(\theta/2)\Big[|L\rangle\langle R| \otimes \sum_l |l-2q\rangle\langle l| + |R\rangle\langle L| \otimes \sum_l |l+2q\rangle\langle l|\Big], \tag{2}$$

where $\hat{\mathbf{I}}$ is a unit matrix, $|L\rangle$ and $|R\rangle$ are the left and right spins, $|l\rangle$ is a Laguerre-Gaussian mode with zero radial index and azimuthal index l [34], $2q = 1$ is the azimuthal number modulated by the q-plate, and the coupling coefficient θ is determined by the voltage applied to the q-plate. The free-space part here realizes the passive DOF mapping between the spin and the spatial modes as follows.

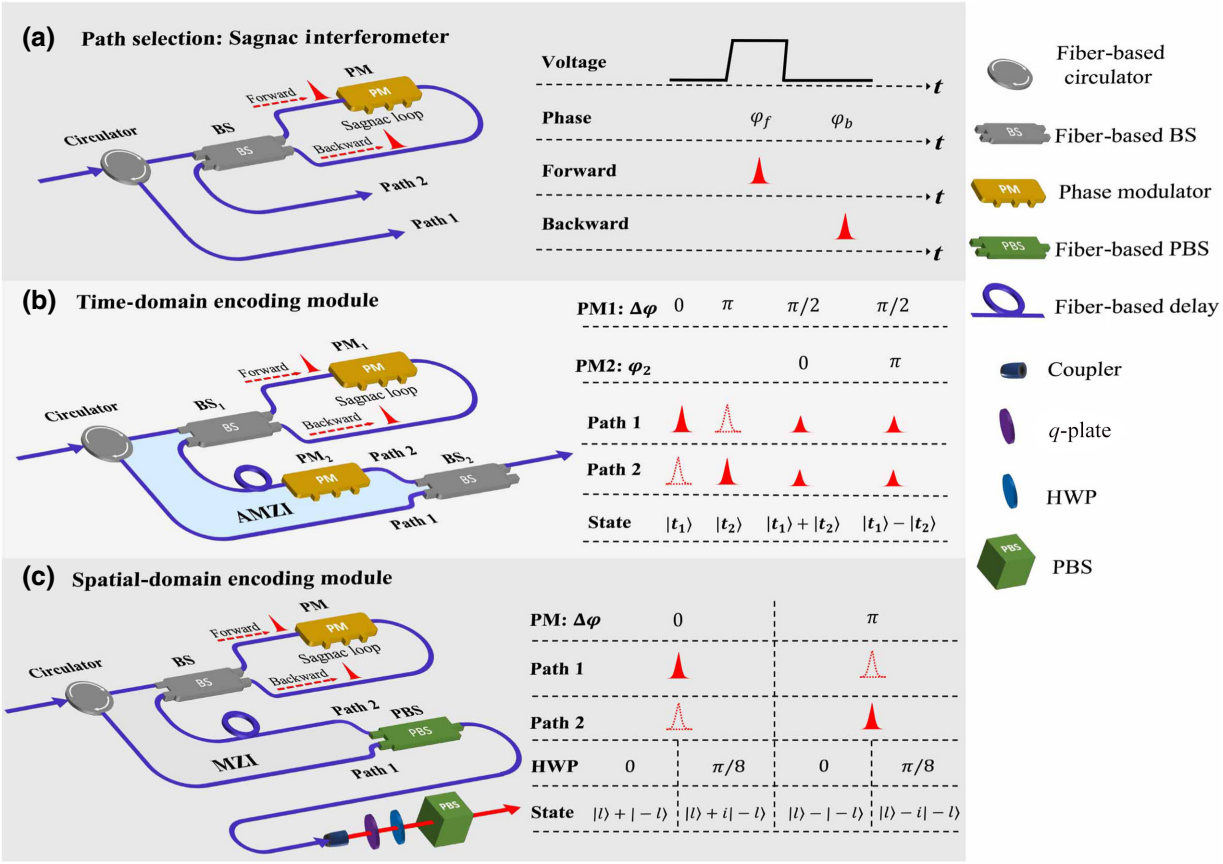

FIG. 3. Elemental DOF-mapping manipulation modules. (a) Path selection using an active Sagnac interferometer. (b) Time-domain encoding module. An asymmetric Mach-Zehnder interferometer (AMZI) is cascaded after the Sagnac interferometer. (c) Spatial-domain encoding module, where a symmetric Mach-Zehnder interferometer based on a polarizing beam splitter (PBS) is cascaded after the Sagnac interferometer.

The coupling coefficient θ is equal to π, so that the q-plate fully couples the DOFs of the spin and spatial modes into the radial vector vortex $(1/\sqrt{2})(|L\rangle|-2q\rangle + |R\rangle|2q\rangle)$. Then, the HWP and PBS project the the vector vortex into a spatially homogeneous linearly polarized Laguerre-Gaussian mode [23,29]. We take one case as an example below. When both $\Delta\varphi$ and the rotation angle of the HWP α equal zero, the spatial-domain encoding module works as follows: $|\text{initial}\rangle \xrightarrow[\text{Sagnac}]{\Delta\varphi=0} |\text{path 1}\rangle \xrightarrow[\text{PBS}]{} |H\rangle \xrightarrow[q\text{-plate}]{2q=l}$ $(1/\sqrt{2})(|R\rangle|l\rangle + |L\rangle|-l\rangle) \xrightarrow[\text{HWP and PBS}]{\alpha=0} (1/\sqrt{2})|H\rangle(|l\rangle + |-l\rangle)$. As shown in Fig. 3(c), the parameter combination $\{\Delta\varphi, \alpha\}$ realizes the preparation of two sets of 2D MUBs in the DOF of spatial modes, where we define $\{|\psi_o\rangle\} \in \{|l\rangle \pm |-l\rangle\}$ and $\{|\xi_o\rangle\} \in \{|l\rangle \pm i|-l\rangle\}$.

