Supplementary Materials for Experimental Demonstration of Long Distance Quantum Communication with Independent Heralded Single Photon Sources

Xiao-Hai Zhan,[1,2,3] Zhen-Qiu Zhong,[1,2,3] Jian-Yu Ma,[1,2,3]
Shuang Wang,[1,2,3,4,*] Zhen-Qiang Yin,[1,2,3,4] Wei Chen,[1,2,3,4]
De-Yong He,[1,2,3,4] Guang-Can Guo,[1,2,3,4] and Zheng-Fu Han[1,2,3,4]

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

[2]*Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, Hefei 230026, China*

[3]*CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

[4]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Dated: March 17, 2025)

I. SOURCE DESIGN

We design our source to be compatible with current commercial optical fiber network, therefore we aim at a single photon spectral bandwidth of 100 GHz, which is from the standard ITU DWDM spacing. For SPDC process, we choose type-II PPKTP to achieve high photon spectral purity. The joint spectral amplitude (JSA) can be given as

$$f(\omega_s,\omega_i) = \alpha(\omega_s+\omega_i)\Phi(\omega_s,\omega_i), \tag{1}$$

where $\alpha(\omega_s+\omega_i)$ stands for the pump spectrum and $\Phi(\omega_s,\omega_i)$ stands for the phase matching condition. Specifically, $\Phi(\omega_s,\omega_i) = \mathrm{sinc}(\Delta k L/2)$. Take the first order approximation, we get

$$\Delta k = (k_s'(\omega_{s0}) - k_p'(\omega_{p0}))\omega_s + (k_i'(\omega_{i0}) - k_p'(\omega_{p0}))\omega_i, \tag{2}$$

where k' stands for the first derivate of the wave vector k. For type-II PPKTP, we can calculate that $(k_s'(\omega_{s0}) - k_p'(\omega_{p0}))/(k_i'(\omega_{i0}) - k_p'(\omega_{p0})) = -1.144$ [1], suggesting that the phase matching condition mainly affects the anti-diagonal distribution of JSA, while the diagonal distribution is mainly determined by pump conditions. For a clearer analysis, we change the basis of JSA to the diagonal-anti-diagonal basis by letting

$$\begin{cases} \omega_+ &= \frac{1}{\sqrt{2}}\left(\omega_s+\omega_i\right) \\ \omega_- &= \frac{1}{\sqrt{2}}\left(\omega_s-\omega_i\right) \end{cases}, \tag{3}$$

then the pump amplitude becomes

$$\alpha(\omega_+,\omega_-) = \exp\left(-4\ln(2)\frac{\omega_+^2}{\Delta\omega_P^2}\right), \tag{4}$$

where $\Delta\omega_P$ is the FWHM of the pump angular frequency. Take the square of the modulus of the amplitude, we can find the FWHM of the JSI at the ω_+ direction is $\Delta\omega_+ = \Delta\omega_P\sqrt{2}$. For our DWDM, we measured a spectral bandwidth of $\Delta\lambda_{\mathrm{DWDM}} = 0.6\,\mathrm{nm}$. Then we can find the suitable spectral bandwidth for our pump pulse to be

$$\Delta\lambda_P = \frac{\sqrt{2}}{4}\Delta\lambda_{\mathrm{DWDM}} = 0.21\,\mathrm{nm}. \tag{5}$$

On the other hand, the phase matching condition becomes

$$\Phi(\omega_+,\omega_-) \approx \mathrm{sinc}\left[\left(k_i'-k_s'\right)\omega_- L/(2\sqrt{2})\right]. \tag{6}$$

* wshuang@ustc.edu.cn

We omit the ω_+ terms under the condition that $\frac{2k_p'-k_i'-k_s'}{k_i'-k_s'}=0.067\ll 1$. Then the suitable crystal length can be found to be $L=\frac{4\sqrt{2}x_0}{\Delta\omega_-\left|k_i'-k_s'\right|}$, where $x0=1.39$ is the first positive root for function $\mathrm{sinc}^2(x)-1/2$, and $\Delta\omega_-$ is the desired FWHM of JSI on the ω_- direction. Finally, we get

$$L=\frac{5.01\lambda_P^2}{c\left|k_i'-k_s'\right|\Delta\lambda_{\mathrm{DWDM}}}=56\,\mathrm{mm}. \tag{7}$$

We also numerically find the photon purity versus KTP crystal length, which is shown in Figure 1. The result shows that the photon purity reaches its maximum value of 0.97 at

