Received 27 April 2022; revised 24 January 2023; accepted 10 March 2023; date of publication 20 March 2023; date of current version 4 April 2023.

Digital Object Identifier 10.1109/TQE.2023.3259043

Analysis of the Effects of the Two-Photon Temporal Distinguishability on Measurement-Device-Independent Quantum Key Distribution

HAOBO GE[1], AKIHISA TOMITA[1], ATSUSHI OKAMOTO[1], AND KAZUHISA OGAWA[2]

[1]Hokkaido University, Sapporo 060-0808, Japan
[2]Osaka University, Osaka 565-0871, Japan

Corresponding author: Akihisa Tomita (e-mail: tomita@ist.hokudai.ac.jp).

This work was supported in part by SIP on Photonics and Quantum Technology for Society 5.0 (Cabinet Office, Government of Japan), in part by the Japan Society for the Promotion of Science KAKENHI under Grant 18H05237, and in part by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) Doctoral program for Data-Related InnoVation Expert Hokkaido University (D-DRIVE-HU) program.

ABSTRACT Measurement-device-independent quantum key distribution (MDI-QKD) protects legitimate users from attacks on measurement devices. The decoy method allows for unconditionally secure quantum key generation using lasers. One of the most important issues in MDI-QKD is that photons from two independent lasers must be indistinguishable. Because Alice and Bob send Charlie laser pulses through separate fiber links, the arrival times of the pulses fluctuate independently. According to the Hong-Ou-Mandel (HOM) interference at Charlie's relay, the time delay between two photons has the greatest effect on distinguishability. However, to date, these effects have not been analyzed. Our study uses simulations to investigate the effects of two-photon temporal distinguishability in terms of the visibility of the HOM-dip of two photons on the final key rate of finite-size MDI-QKD. Furthermore, an acceptable time delay range was estimated based on photons with Gaussian spectral amplitude functions.

INDEX TERMS Decoy method, Hong-Ou-Mandel (HOM) interference, measurement-device-independent quantum key distribution (MDI-QKD), time delay.

I. INTRODUCTION

The security of current cryptography is seriously threatened by the rapid development of computer power and algorithms. Fortunately, quantum key distribution (QKD) allows two distant and independent parties, Alice and Bob, to share a security key even under the eavesdropping of Eve and ensures that it is theoretically unconditionally secure. Since the BB84 protocol was proposed by Bennet and Brassard in 1984 [1], QKD has attracted significant attention and has made great progress in theory and implementation [2]. However, actual QKD systems may have various security loopholes owing to inevitable system errors and equipment defects. Several side-channel attack schemes that utilize these defects have also been proposed. For example, detection efficiency mismatching attacks [3] and time-shift attacks [4] exploit the imperfections of the detectors, and photon number splitting (PNS) attacks [5] exploit the imperfection of the light source.

Several approaches have been proposed to address side-channel attacks [6]. One is to fully analyze and describe the characteristics of all devices and build a mathematical model for ensuring security. This is ideal in theory but difficult to implement in practice. The second is to establish a device-independent QKD (DI-QKD) system, as proposed by Acin et al. [7]. The advantage of this approach is that the unconditional security of a QKD system can be proved based on Bell's inequality without knowledge of the details of the system. However, this scheme requires the single-photon detection efficiency to be close to 100%, which is difficult to achieve with current technology, and its key rate is relatively low.

In between the two approaches above, Lo et al. [6] proposed measurement-device-independent QKD (MDI-QKD) in 2012, which is more practical and feasible than DI-QKD. In this scheme, Alice and Bob send signals to a third untrusted party, Charlie, that can even be controlled by Eve. Charlie performs a Bell state measurement (BSM) and announces the results. Alice and Bob can distill the secret key from public information as long as they ensure that their sources are secret and provide near-perfect state preparation. The security of MDI-QKD does not rely on the performance of detectors; therefore, it can be immune to detector-side channel attacks. In fact, because MDI-QKD is based on a time-reversal EPR protocol [8], [9], the security of MDI-QKD can be proved by the idea of time reversal.

In contrast, as with the BB84 protocol, the source for the ideal MDI-QKD system is a single-photon source, which is still not available with current technology. Weak coherent state sources (WCS) or spontaneous-parametric-down conversion sources are usually used to generate effective single-photon pulses instead of single-photon sources. Therefore, the decoy-state method [10], [11], [12] must be adopted to ensure unconditional security from a PNS attack [5]. The work in [13], [14], and [15] analyzed decoy-state MDI-QKD with an infinite key length, and the decoy-state MDI-QKD of a finite key length with statistical fluctuation was also analyzed [15], [16], [17], [18], [19], [20], [21]. The work in [20], [21], and [22] proposed more the efficient four-intensity with joint constraints for statistical fluctuation protocol. The MDI-QKD protocol has been successfully implemented in the laboratories and field [23], [24], [25], [26], [27], [28] Recently, continuous variable MDI-QKD [29] has also been demonstrated.