The DOF-mapping modules above are based on a highly stable Sagnac interferometer; only the basis $\{\xi_t\}$ needs feedback to compensate for the phase drift between path 1 and path 2 of the AMZI [Fig. 3(b)]. Thanks to the high extinction ratio of the Sagnac interferometer, HD state preparation with ultralow errors can be expected. This also means that we are able to implement a HD-QKD system using three DOFs that is as stable as a 2D-QKD system.

III. EXPERIMENTAL DEMONSTRATION

By fully exploiting the DOF-mapping technologies proposed in Sec. II B, three demonstrations are implemented to verify a high-performance (ultralow QBER) hybrid HD-QKD system and its composability so that it can be used to build a general HD quantum network. The first demonstration implements an 8D-QKD system. The second and third demonstrations show the composability of HD-QKD terminals.

A. Demonstration 1: The 8D-QKD system

Three DOFs, of time bins, spin, and spatial modes, are used to implement the 8D-QKD system. The two sets of MUBs are constructed in the following form:

$$\begin{aligned} |\psi^{\mathcal{Z}}\rangle &= |\psi_t\rangle \otimes |\psi_o\rangle \otimes |\psi_s\rangle, \\ |\xi^{\mathcal{X}}\rangle &= |\xi_t\rangle \otimes |\xi_o\rangle \otimes |\xi_s\rangle, \end{aligned} \tag{3}$$

where $|\psi_s\rangle \in \{|H\rangle, |V\rangle\}$ and $|\xi_s\rangle = |H\rangle \pm |V\rangle$ are the two sets of MUBs in the DOF of spin. The bases $\{|\psi^{\mathcal{Z}}\rangle\}$ and $\{|\xi^{\mathcal{X}}\rangle\}$ are named the $\mathcal{Z}$ and $\mathcal{X}$ bases, respectively. The $\mathcal{Z}$ basis is used to share a secure key, and the $\mathcal{X}$ basis is for eavesdropper monitoring.

The experimental setup of the 8D-QKD system is shown in Fig. 4. In the transmitter [Fig. 4(a)], the laser pulse first goes through an attenuator (Att) and a Sagnac interferometer to prepare decoy states with variable intensities. The signal state is $|\mu_1\rangle$, and the two decoy states are $|\mu_2\rangle$ and $|\mu_3\rangle$, where μ_1, μ_2, and μ_3 are the corresponding average photon numbers, and $\mu_1 > \mu_2 > \mu_3$. Then, the time-domain encoding module prepares $|\psi_t\rangle$ and $|\xi_t\rangle$ in the DOF of time bins. Afterwards, three cascaded Sagnac interferometers implement an active 1×4 optical switcher [in the dashed black box in Fig. 4(a)]. Each of the four paths is followed by a spatial-domain encoding module to prepare $|\psi_o\rangle$ and $|\xi_o\rangle$. Then, each of these four paths is rotated into one particular polarization by HWPs. As shown in the green dashed box in Fig. 4(a)), the two upper paths prepare $|\psi_s\rangle$ (in the $\mathcal{Z}$ basis) and the lower paths prepare $|\xi_s\rangle$ (in the $\mathcal{X}$ basis). Finally, these paths are merged into a single path by two PBSs and one BS. The prepared 8D photon states are then incident into the quantum channel. Because of the preparation procedure of the HD photon states in the transmitter, the modulations of different DOFs are independent.

In the 8D receiver in Fig. 4(b), the decoding modules for the spin (in the green dashed box) and the spatial modes (in the blue dashed box) are the inverse transforms of the corresponding encoding modules. For the MUBs in the DOF of time bins, the $\mathcal{Z}$ basis $\{|\psi_t\rangle\}$ is directly detected by gated-mode (In,Ga)As-type single-photon detectors (SPDs) (in the purple dashed box), and the $\mathcal{X}$ basis $\{|\xi_t\rangle\}$ is decoded by an AMZI (in the purple dashed box again). After decoding, all states are detected by SPDs. Obviously, the independence of the decoding procedures of different DOFs always holds. The length difference among all AMZIs in Fig. 4(a) is 2 m, corresponding to a time interval of 10 ns.

An additional intensity μ_f is used to feed back the phase drift of $\{|\xi_t\rangle\}$ caused by the AMZI of the time-bin encoding module. The feedback pulses are randomly inserted into the encoded pulse sequences. In other words, the first