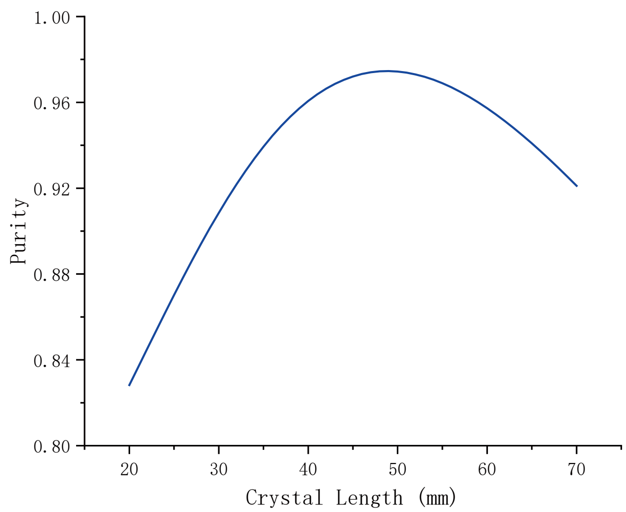

FIG. 1. The photon purity versus type-II PPKTP crystal length.

a crystal length of 49 mm, which aligns with our prediction in Equation 7. However, the maximum length is limited by manufacturing process to 30 mm. A theoretical value of 0.89 can be reached with this length, which is still high enough to perform HOM interference with high visibility. Using the spectrum we measured in Figure 6 in the main text, together with the phase matching condition of the 30 mm PPKTP, we can obtain the eigenvalues of the spectral modes by Schmidt decomposition. The largest three eigenvalues are calculated to be 0.95, 0.044 and 0.0019. This leads to a theoretical HOM visibility of 0.852 at an average photon number of 0.028. In our experiment, we measured a value of 0.845 ± 0.024, which fits well with the theoretical prediction.

II. HOM VISIBILITY WITH SPECTRALLY MULTIMODE EFFECT AND MULTIPHOTON EFFECT

It is known that HOM visibility is affected by single photon spectral purity and average photon numbers. On the one hand, one can obtain spectral modes by doing the Schmidt decomposition on the joint spectral amplitude of SPDC photon pairs. If the number of spectral modes is larger than 1, then the heralded single photon is spectrally impure, leading to decrease in HOM visibility. This is the spectrally multimode effect. On the other hand, there is a non-zero probability that one pump pulse generates more than one pair of photons, which also leads to decrease in HOM visibility. Here we give the quantitative formula for calculating HOM visibility considering these two effects. For detailed derivation, please refer to [2] for more details. Here we give the final results of the theoretical formula.

The visibility of HOM interference is defined with the four-fold coincidence probability $P_4(\tau)$, with τ being the optical delay between the two signal photons. Specifically,

$$V = \frac{P_4(\tau \to \infty) - P_4(\tau = 0)}{P_4(\tau \to \infty)}, \tag{8}$$

where

$$P_4(\tau = 0) = \sum_{\vec{m},\vec{n}=0}^{\infty} P_{\text{source}}(\vec{m},\vec{n}) \sum_{\vec{r}=0}^{\vec{m}+\vec{n}} P_{\text{detect}}(\vec{m},\vec{n},\vec{r}) \prod_{j=1}^{N} P^{0}_{\text{interfere}}(m_j, n_j, r_j), \tag{9}$$

$$P_4(\tau \to \infty) = \sum_{\vec{m},\vec{n}=0}^{\infty} P_{\text{source}}(\vec{m},\vec{n}) \sum_{\vec{s}=0}^{\vec{m}} \sum_{\vec{t}=0}^{\vec{n}} P_{\text{detect}}(\vec{m},\vec{n},\vec{s}+\vec{t}) \prod_{j=1}^{N} P^{\infty}_{\text{interfere}}(m_j, n_j, s_j, t_j), \tag{10}$$

$$\tag{11}$$

with

$$P_{\text{source}}(\vec{m},\vec{n}) = P_i\left(\sum_{j=1}^{N} m_j\right) P_i\left(\sum_{j=1}^{N} n_j\right) \prod_{j=1}^{N} \left[P_{\mu_j}(m_j) P_{\nu_j}(n_j)\right] \tag{12}$$

$$P_{\text{detect}}(\vec{m},\vec{n},\vec{r}) = P_s\left(\sum_{j=1}^{N} m_j + n_j - r_j\right) P_s\left(\sum_{j=1}^{N} r_j\right) \tag{13}$$

$$\begin{aligned} P^{0}_{\text{interfere}}(m_i, n_i, r_i) &= T^{m_i+r_i} R^{n_i-r_i} \frac{(m_i+n_i-r_i)!\,r_i!}{m_i!\,n_i!} \\ &= \left[\sum_{s_i=s_i^{\min}}^{s_i^{\max}} \binom{m_i}{s_i}\binom{n_i}{r_i-s_i} (-1)^{n_i+s_i-r_i} (R/T)^{s_i}\right]^2 \end{aligned} \tag{14}$$

$$P^{\infty}_{\text{interfere}}(m_j, n_j, s_j, t_j) = \binom{m_j}{s_j}\binom{n_j}{t_j} T^{m_j-s_j+t_j} R^{n_j+s_j-t_j}. \tag{15}$$

Here R and T are the reflectance and transmittance of the beam splitter. $P_s(n)$ and $P_i(n)$ are the single photon yield for an input n photon state of the signal and idler photon detectors, respectively. For threshold detectors with dark count rate d_s, d_i and detection efficiency η_s, η_i, we have

$$P_s(n) = 1 - (1 - d_s)(1 - \eta_s)^n \tag{16}$$
$$P_i(n) = 1 - (1 - d_i)(1 - \eta_i)^n.$$

Using parameters from Table I in the main text, we can get the theoretical values of visibility versus the average photon number. We can see that our experimental result fits well with the theoretical predictions (Figure 2).