According to Lo et al. [6], it is critical for the photons emitted by two independent lasers to be indistinguishable. Since MDI-QKD protocol is based on the photon bunching effect of two indistinguishable photons at a 50:50 beam splitter (BS), stable HOM interference [30], [31] should be observed. The validity of the HOM test was probed in principle. However, it is unclear how the imperfect HOM interference affects the security of a practical system. The relationship between the visibility of the HOM interference and the final key rate must be clarified, and methods that improve visibility must be established. Thus far, a few studies have explored this issue, with exceptions including the study by Curty et al. [18], which calculated only the effect of misalignment error in the limit of zero distance.

The effects of imperfect visibility become serious for long distance transmission, because the fiber channel is exposed to perturbations in practical conditions. Precise control of the channel would be necessary to compensate the perturbation. However, the precise control may raise the cost for implementation. It is important to determine the target of the precision to maintain the final key rate in practice.

In this article, we explored the acceptable indistinguishability of the MDI-QKD. We calculated the key generation rate of a three-intensity decoy-state MDI-QKD protocol with a finite key length. Then, we calculated the effect of the visibility of the two-photon interference on the key generation rate. Finally, we calculated the acceptable time delay of the two Gaussian pulses at a 50:50 BS. Our numerical simulations show that high-visibility HOM-dip requires sophisticated time measurement devices.

II. EFFECT OF TWO-PHOTON TEMPORAL DISTINGUISHABILITY

We use a symmetric protocol with three intensities to each basis as shown in Appendix. The final key rate can be estimated by Alice and Bob [13], [14], [15]:

$$R \geq p_{\mu_2} p_{\nu_2} p^{z}_{\mu_2} p^{z}_{\nu_2} \left\{ \mu_2 \nu_2 e^{-\mu_2-\nu_2} s^{z}_{11} \left[1 - H\left(e^{x}_{11}\right)\right] - S^{z}_{\mu_2\nu_2} f H\left(E^{z}_{\mu_2\nu_2}\right) \right\} \tag{1}$$

where $S^{\omega}_{\mu_i\nu_j} = n^{\omega}_{\mu_i\nu_j}/N^{\omega}_{\mu_i\nu_j}$ is the counting rate of the pulse pairs of intensity $\mu_i\nu_j$ in basis ω, f is the error correction inefficiency and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. The probability that Alice (Bob) chooses intensity $\mu_i(\nu_j)$ is $p_{\mu_i}(p_{\nu_j})$ and the probability that Alice (Bob) chooses basis ω is $p^{\omega}_{\mu_i}(p^{\omega}_{\nu_j})$. The yield s^{z}_{11} and phase error rate e^{x}_{11} on z-basis are defined for the pulses when Alice and Bob send those containing a single photon. The detail of decoy method is given in Appendix. The other parameters are also defined.

Our model can be considered a photon-number channel model when the phase of pulses is fully randomized [14], and the overall counting rate and error rate on the x basis and z basis are shown as [14], [15]

$$\begin{aligned} S^{x}_{\mu_i\nu_j} &= 2y^2\left[1 + 2y^2 - 4yI_0(s) + I_0(2s)\right] \\ S^{x}_{\mu_i\nu_j}E^{x}_{\mu_i\nu_j} &= e_0 S^{x}_{\mu_i\nu_j} - 2(e_0 - e_d)y^2\left[I_0(2s) - 1\right] \\ S^{z}_{\mu_i\nu_j} &= S_C + S_E \\ S^{z}_{\mu_i\nu_j}E^{z}_{\mu_i\nu_j} &= e_d S_C + (1 - e_d) S_E \end{aligned} \tag{2}$$

where

$$\begin{aligned} S_C &= 2(1-p_d)^2 e^{-\mu'/2}\left[1 - (1-p_d)e^{-\eta_a\mu_i/2}\right] \\ &\quad \times \left[1 - (1-p_d)e^{-\eta_b\nu_j}/2\right] \\ S_E &= 2p_d(1-p_d)^2 e^{-\mu'/2}\left[I_0(2s) - (1-p_d)e^{-\mu'/2}\right]. \end{aligned} \tag{3}$$