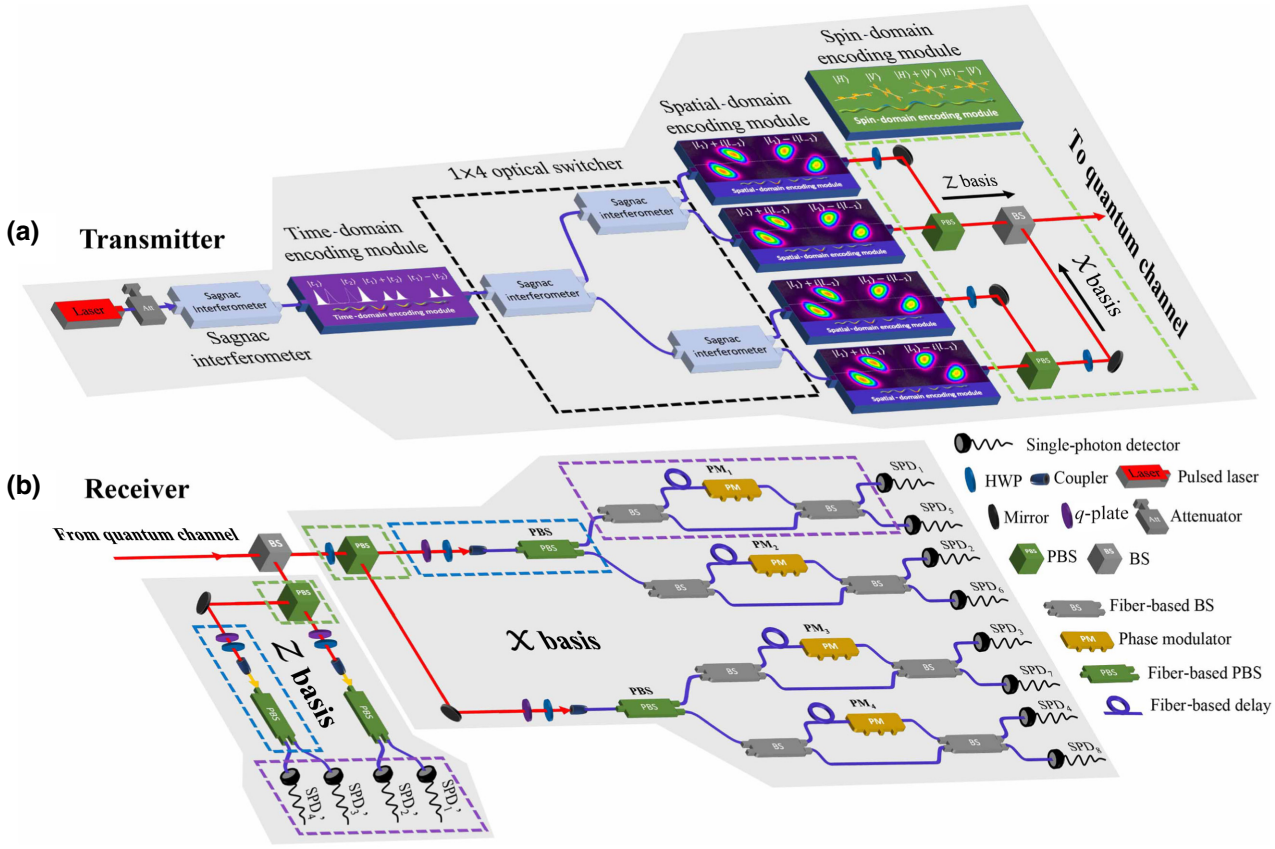

FIG. 4. Setup of the 8D-QKD system. (a) The 8D transmitter. This uses the DOF-mapping method and independent manipulation of subspaces in different DOFs. The laser pulse is attenuated to the single-photon level by an attenuator. The Sagnac interferometers are used to prepare decoy states and to select paths. (b) The 8D receiver. The green, blue, and purple dashed boxes are the decoding modules for the DOFs of spin, spatial modes, and time bins, respectively.

Sagnac interferometer after the laser source generates four intensities. Three intensities are used to execute the QKD procedure, and the fourth intensity, μ_f, is for phase-drift feedback. All of these four intensities go through the time-, spatial-, and spin-domain encoding modules. The transmitter sends the position of the feedback pulses to the receiver every 200 ms. The receiver then calculates and compensates for the phase drift of $\{|\xi^{\mathcal{X}}\rangle\}$ according to the QBERs (calculated from the detected counts of these feedback pulses). This feedback mode gives detailed phase drifts for all states of the $\mathcal{X}$ basis ($\{|\xi^{\mathcal{X}}\rangle\}$). Thus, we can perform accurate phase compensation for all AMZIs. The average photon number μ_f in a feedback pulse varies from 0.75 to 8 as the channel loss increases from 0 to 25 dB. The corresponding feedback duty cycle varies from 0.05% to 20%. The detection efficiency and dark count rate (DCR) of the gated-mode (In,Ga)As SPD are 21% and 1×10^{-6}/gate, respectively. μ_3 is fixed at 1×10^{-4}, while the other decoy parameters are optimized depending on the value of the channel loss. The repetition rate of the system is 10 MHz.

B. Demonstration 2: The 8D-QKD transmitter broadcasts to two four-dimensional (4D)-QKD receivers

In this scenario, bases $\{\psi_o\}$ in the DOF of spatial modes are used as two orthogonal multiplexed channels, and the bases $\{|\xi_o\rangle\}$ are closed. The HD quantum states prepared and measured are

$$\begin{aligned}
|\psi_1^{\mathcal{Z}}\rangle^{4D} &= |\psi_t\rangle \otimes |\psi_s\rangle \otimes (|l\rangle + |-l\rangle),\\
|\psi_2^{\mathcal{Z}}\rangle^{4D} &= |\psi_t\rangle \otimes |\psi_s\rangle \otimes (|l\rangle - |-l\rangle),\\
|\xi_1^{\mathcal{X}}\rangle^{4D} &= |\xi_t\rangle \otimes |\xi_s\rangle \otimes (|l\rangle + |-l\rangle),\\
|\xi_2^{\mathcal{X}}\rangle^{4D} &= |\xi_t\rangle \otimes |\xi_s\rangle \otimes (|l\rangle - |-l\rangle),
\end{aligned} \tag{4}$$

where the subscripts 1 and 2 represent the first and second 4D receivers, respectively. The 8D-QKD transmitter randomly prepares and sends quantum states according to Eq. (4) to both 4D-QKD receivers in a broadcast way. The 4D-QKD terminals filter, decode, and measure photon states accordingly.

In Demonstration 2, the decoding modules of the 8D-QKD receiver are recomposed to implement 4D-QKD terminals. The recomposition is performed by setting the rotation angles of the HWPs adjacent to the couplers to zero. This means that the demonstration requires no hardware change in the 8D-QKD terminals. In fact, the rotation of the HWPs can be achieved in software by using motor-driven rotators. In this demonstration, the 8D transmitter randomly prepares photon states according to Eq. (4). A nonpolarizing beam splitter is used to route the photon state passively. The photon state is then sent to the 4D receivers. If the photon state is prepared in $|\psi_1^{\mathcal{Z}}\rangle$ (or $|\xi_1^{\mathcal{X}}\rangle$) and is received by the first 4D receiver, the detection result is suitable for secure key extraction. If $|\psi_1^{\mathcal{Z}}\rangle$ (or $|\xi_1^{\mathcal{X}}\rangle$) is passively routed to the second 4D receiver, the photon state is filtered out by the demultiplexing module. Unexpected detection results (due to the limited signal-to-noise ratio) are rejected in the basis-choice confirmation step of the QKD procedure. If the photon state is prepared in $|\psi_2^{Z}\rangle$ (or $|\xi_2^{X}\rangle$) and is passively routed to the first 4D receiver, the photon state will be filtered out by the demultiplexing module of the 4D-receiver 1. The states $|l\rangle + |-l\rangle$ and $|l\rangle - |-l\rangle$ are used for multiplexing the channels of the 4D users 1 and 2, respectively.