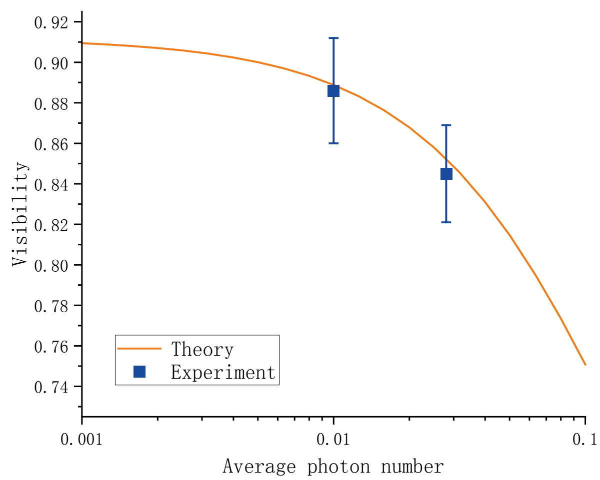

FIG. 2. The four-fold HOM visibility versus the average photon number. The error bars stand for one standard deviation, and is obtained through Monte-Carlo simulation.

III. MDI-QKD WITH THE PASSIVE DECOY STATE METHOD

Based on AYKI [3] and our work before [2], we develop the model of MDI-QKD with a multimode SPDC source using the passive decoy method. The system setup can be modeled with Figure 3. The source produces photon pairs with an average photon number of μ_0. The idler photon is detected locally with a total efficiency of η_I. Due to collecting, filtering and modulation losses, the signal photon is sent into the quantum channel at an average photon number of $\mu_S = \eta_S \mu_0$. The detectors at Charlie's side share a common efficiency of η_d, thus can be accumulated into the channel efficiency η. The dark count rate of the idler detectors and Charlie's detectors are d_I and d, respectively. The setup is the same at Bob's side.

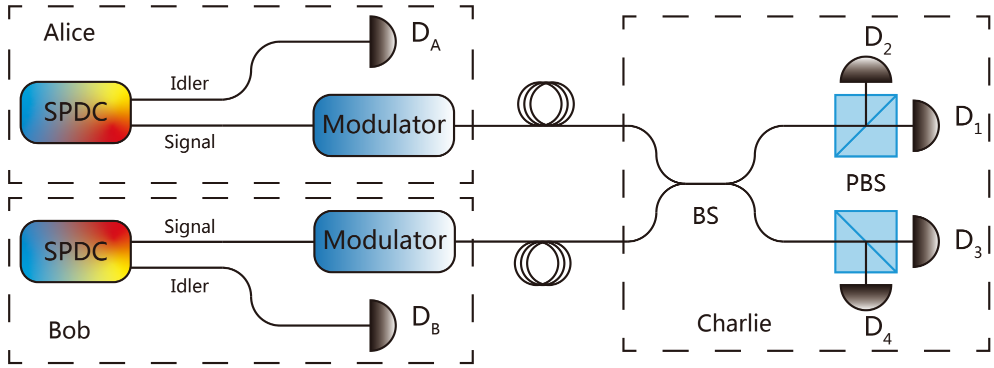

FIG. 3. The illustrated setup of the MDI-QKD with heralded single photons.

Considering the multimode effect of the SPDC sources, the HOM visibility degrades with the increase of the number of spectral modes. To get the final gain and error rate, the contribution of each mode needs to be considered. For detailed calculation, one can refer to [2]. Here we give out the equations we need in this work.

We use polarization coding in this work. Alice and Bob each randomly modulate their state into one of the four states $|H\rangle$, $|V\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ or $|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. H and V represents horizontal and vertical polarization, respectively. The untrusted third party Charlie performs a Bell state measurement on the received photons, and announces the clicking events of his detectors. The four detectors on Charlie's side is numbered from 1 to 4 as in Figure 3. According to [4], four of the two-fold clicks are defined as successful events, which is (1,2), (3,4), (1,4), (2,3) in our case. Based on the detector clicking events, either Alice or Bob does a bit flip on her or his bit except for the cases where they both sent a $|\pm\rangle$ state and the click events are (1,2) or (3,4). All the other events should be discarded, including single clicks and triple or quadruple clicks. The probability of obtaining a two-fold coincidence of detector (i, j) is then given by

$$q_{ij}^{\alpha\beta}(\mu,\nu) = \sum_{\vec{m},\vec{n}=0}^{\infty} f_{\mu_A}(\vec{m}) f_{\mu_B}(\vec{n}) P_{ij}^{\alpha\beta}(\vec{m},\vec{n}), \tag{17}$$