In (2) and (3), $I_0(s)$ is the modified Bessel function of the first kind, p_d is the dark count rate of the photon detector, e_0 is the error rate of the background, and e_d is the error rate due to two-photon distinguishability. The transmittance from Alice or Bob to Charlie is given by $\eta_a = \eta_b = \eta_d 10^{-\alpha l/20}$, where α is the loss coefficient of the standard fiber link, η_d is the detection efficiency, and l is the total distance between Alice and Bob. The other parameters are given by [13], [14], [15]

$$\begin{aligned} \mu' &= \eta_a\mu_i + \eta_b\nu_j \\ s &= \sqrt{\eta_a\mu_i\eta_b\nu_j}/2 \\ y &= (1-p_d)e^{-\mu'/4}. \end{aligned} \tag{4}$$

Then, we focus on the error rate e_d, which is directly related to the visibility of the two-photon interference, and it can be written as

$$e_d = e_d^0 + \frac{1-V}{2} \tag{5}$$

where e_d^0 is the correction parameter and is assumed to be 0. The quantum bit error rate (QBER) in x basis can be related to the visibility with (2) and (5).

Notice that according to different BSM implementation methods adopted by different protocols, the error rates for x- and z-basis are also different. When polarization-encoding protocol is adopted, BSM with a BS followed by polarization beam splitters (PBSs) is considered successful when photons are detected at different ports of the PBS. The success probability of BSM is 1/2. Suppose photons are distinguishable. In z-basis, BSM succeeds when Alice and Bob send different polarization. Although Ψ^+ may be mistaken for Ψ^-, bits are flipped for both Ψ^+ and Ψ^- outcomes, so there is no bit error. In x-basis, even if Alice and Bob send same polarization, photons may be detected at different ports of the PBS to cause error with the probability of 1/2. On the other hand, the BSM with only a BS is successful, when it detects Ψ^-, that is, the photons are detected on the different ports of the BS. It happens with the probability of 1/2 regardless of the polarization. Therefore, the error rate is 1/2 for both bases. If it is a complete BSM, the probability of success is unity, but both x- and z-basis will have errors with the probability of 1/2. As a result, the BS+PBS method seems to be practical in terms of the asymmetry of error rate. In this case, e_d should have no effect on z-basis in the error rate calculation in (2).

The error rate is related to the HOM interference visibility as follows. We can model the photon-pair state as a mixture of perfectly indistinguishable photons and the completely independent photons with the fraction of $1-\varepsilon$ and ε, respectively. The two-photon interference in the BSM on the indistinguishable photons provides only two possible outcomes with probability of 1/2, whereas it provides all four outcomes with the probability of 1/4 for the independent photons. For example, if both Alice and Bob send x_0, the BSM fails with BS+PBS implementation for the indistinguishable photons, however, the outcomes Ψ^+ or Ψ^- may appear for the independent photons with each probability of 1/4. Therefore, the error rate in the BSM on the mixture will read $\varepsilon/2$. Since the visibility of the HOM interference of the mixture is reduced to $V = 1-\varepsilon$, we obtain the error rate given in (5). If Alice and Bob send the other photon-pair states, the same error rate is obtained. If there is no eavesdropper on the channel, the phase error rate e_{11}^x coincides with the background error rate e_d. Fig. 1 shows the relationship between the visibility and phase error rate.

The visibility of the two-photon interference V can be directly estimated from the coincidence probability in the HOM interference experiment by

$$V = \frac{p_{\max} - p_{\min}}{p_{\max}} \tag{6}$$

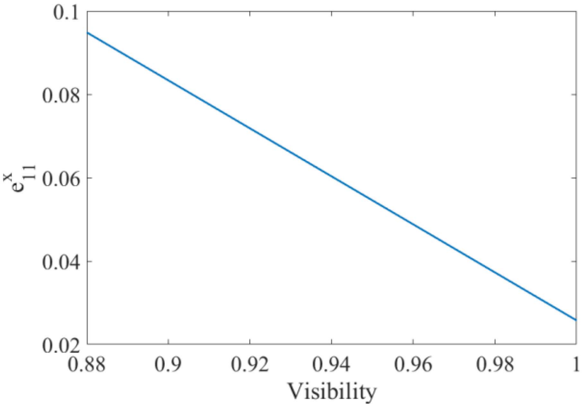

FIGURE 1. Relationship between error rate of single photon pairs e_{11}^x and visibility.