C. Demonstration 3: The 8D-QKD transmitter broadcasts to four 2D-QKD receivers

Here, MUBs of $\{|\psi_t\rangle\}$ and $\{|\xi_t\rangle\}$ in the DOFs of both spatial modes and spin are used as four multiplexed channels. The $\mathcal{Z}$ basis $\{|\psi_t\rangle\}$ and the $\mathcal{X}$ basis $\{|\xi_t\rangle\}$, in the DOF of time bins, are used to execute the 2D-QKD protocol. The quantum states used are

$$\begin{aligned}
|\psi^{\mathcal{Z}}\rangle_n^{2D} &= |\psi_t\rangle \otimes |\psi_s\rangle_n \otimes |\psi_o\rangle_n,\\
|\xi^{\mathcal{X}}\rangle_n^{2D} &= |\xi_t\rangle \otimes |\psi_s\rangle_n \otimes |\psi_o\rangle_n,
\end{aligned} \tag{5}$$

where the subscript n denotes the nth 2D user, $|\psi_s\rangle_n \otimes |\psi_o\rangle_n \in \{|H\rangle, |V\rangle\} \otimes (|l\rangle \pm |-l\rangle)$, $\langle\psi_s|_{n_1}\langle\psi_o|_{n_1}|\psi_s\rangle_{n_2}|\psi_o\rangle_{n_2} = \delta(n_1, n_2)$, and $\delta(n_1, n_2)$ is the Dirac function.

In Demonstration 3, the 2D-QKD receiver is also composed from the 8D-QKD receiver. In this demonstration, the passive router consists of one BS and two PBSs. Similarly to Demonstration 2, we need only to set the rotation angles of all HWPs in the receiver to zero, and neither the 8D-QKD transmitter nor the receiver needs any change in the optical or electrical hardware. $|H\rangle(|l\rangle + |-l\rangle)$, $|V\rangle(|l\rangle + |-l\rangle)$, $|H\rangle(|l\rangle - |-l\rangle)$, and $|V\rangle(|l\rangle - |-l\rangle)$ are the multiplexed channels for the 2D users 1–4, respectively.

It should be noted that all demonstrations above are run in real time. The transmitter prepares photon states randomly (using pseudorandom numbers) in each round. In both Demonstration 2 and Demonstration 3, all receivers work independently and simultaneously. Only a single pulse is prepared and sent by the transmitter in each round, to avoid unexpected security loopholes.

IV. RESULTS AND DISCUSSION

In Demonstration 1, we verify the performance of the 8D-QKD system for channel losses of 0, 10, 20, and 25 dB. The channel loss is adjusted by use of a variable optical attenuator. For each loss value, the decoy-state parameters are reoptimized, and the system runs continuously for nearly 3 h (10^4 s). Figure 5 gives the QBERs of the 8D-QKD system for losses of 0 and 25 dB. For a 0-dB-loss channel, the online running QBERs of the system are

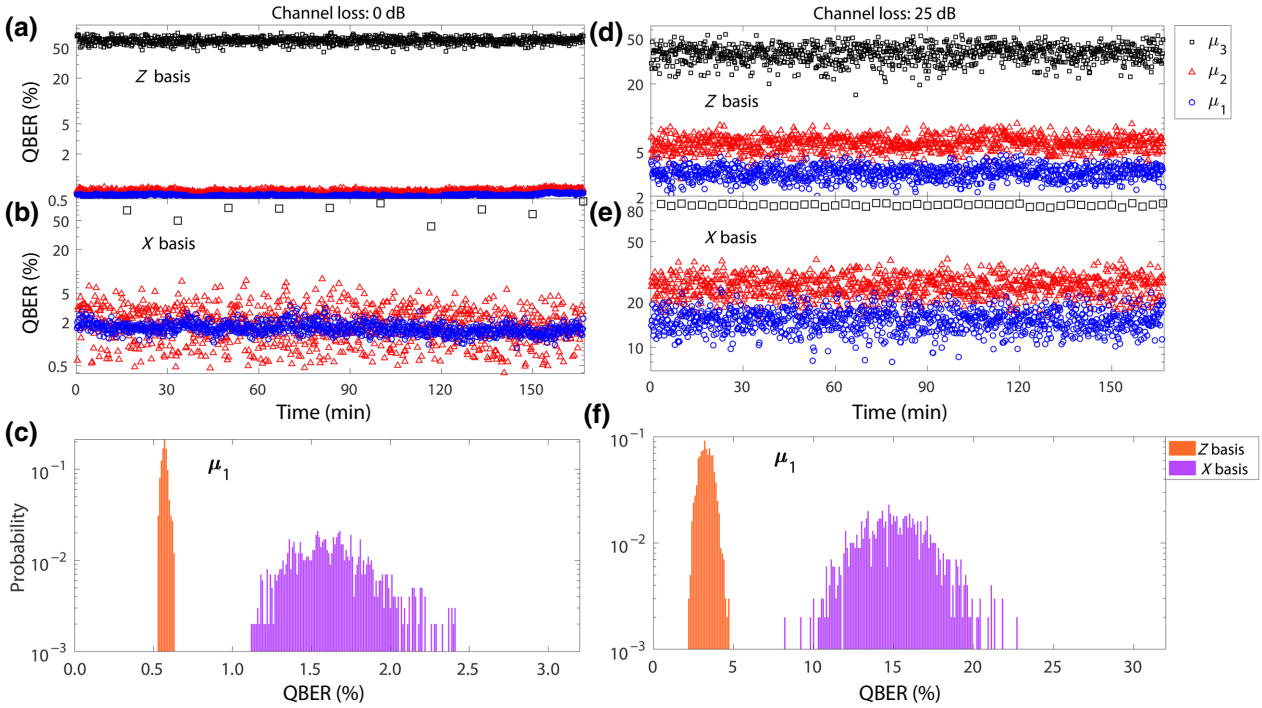

FIG. 5. Performance of the point-to-point 8D-QKD system. Real-time running QBERs for (a),(d) $\mathcal{Z}$ and (b),(e) $\mathcal{X}$ bases, and (c),(f) probability distributions of QBER of signal state. The first and second columns correspond to 0- and 25-dB-loss channels, respectively. The blue circles, red triangles, and black squares represent $|\mu_1\rangle$, $|\mu_2\rangle$, and $|\mu_3\rangle$, respectively. The orange and purple bars represent the signal states for $\mathcal{Z}$ and $\mathcal{X}$, respectively.