where $\alpha, \beta \in \{H, V, +, -\}$ represent the polarization states. In Equation 17, μ_A and μ_B represent the total average photon numbers sent by Alice and Bob, respectively. To simplify the denotations for spectral multimode, we use vector-like characters to represent the lists of multimode variables. For example, the photon number of each spectral mode that Alice sent is $m_1, m_2, ..., m_N$, and we denote this list as $\vec{m}$, N is the number of spectral modes. $f_\mu(\vec{m})$ is the photon number distribution (PND) after the transmission loss. $P_{ij}^{\alpha\beta}$ is the probability of two-fold coincidence rate of detector (i,j), conditioned on the input photons of the beam splitter having $m_1, m_2, ..., m_N$ photons from Alice with polarization α, and $n_1, n_2, ..., n_N$ photons from Bob with polarization β. Explicitly,

$$
\begin{aligned}
P_{12}^{HH} &= P_{34}^{HH} = P_{14}^{HH} = P_{23}^{HH} = P_{12}^{VV} = P_{34}^{VV} = P_{14}^{VV} = P_{23}^{VV} \\
&= \left(\frac{1}{2}\right)^{\sum_{i=1}^{N}(m_i+n_i)} P_{d_S}\left(\sum_{i=1}^{N}(m_i+n_i), 0\right) \prod_{i=1}^{N} \frac{(m_i+n_i)!}{m_i!n_i!} \\
P_{12}^{HV} &= P_{34}^{HV} = P_{14}^{HV} = P_{23}^{HV} = P_{12}^{VH} = P_{34}^{VH} = P_{14}^{VH} = P_{23}^{VH} \\
&= \left(\frac{1}{2}\right)^{\sum_{i=1}^{N}(m_i+n_i)} P_{d_S}\left(\sum_{i=1}^{N} m_i, \sum_{i=1}^{N} n_i\right), \\
P_{12}^{+-} &= P_{34}^{+-} = P_{14}^{++} = P_{23}^{++} = P_{12}^{-+} = P_{34}^{-+} = P_{14}^{--} = P_{23}^{--} \\
&= \left(\frac{1}{4}\right)^{\sum_{i=1}^{N}(m_i+n_i)} \sum_{\vec{r}=0}^{\vec{m}+\vec{n}} \left[\prod_{i=1}^{N} \frac{(m_i+n_i-r_i)!r_i!}{m_i!n_i!} \left|\xi^{(-)}(m_i,n_i,r_i)\right|^2\right] \\
&\times P_{d_S}\left(\sum_{i=1}^{N}(m_i+n_i-r_i), \sum_{i=1}^{N} r_i\right) \\
P_{12}^{++} &= P_{34}^{++} = P_{14}^{+-} = P_{23}^{+-} = P_{12}^{--} = P_{34}^{--} = P_{14}^{-+} = P_{23}^{-+} \\
&= \left(\frac{1}{4}\right)^{\sum_{i=1}^{N}(m_i+n_i)} \sum_{\vec{r}=0}^{\vec{m}+\vec{n}} \left[\prod_{i=1}^{N} \frac{(m_i+n_i-r_i)!r_i!}{m_i!n_i!} \left|\xi^{(+)}(m_i,n_i,r_i)\right|^2\right] \\
&\times P_{d_S}\left(\sum_{i=1}^{N}(m_i+n_i-r_i), \sum_{i=1}^{N} r_i\right),
\end{aligned}
$$

where

$$
P_{d_S}(n_1,n_2) = \begin{cases} d^2(1-d)^2 & n_1+n_2=0 \\ d(1-d)^2 & n_1 n_2 = 0 \\ (1-d)^2 & n_1 n_2 > 0 \end{cases}, \tag{18}
$$

and

$$
\xi^{(\pm)}(m_i,n_i,r_i) = \sum_{s_i=\max\{0,r_i-n_i\}}^{\min\{r_i,m_i\}} \binom{m_i}{s_i}\binom{n_i}{r_i-s_i}(\pm1)^{r_i-s_i}. \tag{19}
$$

For passive decoy-state method, the photon number distribution is determined by triggering. Denote μ and ν the average photon number of the triggered and non-triggered events, respectively. It can be calculated that

$$f_\nu(\vec{m}) = (1-d_I)(1-\eta_I)^{\sum_{i=1}^N m_i} \prod_{i=1}^{N} \frac{(\eta_S \mu_i)^{m_i}}{[1+(\eta_I+\eta_S-\eta_I\eta_S)\mu_i]^{1+m_i}}, \tag{20}$$

$$f_\mu(\vec{m}) = \prod_{i=1}^{N} \frac{(\eta_S \mu_i)^{m_i}}{(1+\eta_S\mu_i)^{1+m_i}} - f_\nu(\vec{m}), \tag{21}$$

$$\tag{22}$$

where d_I is the dark count rate of the local detector, η_I is the detection efficiency of the idler photon, η_S is the transmission efficiency of the signal photon before entering the quantum channel.