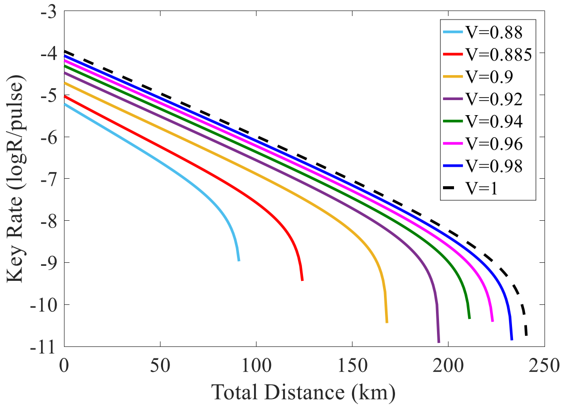

FIGURE 2. Key rate with different visibilities of infinite sized MDI-QKD protocol with a complete BSM.

where $p_{\max}$ and $p_{\min}$ are the maximum and minimum coincidence probabilities, respectively. In the HOM experiment, we measure the coincidence probability, defined as the probability of detecting photons at each output port of the BS in a time window smaller than the pulse duration. The coincidence probability takes the minimum $p_{\min}$ when photons arrive at the BS simultaneously, but almost constant value $p_{\max}$ when the time delay between the photons is larger than the pulse duration.

Considering the different success rates of different BSM methods, we need to multiply the key rate R in (1) by a coefficient, which is 1 for complete BSM, 1/2 for BS+PBS and 1/4 for BS-only. We verify the difference between the effects of indistinguishability of these methods as shown in Figs. 2–4 with the parameters given in Table 1. The key rate of complete BSM is highest when $V = 1$, but when V is near 0.9, the key rate becomes lower than the BS+PBS method. We can also clearly see that the BS+BPS method has much higher tolerance for indistinguishability.

Due to the lack of an evaluation criterion, we tentatively decided on the definition of acceptable visibility range. First, we define the maximum communication distance where the

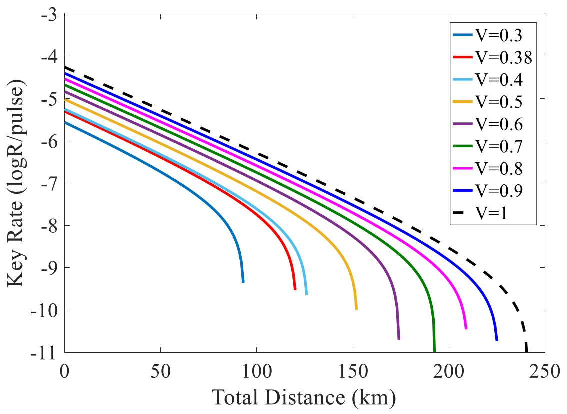

FIGURE 3. Key rate with different visibilities of infinite-sized MDI-QKD protocol with a BS+PBS BSM.

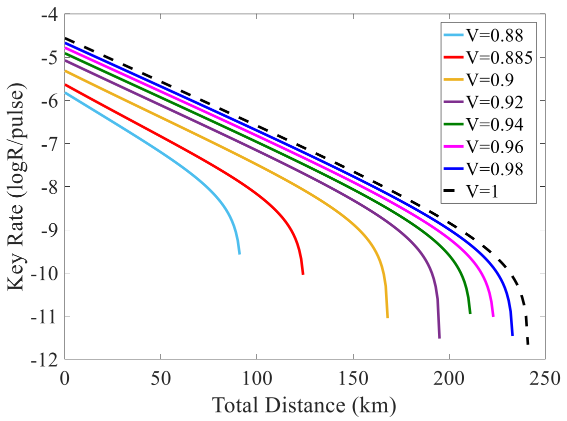

FIGURE 4. Key rate with different visibilities of infinite-sized MDI-QKD protocol with a BS-only BSM.

TABLE 1 Parameters for Simulation of MDI-QKD

Symbol	Parameter	Quantity
f	error correction inefficiency	1.16
α	loss coefficient of fiber	0.2 dB/km
p_d	dark count rate	3×10^{-6}
e_0	error rate of background	0.5
η_d	detection efficiency	14.5%

key rate falls into zero in our simulation. Then, we define the acceptable visibility which provide the maximum communication distance more than the half of that calculated for the ideal situation ($V = 1$). The minimum visibility is 0.38 for successful infinite-sized key generation.