shown in Figs. 5(a) ($\mathcal{Z}$ basis) and 5(b) ($\mathcal{X}$ basis). The QBERs are evaluated every 10 s, with 1000 points in total for each intensity. For the $\mathcal{Z}$ basis, the QBERs for $|\mu_1\rangle$ are all within [0.51%, 0.64%], according to the statistical probability distribution shown in Fig. 5(c) (orange bars). The average QBERs for all intensities are $\langle \mathrm{QBER}\rangle^{\mathcal{Z}}_{\mu_1} = 0.57\%$, $\langle \mathrm{QBER}\rangle^{\mathcal{Z}}_{\mu_2} = 0.64\%$, and $\langle \mathrm{QBER}\rangle^{\mathcal{Z}}_{\mu_3} = 62.68\%$. For the $\mathcal{X}$ basis, the statistical-probability-distribution data show that the running QBERs for the signal state are mostly smaller than 2.5% [purple bars in Fig. 5(c)]. The average QBERs for all intensities are $\langle \mathrm{QBER}\rangle^{\mathcal{X}}_{\mu_1} = 1.66\%$, $\langle \mathrm{QBER}\rangle^{\mathcal{X}}_{\mu_2} = 1.87\%$, and $\langle \mathrm{QBER}\rangle^{\mathcal{X}}_{\mu_3} = 70.68\%$. The results demonstrate that we implement an ultralow-QBER and highly stable 8D-QKD system, which improves the performance of HD-QKD significantly compared with previous work [21,22,30,35,36].

For the 25-dB-loss channel, the high loss results in a low effective photon count rate and requires a longer time to feed back the phase drift of $|\xi_t\rangle$. However, the DCR does not change with the channel loss. Considering these downsides, we find that the QBER in the $\mathcal{X}$ basis increases faster than that in the $\mathcal{Z}$ basis. Figures 5(d)–5(f) show the performance of the 8D-QKD system with a 25-dB-loss channel. The effective count rate is around 2×10^{-5}, and the average QBER for $|\mu_1\rangle$ in the $\mathcal{X}$ basis is 15.19% with a feedback duty cycle of 20%. However, it is still possible to share keys securely with the 8D-QKD system (see Sec. IV A). By increasing the time consumption of the feedback or using SPDs with a lower DCR, the QBER for the $\mathcal{X}$ basis can be significantly suppressed further for a high-loss channel.

In Demonstration 2, we run the quantum network by broadcasting quantum states from the 8D transmitter to two 4D receivers simultaneously. According to the experimental data (for a 0-dB-loss channel) given in Figs. 6(a)–6(c), we can see no significant crosstalk between these two channels during several hours of running. The average QBERs of the signal states for both quantum links are $\langle \mathrm{QBER}\rangle^{\mathcal{X},4\mathrm{D}}_{1(2),\mu_1} = 0.30\%$, $\langle \mathrm{QBER}\rangle^{\mathcal{X},4\mathrm{D}}_{1,\mu_1} = 1.57\%$, and $\langle \mathrm{QBER}\rangle^{\mathcal{X},4\mathrm{D}}_{2,\mu_1} = 1.07\%$. The subscripts 1 and 2 denote the first and second 4D terminals, respectively. The probability distribution of the QBERs in Fig. 6(c) demonstrates the consistency of the performance (with ultralow QBER and high stability) of the quantum network with multiple QKD terminals.

In Demonstration 3, the QBERs are even lower due to the lower total DCR in each 2D-QKD receiver. The performances of all four quantum links are consistent; two examples, for a 0-dB-loss channel, are shown in Figs. 6(d)–6(f) (the first quantum link, 2D user 1) and Figs. 6(h)–6(i) (the fourth quantum link, 2D user 4). For the $\mathcal{Z}$ basis, the average QBERs for $|\mu_1\rangle$ of these two quantum links are