Due to the imperfections of realistic devices, there is a small probability e_d that a photon is detected to be in its orthogonal state. For example, a limited extinction ratio of the polarization beam splitter on Charlie's side would leave a small chance of letting a H photon be reflected to the V detector. Thus, we divide the total gain into two parts for each selected basis, which is

$$\begin{aligned}
Q_{\mu,\nu}^{Z,C} &= \frac{1}{4}\left[q_{12}^{HV}+q_{34}^{HV}+q_{14}^{HV}+q_{23}^{HV}+q_{12}^{VH}+q_{34}^{VH}+q_{14}^{VH}+q_{23}^{VH}\right] \\
Q_{\mu,\nu}^{Z,E} &= \frac{1}{4}\left[q_{12}^{HH}+q_{34}^{HH}+q_{14}^{VV}+q_{23}^{VV}+q_{12}^{VV}+q_{34}^{VV}+q_{14}^{HH}+q_{23}^{HH}\right] \\
Q_{\mu,\nu}^{X,C} &= \frac{1}{4}\left[q_{12}^{++}+q_{34}^{++}+q_{14}^{+-}+q_{23}^{+-}+q_{12}^{--}+q_{34}^{--}+q_{14}^{-+}+q_{23}^{-+}\right] \\
Q_{\mu,\nu}^{X,E} &= \frac{1}{4}\left[q_{12}^{+-}+q_{34}^{+-}+q_{14}^{++}+q_{23}^{++}+q_{12}^{-+}+q_{34}^{-+}+q_{14}^{--}+q_{23}^{--}\right].
\end{aligned} \tag{23}$$

Here Z and X are the two mutually unbiased bases, where Z basis includes rectilinear polarization states $|H\rangle$ and $|V\rangle$ and X basis includes diagonal polarization states $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ [4]. The superscript C represents the correct response and E represents errors. Then the averaged total gain and error rate can be calculated through

$$\begin{aligned}
Q_{\mu,\nu}^{Z} &= Q_{\mu,\nu}^{Z,C} + Q_{\mu,\nu}^{Z,E} \\
E_{\mu,\nu}^{Z} Q_{\mu,\nu}^{Z} &= e_d Q_{\mu,\nu}^{Z,C} + (1-e_d) Q_{\mu,\nu}^{Z,E},
\end{aligned} \tag{24}$$

similar for X basis.

For the analysis of statistical fluctuations, we use the method as in [5]. By dividing the pulses into two groups based on the heralding result, we get two groups of events with different effective intensities passively. We use the yields and error rate of the events at X basis of both of these intensities to estimate the lower bound of Y_{11} and upper bound of e_{11}.

We denote the average photon number of the pulses when the idler detector clicks as μ and that not clicks with ν, such that $\mu > \nu > 0$. Then

$$Y_{11}^L(\mathcal{H}) = \frac{P_\mu^1 P_\mu^2 Q_{\nu\nu}^{X,L} - P_\nu^1 P_\nu^2 Q_{\mu\mu}^{X,U} - P_\mu^1 P_\mu^2 \mathcal{H}}{P_\mu^1 P_\nu^1 (P_\mu^2 P_\nu^1 - P_\nu^2 P_\mu^1)} \tag{25}$$

$$e_{11}^U(\mathcal{H}) = \frac{T_{\nu\nu}^{X,U} - \frac{1}{2}\mathcal{H}}{(P_\nu^1)^2 Y_{11}^L(\mathcal{H})},$$

where $\mathcal{H} = P_\nu^0 P_\nu^0 Y_{00} + \sum_{m=1}^{\infty} P_\nu^0 P_\nu^m (Y_{0m} + Y_{m0})$. The bound can be found by $e_{11}^U(\mathcal{H}) > 0$, thus $\mathcal{H} \in [0, 2T_{\nu\nu}^{X,U}]$. The lower bound and upper bound of $\xi_{x,y}$ can be found to be $\xi_{x,y}^L = \xi_{x,y} - \gamma\sqrt{\xi_{x,y}/N_{x,y}}$ and $\xi_{x,y}^U = \xi_{x,y} + \gamma\sqrt{\xi_{x,y}/N_{x,y}}$, where $\xi \in \{Q, T\}$. $\gamma = 5.3$, corresponding to a failure probability of $\varepsilon = 10^{-7}$. The final key rate is given by

$$R(\mathcal{H}) = (p_Z)^2 \left\{(P_\mu^1)^2) Y_{11}^L(\mathcal{H}) \left[1 - H_2\left(e_{11}^U(\mathcal{H})\right)\right] - f Q_{\mu\mu}^Z H_2(E_{\mu\mu}^Z)\right\}. \tag{26}$$

The secure key rate is obtained by minimizing the above expression

$$R_{\text{secure}} = \min_{\mathcal{H}} R(\mathcal{H}). \tag{27}$$

IV. POLARIZATION STATE MODULATOR

The polarization state modulator in this demonstration experiment consists of four wave plates. The goal of this setup is to modulate out the four BB84 polarization states explicitly, which is $|H\rangle$, $|V\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ or $|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. The four wave plates are placed in the order of HWP1, QWP1, HWP2, QWP2. The input polarization state is linearly polarized, so the function of HWP1 is to rotate the polarization state into any other state in the XZ plane on the Bloch sphere surface. However, due to the transformation of the polarization state in the fiber channel, the extra phase between the H and V component needs to be compensated.