III. SIMULATION OF FINITE SIZED MDI-QKD

In practical situations, the length of the raw key is finite, which induces a statistical fluctuation in parameter estimation. Here, we refer to [22] to calculate the effect of finite size. The expected lower and upper bounds of $\langle n^{\omega}_{\mu_i\nu_j}\rangle$ and $\langle m^{\omega}_{\mu_i\nu_j}\rangle$ are given by

$$\begin{aligned}\underline{E}\left(n^{\omega}_{\mu_i\nu_j}\right) \le \left\langle n^{\omega}_{\mu_i\nu_j}\right\rangle \le \overline{E}\left(n^{\omega}_{\mu_i\nu_j}\right)\\ \underline{E}\left(m^{\omega}_{\mu_i\nu_j}\right) \le \left\langle m^{\omega}_{\mu_i\nu_j}\right\rangle \le \overline{E}\left(m^{\omega}_{\mu_i\nu_j}\right)\end{aligned} \tag{7}$$

where $\overline{E}(X)$ and $\underline{E}(X)$ can be defined as

$$\begin{aligned}\underline{E}\left(X,\xi\right) &= \frac{X}{1+\delta_1\left(X,\xi\right)}\\ \overline{E}\left(X,\xi\right) &= \frac{X}{1-\delta_2\left(X,\xi\right)}\end{aligned} \tag{8}$$

where $\delta_1(X,\xi)$ and $\delta_2(X,\xi)$ are the positive solutions of

$$\begin{aligned}\left(\frac{e^{\delta_1}}{(1+\delta_1)^{1+\delta_1}}\right)^{\frac{X}{1+\delta_1}} &= \xi\\ \left(\frac{e^{-\delta_2}}{(1-\delta_2)^{1-\delta_2}}\right)^{\frac{X}{1-\delta_2}} &= \xi\end{aligned} \tag{9}$$

where ξ is the failure probability, which is set to 10^{-7}. Then, the expected lower bound of $\langle \underline{s^{\omega}_{11}}\rangle$ and upper bound of $\langle \overline{e^{\omega}_{11}}\rangle$ can be calculated from the Chernoff bound in (7). Then, the worst values of lower bound of s^{ω}_{11} and upper bound of e^{ω}_{11} become

$$s^{\omega}_{11} \ge \underline{\underline{s^{\omega}_{11}}} = \frac{\underline{O}\left(N^{\omega}_{\mu_2\nu_2}a_1^{\mu_2}b_1^{\mu_2}\left\langle\underline{s^{\omega}_{11}}\right\rangle\right)}{N^{\omega}_{\mu_2\nu_2}a_1^{\mu_2}b_1^{\mu_2}} \tag{10}$$

and

$$e^{\omega}_{11} \le \overline{\overline{e^{\omega}_{11}}} = \frac{\overline{O}\left(N^{\omega}_{\mu_2\nu_2}a_1^{\mu_2}b_1^{\mu_2}\underline{s^{\omega}_{11}}\left\langle\overline{e^{\omega}_{11}}\right\rangle\right)}{N^{\omega}_{\mu_2\nu_2}a_1^{\mu_2}b_1^{\mu_2}\underline{s^{\omega}_{11}}}. \tag{11}$$

where $\overline{O}(X)$ and $\underline{O}(X)$ can be defined as

$$\begin{aligned}\overline{O}\left(X,\xi\right) &= \left[1+\delta_3\left(X,\xi\right)\right]X\\ \underline{O}\left(X,\xi\right) &= \left[1-\delta_4\left(X,\xi\right)\right]X\end{aligned} \tag{12}$$

where $\delta_3(X,\xi)$ and $\delta_4(X,\xi)$ are the positive solutions of

$$\begin{aligned}\left(\frac{e^{\delta_3}}{(1+\delta_3)^{1+\delta_3}}\right)^{X} &= \xi\\ \left(\frac{e^{-\delta_4}}{(1-\delta_4)^{1-\delta_4}}\right)^{X} &= \xi\end{aligned}. \tag{13}$$

The final key rate with finite-sized effects will be [18], [22]

$$\begin{aligned}R \ge p_{\mu_2}p_{\nu_2}p^{\mathrm{z}}_{\mu_2}p^{\mathrm{z}}_{\nu_2}&\left\{\mu_2\nu_2e^{-\mu_2-\nu_2}s^{\mathrm{z}}_{11}\left[1-H\left(e^{\mathrm{x}}_{11}\right)\right]\right.\\ &\left.-S^{\mathrm{z}}_{\mu_2\nu_2}fH\left(E^{\mathrm{z}}_{\mu_2\nu_2}\right)\right\}\\ &-\frac{1}{N}\left(\log_2\frac{8}{\varepsilon_{\mathrm{cor}}}+2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}}+2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\right)\end{aligned} \tag{14}$$

where $\varepsilon_{\mathrm{cor}}$ is the failure probability of error correction, ε' and $\hat{\varepsilon}$ are the coefficients while using the chain rules of smooth min- and max-entropy, $\varepsilon_{\mathrm{PA}}$ is the failure probability of privacy amplification [22].