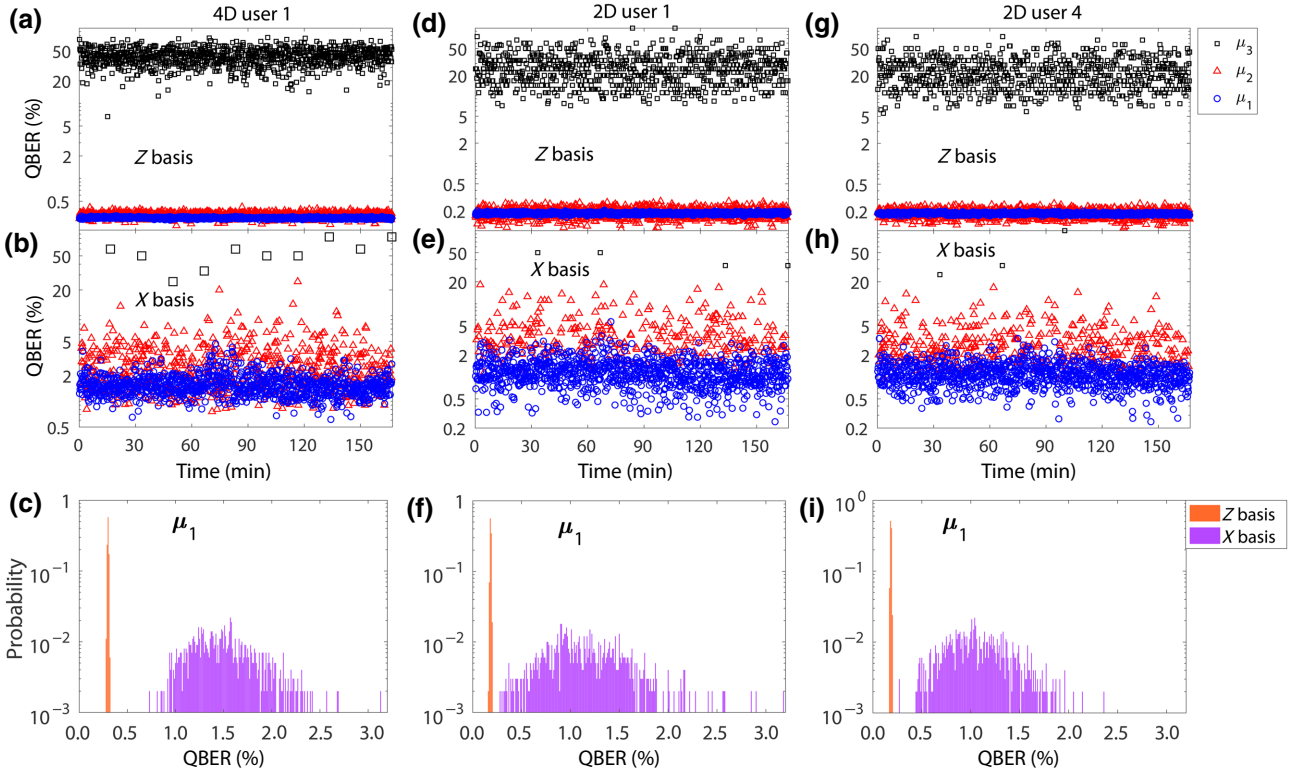

FIG. 6. Performance of the compatible HD quantum network. Real-time running QBERs for (a),(d),(g) $\mathcal{Z}$ and (b),(e),(h) $\mathcal{X}$ bases, and statistical probability distributions of QBER of signal state for 0-dB channel loss in (c) Demonstration 2 and (f),(i) Demonstration 3. The blue circles, red triangles, and black squares show the real-time QBERs for μ_1, μ_2, and μ_3, respectively. The orange and purple bars represent the $\mathcal{Z}$ and $\mathcal{X}$ bases, respectively.

all about 0.18%. For the $\mathcal{X}$ basis, $\langle \mathrm{QBER} \rangle_{1,\mu_1}^{\mathcal{X},2\mathrm{D}} = 1.22\%$ and $\langle \mathrm{QBER} \rangle_{4,\mu_1}^{\mathcal{X},2\mathrm{D}} = 1.12\%$. Figures 6(f) and 6(i) show that the quantum network is stable with multiuser connections, and no conspicuous crosstalk between different channels occurs.

A. Secure key rate

When finite-length effects are considered, the secure key rate of the HD quantum network is given by the following formula [21,37]:

$$R \leq \frac{1}{N} \max_{\beta \geq 0} \left\lfloor 2\tilde{s}_{\mathcal{Z},0} + \tilde{s}_{\mathcal{Z},1} \left[\log_2 d - H_d \left(e_{\mathcal{X},1}^U \right) \right] - \mathrm{leak}_{\mathrm{EC}} + \Delta_{\mathrm{FK}} \right\rfloor, \tag{6}$$

where $N = 10^{11}$ is the number of pulses sent by the transmitter, $\tilde{s}_{\mathcal{Z},0}$ and $\tilde{s}_{\mathcal{Z},1}$ are the numbers of vacuum and single-photon detections, respectively, in the $\mathcal{Z}$ basis of the raw key, d is the dimensionality of the HD quantum system, $e_{\mathcal{X},1}^U$ is the upper bound of the single-photon phase error rate according to the observed QBER in the $\mathcal{X}$ basis, $H_d(x) = -(1-x)\log_2(1-x) - x\log_2(x/d)$ is the d-dimensional Shannon entropy, $\mathrm{leak}_{\mathrm{EC}}$ is the number of bits used during the error-correction process, and $\Delta_{\mathrm{FK}} = -\log[32/(\beta^8 \epsilon_{\mathrm{cor}})]$. The correctness and secrecy parameters ϵ_{cor} and ϵ_{sec} are set to 10^{-12} and 10^{-10}, respectively. The secure key rate R is maximized numerically over values of β satisfying $4\epsilon_{\mathrm{cor}} + 18\beta \leq \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{sec}}$.

The decoy-state parameters of the 8D-QKD system in Demonstration 1 are numerically optimized according to Eq. (6) and are shown in Fig. 7(a). The optimized choice probabilities and the intensities of the decoy states increase to support accurate security estimation for a high-loss channel. Figure 7(b) shows simulated and experimental secure key rates. The blue dashed line shows the potential secure key rate that can be achieved by the 8D-QKD system when superconducting nanowire single-photon detectors (SNSPDs) are used. This indicates that a secure key rate of over 1 Mbps can be obtained using SNSPDs with a 10-MHz repetition rate. The experimental data (blue triangles) obtained using (In,Ga)As SPDs are consistent with the simulated expectations (blue solid line). This demonstrates that the 8D-QKD system achieves a secure key rate of 24.76 kbps for a 10-dB channel loss and performs better than a recent time-bin-based 4D-QKD system with a 300-MHz state-preparation rate [36]. In fact, the secure key rate of the 8D-QKD system achieved (217 kbps for a 2-dB channel loss) is comparable to that of typical gigahertz