As illustrated in Figure 4, let the angle between the fast axis of the wave plates and the horizontal plane to be θ, then the Jones matrices for the HWP and QWP is (ignoring global phases)

$$H(\theta) = \begin{pmatrix} \cos^2(\theta) - \sin^2(\theta) & 2\sin(\theta)\cos(\theta) \\ 2\sin(\theta)\cos(\theta) & \sin^2(\theta) - \cos^2(\theta) \end{pmatrix} \tag{28}$$

and

$$Q(\theta) = \begin{pmatrix} \cos^2(\theta) + i\sin^2(\theta) & (1-i)\sin(\theta)\cos(\theta) \\ (1-i)\sin(\theta)\cos(\theta) & \sin^2(\theta) + i\cos^2(\theta) \end{pmatrix}. \tag{29}$$

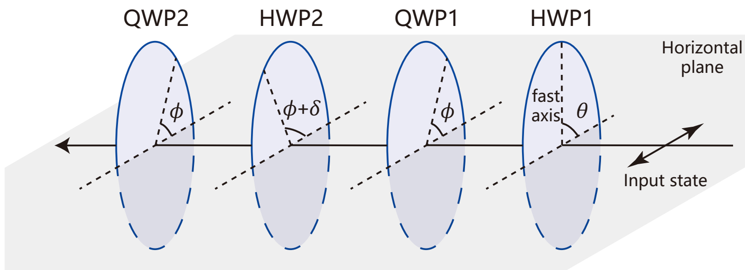

FIG. 4. The illustration of polarization state modulation setup.

Let the two QWPs have the same angle set at ϕ and the HWP set with an angle offset of δ, then the transformation becomes

$$Q_2(\phi)H_2(\phi+\delta)Q_1(\phi) = \begin{pmatrix} \cos(2\delta) - i\sin(2\delta)\sin(2\phi) & i\sin(2\delta)\cos(2\phi) \\ i\sin(2\delta)\cos(2\phi) & \cos(2\delta) + i\sin(2\delta)\sin(2\phi) \end{pmatrix}. \tag{30}$$

Now if we set $\phi = \pi/4$, then the transformation can be simplified to

$$Q_2\left(\frac{\pi}{4}\right) H_2\left(\frac{\pi}{4}+\delta\right) Q_1\left(\frac{\pi}{4}\right) = \begin{pmatrix} e^{-2i\delta} & 0 \\ 0 & e^{2i\delta} \end{pmatrix}. \tag{31}$$

Then an extra relative phase of 4δ is applied to the H and V component, which can be controlled by simply rotating the angle of the HWP2. More generally, as long as the two QWPs align with each other by their fast axes, an extra phase can be explicitly added to the two components with designed axis. One can verify that

$$R(-\phi)\, Q_2\left(\phi+\frac{\pi}{4}\right) H_2\left(\phi+\frac{\pi}{4}+\delta\right) Q_1\left(\phi+\frac{\pi}{4}\right) R(\phi) = \begin{pmatrix} e^{-2i\delta} & 0 \\ 0 & e^{2i\delta} \end{pmatrix} \tag{32}$$

returns the same result, where

$$R(\phi) = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix} \tag{33}$$

is the rotation matrix, which does the function of rotating the reference frame here.

V. LOSS DUE TO DETECTION DEAD TIME

For QKD system using local detection for classifying decoy states, the pulses that are sent during the dead time of local detectors should be treated carefully.

First let us look into the average photon number of the classified events using detector triggering. It is perceptible that the average photon number of the triggered events are larger than the generated average photon number from the source. Here we prove this claim. Let the photon number distribution of the generated photon pairs is $P_G(n)$, then the average photon number is defined to be

$$\mu_G = \sum_{n=0}^{\infty} n P_G(n), \tag{34}$$

that $P_G(n)$ satisfies the normalization condition

$$\sum_{n=0}^{\infty} P_G(n) = 1. \tag{35}$$

After triggering, the average photon number can be defined as

$$\mu_T = \sum_{n=0}^{\infty} n P_T(n) P_G(n), \tag{36}$$

where $P_T(n)$ is the triggering coefficient that also satisfies the normalization condition

$$\sum_{n=0}^{\infty} P_T(n) P_G(n) = 1. \tag{37}$$

We consider a threshold single photon detector, which is expected that the response rate increase monotonically with the incident photon number n. Therefore, we have

$$P_T(n+1) > P_T(n) > 0, \tag{38}$$

for every $n \geq 0$. From 37, it is obvious that there exists a positive integer M, such that

$$0 < P_T(n \leq M) \leq 1 < P_T(n > M). \tag{39}$$

Take the subtraction of 37 and 35, we have

$$\sum_{n=M+1}^{\infty} \left[P_T(n) - 1\right] P_G(n) - \sum_{n=0}^{M} \left[1 - P_T(n)\right] P_G(n) = 0. \tag{40}$$