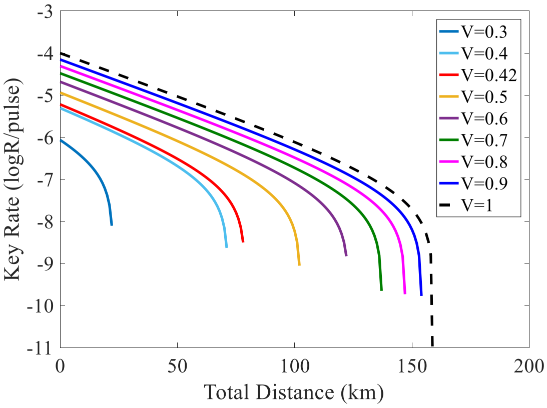

FIGURE 5. **Key rate with different visibilities of finite-sized MDI-QKD protocol with a BS + PBS BSM. The total number of pulses send by Alice and Bob is $N = 10^{14}$.**

For the convenience of calculation, we set Alice and Bob to have the same light source intensity and probability. Here we have chosen 0.4 and 0.05 for the signal and decoy intensity. The optimization of each distance point requires a large amount of additional calculation, so we refer to the probabilities of sources chosen by Alice and Bob in [20] to carry out the simulation calculation. We set the probability of signal and decoy source to 0.6 and 0.3 and the probability of signal and decoy source in z-basis to 0.98 and 0.27. Here, we use the same three intensities for each basis and the same parameter values. Although an increase in N moves the key rate closer to that of the infinite case, the total data length is limited to ensure key sharing in a realistic time frame. The effect of the total data length on communication speed should be considered in practice. In the next, we select $N = 10^{14}$ for a clock rate of 2.5 GHz and communication duration of 4×10^5 s to obtain a high key rate and practical communication period for calculation.

In the following, we calculate the finite-sized final key rates with different visibilities to examine the effect of the distinguishability of the two photons. Here, we set $N = 10^{14}$ and changed V from 0.3 to 1. The curves in Fig. 5 show that the acceptable condition of visibility $V = 0.42$ is more stringent for finite-size key generation than the $V = 0.38$ of the infinite-size, as shown in Fig. 3.

IV. CALCULATION FOR ACCEPTABLE TIME DELAY

With the acceptable visibility we can also calculate the acceptable time delay between the two photons from Alice and Bob. We considered two Gaussian photon pulses, which are typically assumed [31]:

$$\varphi_i(\omega) = \frac{1}{\pi^{1/4}\sqrt{\sigma_i}} e^{-\frac{(\omega-\bar{\omega}_i)^2}{2\sigma_i^2}}, (i = a, b) \tag{15}$$

where $\overline{\omega_i}$ is the central frequency of pulse i, and σ_i is its spectral width. If Alice's and Bob's Gaussians are identical, the coincidence probability of the HOM dip can be simply written as [33]

$$p = 1 - \frac{1}{2} e^{-\sigma_i^2 \tau^2} \tag{16}$$

which refers to the visibility V. The time delay of Alice's and Bob's photon pulses is τ. If the time duration of the photon pulse is assumed to be τ_L, the product of the time and bandwidth $\Delta\nu_L$ when both are at full width at half maximum (FWHM) is [34]

$$\tau_L \Delta\nu_L = \frac{2\ln 2}{\pi}\left[1 + \left(\frac{\beta}{\gamma}\right)^2\right]^{1/2} \geq C_B \tag{17}$$

where β is the phase modulation parameter, and γ describes the Gaussian pulse envelope relation to the temporal half-width of the radiant power of the pulse by

$$\tau_L = \left(\frac{2\ln 2}{\gamma}\right)^{1/2}. \tag{18}$$

The spectral FWHM is given by the spectral width as

$$\Delta\omega^2 = (2\pi\Delta\nu_L)^2 = \left(2\sqrt{2\ln 2}\sigma\right)^2. \tag{19}$$

So, (15) provides the condition of $\Delta\nu_L$ for Gaussian pulses as

$$\exp\left(-\frac{(2\pi\Delta\nu_L)^2}{8\sigma_i^2}\right) = \frac{1}{2}. \tag{20}$$

In the special case of a transform-limited pulse $\beta = 0$ (without phase modulation), the product C_B results becomes 0.441 [34]. By substituting (17) and (20) into (16), we can calculate the coincidence probability, p as follows:

$$p = 1 - \frac{1}{2} e^{-\frac{(2\ln 2)\tau^2}{\tau_L^2}}. \tag{21}$$

The $\beta = 0$ is the simplest case but can be achievable with proper dispersion compensation in the experiment. If $\beta \neq 0$, the phase modulation results in the temporal frequency shift or chirping, which would increase the distinguishability.