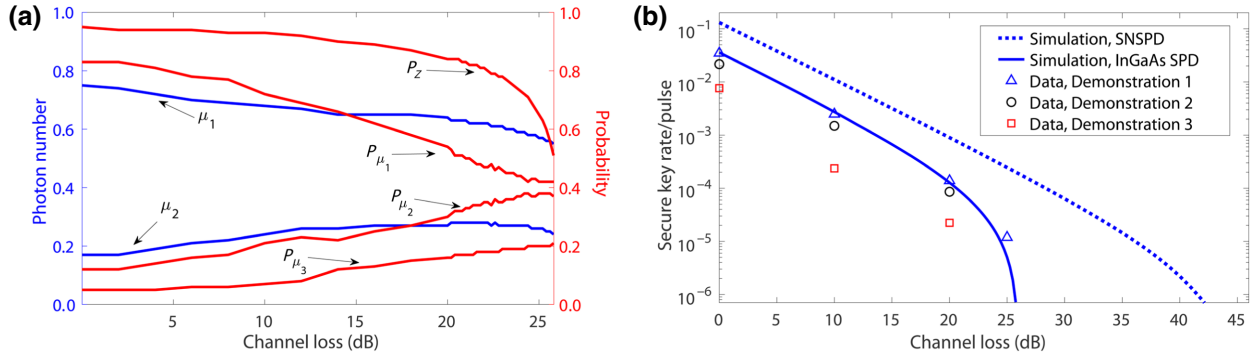

FIG. 7. (a) Optimized decoy-state parameters of the 8D-QKD system, where the blue and red lines correspond to the left and right y axes, respectively. P_Z is the probability of the $\mathcal{Z}$ basis being chosen, and P_{μ_i} is the probability of $|\mu_i\rangle$ being sent by the transmitter. (b) Secure key rates of the 8D-QKD system and the HD quantum network. The blue dashed and solid lines are the simulated secure key rates of the 8D-QKD system when superconducting nanowire single-photon detectors (with 70% detection efficiency and 10^{-8} DCR) and (In,Ga)As-type SPDs (21% detection efficiency and 10^{-6} DCR), respectively, are used. The blue triangles are experimental data obtained from Demonstration 1 (8D-QKD) using (In,Ga)As SPDs.

2D-QKD systems [7,38,39]. As the Sagnac interferometer has been verified to have an extinction ratio of over 30 dB in a 2-GHz system [40], the 8D-QKD system implemented here has the potential to achieve a secure key rate of 48 Mbps for a 4-dB channel loss, much higher than that of state-of-art HD-QKD systems [21,22,35], if it is updated to a gigahertz repetition rate.

The total secure key rates achieved by the broadcast quantum network implemented in Demonstrations 2 (black circles) and 3 (red squares) are given in Fig. 7(b). This shows that the composable quantum network can support secure key distribution via a quantum channel with a loss of over 20 dB. Both the 8D transmitter and the receiver are recomposed in a "software" manner in these two demonstrations. Thus, the composability and compatibility of the HD-QKD scheme are verified clearly. The decline of the secure key rates is attributed to the reduction of the dimensionality of the QKD process from eight to four and two dimensions. By replacing the 8D receiver with optimized 4D and 2D-QKD terminals, the corresponding decoy parameters and insertion losses could be optimized further to maximize the performance of the composable HD quantum network.

The QBERs for the $\mathcal{X}$ basis are higher than those for the $\mathcal{Z}$ basis. This is due to the phase drifts resulting from the long AMZIs, which are fixed on an optical table with neither temperature control nor active vibration isolation. Another reason for the QBERs for the $\mathcal{X}$ basis being distributed on a larger scale is the unbalanced basis-choice probability. This leads to a much smaller effective count rate for the $\mathcal{X}$ basis, and the fluctuations of the corresponding QBERs are larger. If the system were updated to a higher repetition rate, the length of the AMZIs could be shortened significantly. If this was combined with active environment control, the phase drift for the $\mathcal{X}$ basis would be much slower. Our feedback system would then show promise to reduce the corresponding optical QBERs to less than 1%.

In Demonstrations 2 and 3, the 4D (sub-HD) and 2D receivers are implemented by recomposing the 8D receivers. This arrangement allows us to verify the composability of both the HD transmitters and the receivers simultaneously. It is certain that the HD-QKD system can also be recomposed to connect it to QKD terminals that cannot manipulate the multiplexed DOFs. Take the quantum link between user T and user F in Fig. 2 as an example. When the receiver is a time-bin-encoded 2D-QKD terminal (user F), the 8D-QKD transmitter (user T) can be recomposed into a time-bin-encoded 2D-QKD transmitter by fixing the 1×4 optical switcher to select the upper path and adjusting the coupling coefficient θ so that it is equal to 0. Similarly, we can "erase" the time-bin manipulation module of the 8D-QKD terminal by applying a dc voltage to PM1 in Fig. 3(b) to connect it with QKD terminals encoded in the other DOFs (such as the quantum links between user T and user C, or between user B and user D). The 8D receiver can be recomposed in a similar way. Hence, the 8D-QKD system is composable so that it can fit different QKD terminals (HD, sub-HD, and 2D) and quantum networks. Although the broadcast quantum network here can establish a secure link between only two users in any particular round, it can share a secure key between multiple users simultaneously if the number of encoding modules in the HD transmitter is increased.

Additionally, the (sub-)HD terminals here can also play a role as trusted repeaters that can connect QKD terminals encoded in different DOFs. In this mode, as shown in Fig. 2, the HD terminal user T opens the encoding module only in the DOF of spin (time-bins) when connecting with user D (user F). Then, by applying the trusted-repeater protocol, user D and user F are able to share a secure key. Additionally, our composable proposal may

have potential applications in some other HD quantum networks [41].

V. CONCLUSION

In conclusion, we propose and implement a hybrid HD-QKD system. The HD-QKD system has an ultralow QBER and is stable during long-time running. Hence, its secure key rate is comparable to that of typical gigahertz 2D-QKD systems, the cost of which is much higher. Furthermore, the HD-QKD system is composable, so that it is compatible with both HD and 2D-QKD terminals encoded in different DOFs. These merits allow one to establish a general quantum network to connect QKD terminals based on polarization, phase, time bins, and spatial modes with quantum networks. This will significantly enhance the performance and accessibility of a composable hybrid HD quantum network.

The data from this work are available on reasonable request.

ACKNOWLEDGMENTS

This work is supported by the National Key Research and Development Program of China (Grant No. 2018YFA 0306400), the National Natural Science Foundation of China (Grants No. 61905235, No. 62171424, and No. 61961136004), and the Fundamental Research Funds for the Central Universities (Grant No. KY2470000006).

The authors declare that they have no conflicts of interest.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in Proceedings of IEEE International Conference on Computing Systems and Signal Processing (IEEE, Bangalore, 1984), pp. 175.