Notice that the coefficients before $P_G(n)$ are all positive, then it can be found that

$$\begin{aligned} 0 &= M \sum_{n=M+1}^{\infty} \left[P_T(n) - 1\right] P_G(n) - M \sum_{n=0}^{M} \left[1 - P_T(n)\right] P_G(n) \\ &< \sum_{n=M+1}^{\infty} n \left[P_T(n) - 1\right] P_G(n) - \sum_{n=0}^{M} n \left[1 - P_T(n)\right] P_G(n). \end{aligned} \tag{41}$$

This gives

$$\sum_{n=0}^{\infty} nP_T(n)P_G(n) > \sum_{n=0}^{\infty} nP_G(n), \tag{42}$$

which is exactly

$$\mu_T > \mu_0. \tag{43}$$

Similarly, the non-triggered events must have an average photon number of $\mu_N < \mu_G$.

During the dead time of the single photon detectors, the pulses that arrive at the detector can never cause a triggering event, no matter how much is the incident photon number. Therefore, the average photon number during the detector dead time is $\mu_D = \mu_G > \mu_N$. If one does not discriminate these events from the non-triggered events, then pulses with a larger average photon number is sent during the dead times, which might be attacked by potential eavesdroppers with photon-number-splitting attacks. Thus, it is necessary to either discard the pulses that come during the detection dead time, or label them with the generated average photon number μ_G. In our experiment, we discard these pulses for an easier treatment. However, for experiments with a higher repetition rate or a larger detector dead time, it is more efficient to keep these pulses.

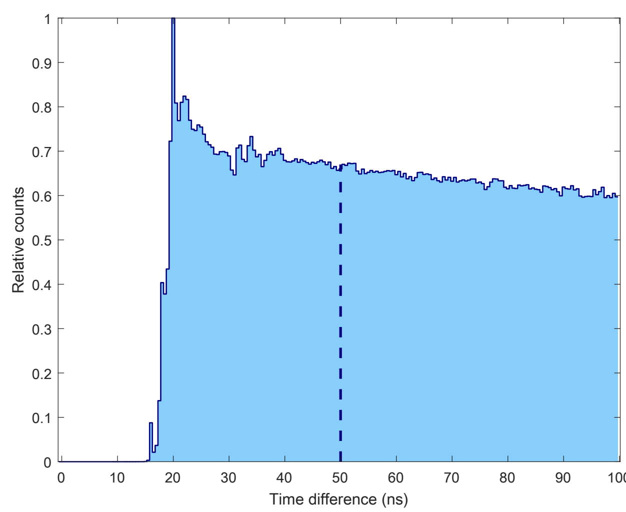

FIG. 5. Detection dead time test. The time differences of consecutive signals within the same start period are plotted in the histogram. The non-zero start point shows the dead time effect of the detection system.

To determine the dead time of our system, we injected continuous wave light into the Scontel SNSPD and recorded signals using an Agilent TDC (TC890). The time differences between consecutive signals were calculated and plotted in a histogram, as shown in Figure 5. Due to very slight variations across channels, we present results from one representative channel. Given that we only consider signals within the same start signal period (with a frequency of 1 MHz for the TDC in our experiment), detected counts are expected to degrade gradually as time differences increase. In an ideal detection module with zero dead time, the count distribution would initiate at zero time difference. However, due to the presence of dead time, the count distribution begins at a non-zero point.

The analysis reveals that the overall detection system exhibits a dead time of approximately 20 ns. However, stability in results is achieved only after 40 ns, necessitating a conservative estimate. To ensure safety and accuracy in post-processing, we set the dead time to 50 ns.

To quantitatively describe detection loss caused by dead time, we developed a theoretical model for threshold detectors. For detailed derivation, one can refer to the appendix in our previous work [6]. Here we give the theoretical formula

$$F_{\text{eff}} = F_0 \times \eta_{\text{dead}} = \frac{F_0}{1 + (1 - \exp(-\eta\mu)) \times \text{floor}(t_{\text{dead}} F_0)}, \tag{44}$$

where F_{eff} represents the effective repetition rate accounting for dead time effects, and F_0 is the original repetition rate. η denotes detection efficiency, while μ indicates the average photon number entering the detector. The function floor(x) stands for rounding the number x down to the nearest integer less than or equal to it.

Note that Equation 44 is based on Poissonian distribution, while in our experiment the photon number distribution is more close to thermal distribution. However, since we operate under the condition that $\mu \ll 1$, the variation in the results are quite slight. Finally, considered that valid communication occurs only when both Alice's and Bob's detectors have recovered from the dead time state, the total efficiency requires squaring. Set F_0=99.73 MHz, η=0.51, μ=0.028 and t_{dead}=50 ns, this yields a final efficiency of $\eta'_{\text{dead}} = \eta^2_{\text{dead}}$=0.90.