In the following, we fix the time duration to 100 and 200 ps. Because of the different key rates obtained by different decoy state calculation methods, we choose the result of the most efficient infinite-sized protocol. The HOM dips are shown in Fig. 6. They show that the acceptable time delay is 45.5 ps for 100-ps width and 89.0 ps for 200-ps width.

It should be noted that the calculation results we obtained are based on the three-intensity model. However, the four-intensity model [21], [22] with better performance have been proposed and implemented. It was suggested in four-intensity model will improve the performance for smaller number of pulses. Since the small data size is very important for practical QKD application, we should explore the improvement of the estimation with decoy method in the future. Fortunately, our conclusions are based on HOM interference, so this method is applicable to any quantum communication model (including MDI-QKD, mode-pairing QKD [35], etc.) that depends on two-photon interference.

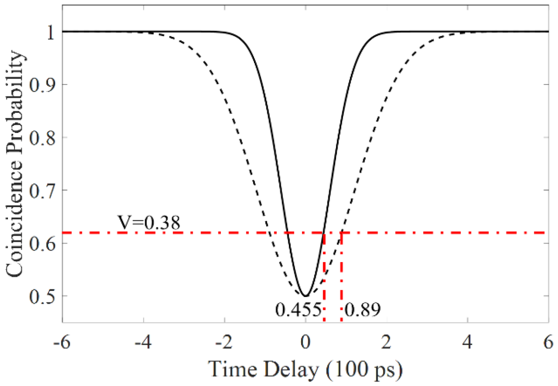

FIGURE 6. HOM-dip of 100 ps (black solid line) and 200 ps (black dotted line) time duration. The red dotted line of V = 0.38 represents the position with the minimum coincidence probability of 0.62.

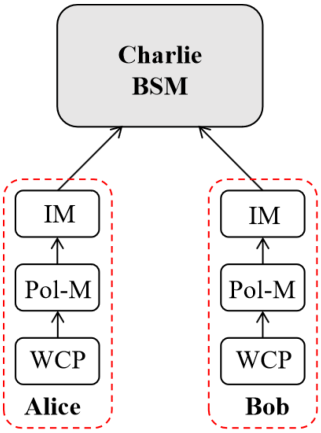

FIGURE 7. Schematic diagram of the polarization coding decoy state MDI-QKD. WCP: Weak coherent pulses source, Pol-M: Polarization modulator for state generation, IM: Intensity modulator for decoy method, BSM: Bell state measurement.

Time control is important because the fluctuation in the fiber length in the field has a greater effect as the distance increases. If the pulse duration increases, the time-control requirement is relaxed. However, this implies low clock frequency. A shorter time duration requires strict control of the laser spectrum, and a longer time duration reduces the pulse generation rate and, thus, the key generation rate. In addition, if the window of the photon detector is widened, the dark counts and, thus, the error rate increase.

The time delay of the two pulses is detected using Charlie's time-digital converter (TDC). The measured time delay data are processed by a computer and used to control the delay line on one side to reduce the time delay of the two photon pulses to increase visibility.

Commercially available TDC devices, such as Maxim Integrated's MAX35101 and Sciosense's TDC-GPX2, provide a time resolution of 10–20 ps. Although an accuracy of 45.5 ps can be realized with these devices, stricter control would be required to reduce the errors due to the distinguishability. We still need to explore electrical methods with more sophisticated TDC devices or optical methods to detect differences in arrival time.

Note that this value is for the present criteria. A different criterion will change the requirement. It is necessary to calculate it according to the system specifications.

V. CONCLUSION

In this article, we analyzed the finite-sized decoy state MDI-QKD protocol, which allows the receiver to be protected from attacks on the measurement device. For the implementation of this protocol, the photons generated by the two independent laser sources must be indistinguishable. We calculated the final key rate of the infinite-sized and finite-sized MDI-QKD to determine the effects of two-photon distinguishability on the visibility of their interference. We also estimated an acceptable time delay between two photons from two independent pulse lasers.