[2] 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).

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[4] M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[5] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, Nature **501**, 69 (2013).

[6] S. Wang *et al.*, Field and long-term demonstration of a wide area quantum key distribution network, Opt. Express **22**, 21739 (2014).

[7] Y. A. Chen *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[8] D. Gottesman, Hoi-Kwong Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[9] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

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

[11] C. Simon, Towards a global quantum network, Nat. Photonics **11**, 678 (2017).

[12] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, Nature **564**, 225 (2018).

[13] W. Kozlowski and S. Wehner, Towards large-scale quantum networks, arXiv:1909.08396 (2019).

[14] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, Quantum key distribution with 1.25 Gbps clock synchronization, Opt. Express **12**, 2011 (2004).

[15] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, Faraday–Michelson system for quantum cryptography, Opt. Lett. **30**, 2632 (2005).

[16] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

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

[18] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[19] H. Bechmann-Pasquinucci and W. Tittel, Quantum cryptography using larger alphabets, Phys. Rev. A **61**, 062308 (2000).

[20] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using D-Level Systems, Phys. Rev. Lett. **88**, 127902 (2002).

[21] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, Sci. Adv. **3**, e1701491 (2017).

[22] C. Lee, D. Bunandar, Z. Zhang, G. R. Steinbrecher, P. Ben Dixon, F. N. C. Wong, J. H. Shapiro, S. A. Hamilton, and D. Englund, Large-alphabet encoding for higher-rate quantum key distribution, Opt. Express **27**, 17539 (2019).

[23] F.-X. Wang, W. Chen, Z.-Q. Yin, S. Wang, G.-C. Guo, and Z.-F. Han, Characterizing High-Quality High-Dimensional Quantum Key Distribution by State Mapping Between Different Degrees of Freedom, Phys. Rev. Appl. **11**, 024070 (2019).

[24] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, High-dimensional quantum communication: Benefits, progress, and future challenges, Adv. Quantum Technol. **2**, 1900038 (2019).

[25] X.-M. Hu *et al.*, Pathways for Entanglement-Based Quantum Communication in the Face of High Noise, Phys. Rev. Lett. **127**, 110505 (2021).

[26] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D.

J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, New J. Phys. **17**, 033033 (2015).

[27] A. Sit, Frédéric Bouchard, Robert Fickler, Jérémie Gagnon-Bischoff, Hugo Larocque, Khabat Heshami, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, Christoph Marquardt, Gerd Leuchs, Robert W. Boyd, and Ebrahim Karimi, High-dimensional intracity quantum cryptography with structured photons, Optica **4**, 1006 (2017).

[28] I. Nape, E. Otte, A. Valles, C. Rosales-Guzman, F. Cardano, C. Denz, and A. Forbes, Self-healing high-dimensional quantum key distribution using hybrid spin-orbit Bessel states, Opt. Express **26**, 26946 (2018).

[29] Q.-K. Wang, F.-X. Wang, J. Liu, W. Chen, Z.-F. Han, A. Forbes, and J. Wang, High-Dimensional Quantum Cryptography with Hybrid Orbital-Angular-Momentum States through 25 km of Ring-Core Fiber: A Proof-of-Concept Demonstration, Phys. Rev. Appl. **15**, 064034 (2021).

[30] D. Cozzolino, Davide Bacco, Beatrice Da Lio, Kasper Ingerslev, Yunhong Ding, Kjeld Dalgaard, Poul Kristensen, Michael Galili, Karsten Rottwitt, Siddharth Ramachandran, and Leif Katsuo Oxenløwe, Orbital Angular Momentum States Enabling Fiber-Based High-Dimensional Quantum Communication, Phys. Rev. Appl. **11**, 064058 (2019).

[31] Y. Zhou, M. Mirhosseini, S. Oliver, J. Zhao, S. M. H. Rafsanjani, M. P. J. Lavery, A. E. Willner, and R. W. Boyd, Using all transverse degrees of freedom in quantum communications based on a generic mode sorter, Opt. Express **27**, 10383 (2019).

[32] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, All-fiber self-compensating polarization encoder for quantum key distribution, Opt. Lett. **44**, 2398 (2019).

[33] Y.-P. Li, Wei Chen, Fang-Xiang Wang, Zhen-Qiang Yin, Li Zhang, Hang Liu, Shuang Wang, De-Yong He, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, Experimental realization of a reference-frame-independent decoy BB84 quantum key distribution based on Sagnac interferometer, Opt. Lett. **44**, 4523 (2019).

[34] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes, Phys. Rev. A **45**, 8185 (1992).

[35] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Sci. Technol. **4**, 035008 (2019).

[36] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient Time-Bin Encoding for Practical High-Dimensional Quantum Key Distribution, Phys. Rev. Appl. **14**, 014051 (2020).

[37] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[38] S. Wang, Wei Chen, Zhen-Qiang Yin, De-Yong He, Cong Hui, Peng-Lei Hao, Guan-Jie Fan-Yuan, Chao Wang, Li-Jun Zhang, Jie Kuang, Shu-Feng Liu, Zheng Zhou, Yong-Gang Wang, Guang-Can Guo, and Zheng-Fu Han, Practical gigahertz quantum key distribution robust against channel disturbance, Opt. Lett. **43**, 2030 (2018).

[39] F.-X. Wang, Weiqiang Wang, Rui Niu, Xinyu Wang, Chang-Ling Zou, Chun-Hua Dong, Brent E. Little, Sai T. Chu, Hang Liu, Penglei Hao, Shufeng Liu, Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wenfu Zhang, Wei Zhao, Zheng-Fu Han, Guang-Can Guo, and Wei Chen, Quantum key distribution with on-chip dissipative Kerr soliton, Laser Photon. Rev. **14**, 1900190 (2020).

[40] G. L. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution, Opt. Lett. **43**, 5110 (2018).

[41] D. Bacco, J. F. F. Bulmer, M. Erhard, M. Huber, and S. Paesani, Proposal for practical multidimensional quantum networks, Phys. Rev. A **104**, 52618 (2021).