VI. GAIN AND ERROR RATE

In Table I, we give the detailed gain and error rate of the MDI-QKD process. N_{total} is the total number of pulses that is sent according to the protocol. Note that $1 - \eta_{\text{dead}} = 0.10$ of total pulses are discarded due to the dead time of local detectors. Thus, the gain Q are calculated under an effective total number of pulses of $\eta_{\text{dead}}N_{\text{total}}$.

N_{total}		10^{12}			10^{13}		
Fiber length (km)		0	20	50	0	20	50
p_X		0.41	0.58	0.83	0.21	0.30	0.44
Z basis	$Q_{\mu\mu}$	1.812×10^{-6}	5.362×10^{-7}	1.823×10^{-7}	1.808×10^{-6}	5.319×10^{-7}	1.861×10^{-7}
	$Q_{\nu\nu}$	1.550×10^{-6}	5.440×10^{-7}	2.121×10^{-7}	1.513×10^{-6}	5.414×10^{-7}	2.070×10^{-7}
	$E_{\mu\mu}$	0.04387%	0.09516%	0.3375%	0.04794%	0.08402%	0.1864%
	$E_{\nu\nu}$	0.4317%	0.6947%	1.940%	0.4768%	0.6824%	1.674%
X basis	$Q_{\mu\mu}$	1.977×10^{-6}	5.761×10^{-7}	1.895×10^{-7}	1.974×10^{-6}	5.738×10^{-7}	1.842×10^{-7}
	$Q_{\nu\nu}$	5.144×10^{-6}	1.554×10^{-6}	5.619×10^{-7}	5.154×10^{-6}	1.547×10^{-6}	5.540×10^{-7}
	$E_{\mu\mu}$	9.303%	9.644%	11.08%	9.983%	9.903%	12.02%
	$E_{\nu\nu}$	37.59%	36.75%	37.33%	37.82%	36.87%	37.68%
Key rate per pulse		1.695×10^{-7}	2.074×10^{-8}	4.147×10^{-10}	5.141×10^{-7}	1.269×10^{-7}	1.893×10^{-8}

TABLE I. Gain and error rate upon transmission of 0 km, 20 km and 50 km fiber channel with 10^{12} and 10^{13} total number of pulses.

To show the stability of our running system, we plot the calculated error rate over time. The data is plot in Figure 6. In our demonstration experiment, we gather the data for each combination of sent states separately. Then the error rate is calculated according to 23. Each data point is accumulated for 1 minute. There are four possible valid combinations for each basis, i.e. HH, HV, VH, VV for Z basis and $++$, $+-$, $-+$, $--$ for X basis, therefore the total amount of time used for each distance is 4 times of the horizontal axis in the plot. One can see that for the whole running process, the error rate oscillates in a reasonable range, showing the long term stability of our system.

[1] K. Kato and E. Takaoka, Sellmeier and thermo-optic dispersion formulas for KTP, Applied Optics **41**, 5040 (2002).

[2] X.-H. Zhan, Z.-Q. Zhong, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Measurement-Device-Independent Quantum Key Distribution with Practical Spontaneous Parametric Down-Conversion Sources, Physical Review Applied **20**, 034069 (2023).

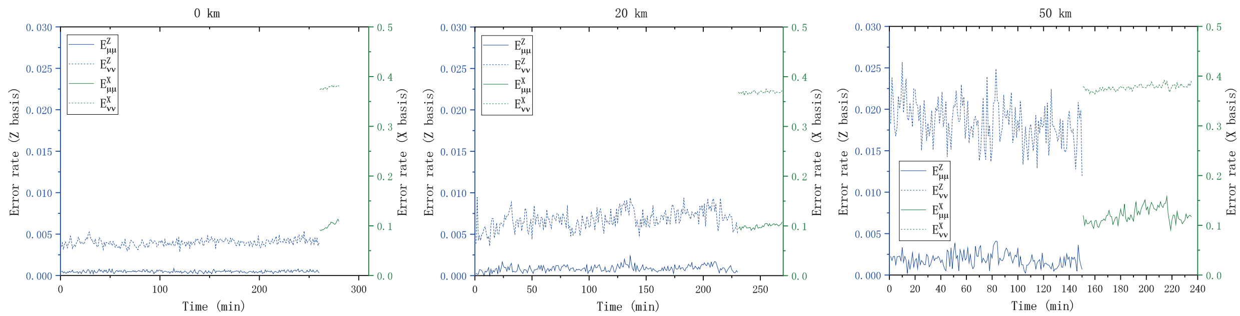

FIG. 6. Error rate over time. See text for details.

[3] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion, Physical Review Letters **99**, 180503 (2007).

[4] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Physical Review Letters **108**, 130503 (2012).

[5] X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Efficient measurement-device-independent quantum key distribution without vacuum sources, Physical Review A **98**, 032303 (2018).

[6] X.-H. Zhan, S. Wang, Z.-Q. Zhong, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Quantum Key Distribution with a Continuous-Wave-Pumped Spontaneous-Parametric-Down-Conversion Heralded Single-Photon Source, Physical Review Applied **19**, 034027 (2023).