This article provides quantitative conditions for timing-control accuracy, which will play an important role in improving the performance of practical MDI-QKD systems. Because synchronization is crucial to achieving high visibility of two-photon interference, we still need to improve the method to measure and control the relative time difference between photons from remote sources.

APPENDIX

PROTOCOL

In practice, Alice and Bob use WCS to generate quantum signals. Each pulse state is prepared as one of the BB84 states, which are randomly generated from two mutually unbiased orthogonal basis (generally defined as z and x basis). The encoding can be polarization-encoding or phase-encoding, and these encodings are interchangeable in protocol and time-delay error analysis.

Polarization coding is considered in this article, as shown in Fig. 7. We assume that Alice and Bob use weak coherent pulses. The total number of pulses sent by Alice and Bob in the practical protocol is finite. The effects of the finite key length cannot be ignored. The protocol of the finite-size decoy method MDI-QKD considered here is as follows.

1) Alice and Bob select the basis from $\omega \in \{x, z\}$ with probability p_ω (where $\sum p_\omega = 1$). Then, they randomly assign bit values from $\{0, 1\}$. For the polarization-encoding scheme, the four states are $z_0 = 0°$, $z_1 = 90°$, $x_0 = 45°$, and $x_1 = 135°$.
2) Alice and Bob randomly generate three types of pulses with different intensities μ_i and ν_j $(i, j = 0, 1, 2)$ with probabilities p_{μ_i} and p_{ν_j} (where $\sum p_{\mu_i} = 1$ and $\sum p_{\nu_j} = 1$), respectively. Here, μ_2 and ν_2 represent the signal state, μ_1 and ν_1 represent the decoy state, and $\mu_0 = \nu_0 = 0$ represents the vacuum state. We assume that $\mu_2 > \mu_1 > 0$ and $\nu_2 > \nu_1 > 0$.

TABLE 2 **Bit Flip in Postprocessing**

Bell state	|Ψ⁻>	|Ψ⁺>	|Φ⁻>	|Φ⁺>
z	bit flip	bit flip	nonflip	nonflip
x	bit flip	nonflip	bit flip	nonflip

3) Alice and Bob send pulses via a quantum channel to Charlie, whose device may be under the control of eavesdropper Eve. The total number of pulses is recorded as *N*.
4) Charlie performs the BSM. Successful results are announced to Alice and Bob via an authenticated classical channel.
5) If a successful result is reported, Alice and Bob compare their basis and intensities via an authenticated classical channel. If Alice and Bob use the same basis, Bob (or Alice) performs a bit flip according to Charlie's result (see Table 2) to match with the other [18]. They then keep these bits as a sift key. The remaining bits are discarded.
6) Alice and Bob calculate the overall gain $S^{\omega}_{\mu_i\nu_j}$, which is defined as the probability of a successful BSM when Alice and Bob send pulses with intensities of μ_i and ν_j, respectively, in the basis of x or z.
7) Alice and Bob disclose the sift key sent with basis x to estimate error rate $E^{\mathrm{x}}_{\mu_i\nu_j}$. They disclose part of the sift key with basis z to estimate $E^{\mathrm{z}}_{\mu_i\nu_j}$. Then, they use the rest of the sift key with basis z of signal states μ_2 and ν_2 to generate the final key.
8) Alice and Bob correct these errors to generate an error-corrected key. Then, they determine the number of sacrificed bits from the yield and error rate based on the decoy method and perform privacy amplification to obtain the final key.

The overall gain $S^{\omega}_{\mu_i\nu_j} = n^{\omega}_{\mu_i\nu_j}/N^{\omega}_{\mu_i\nu_j}$ and QBER $E^{\omega}_{\mu_i\nu_j} = m^{\omega}_{\mu_i\nu_j}/n^{\omega}_{\mu_i\nu_j}$ are related to the counting rate and error rate by [6], [13], [14], [15]

$$S^{\omega}_{\mu_i\nu_j} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} e^{-\mu_i-\nu_j} s^{\omega}_{nm}$$

$$E^{\omega}_{\mu_i\nu_j} S^{\omega}_{\mu_i\nu_j} = \sum_{n,m=0}^{\infty} \frac{\mu_i^n \nu_j^m}{n!m!} e^{-\mu_i-\nu_j} s^{\omega}_{nm} e^{\omega}_{nm} \tag{22}$$

where $N^{\omega}_{\mu_i\nu_j}$ is the total number of pulse pairs with intensity μ_i and ν_j in basis ω, $n^{\omega}_{\mu_i\nu_j}$ $(m^{\omega}_{\mu_i\nu_j})$ is the number of effective (wrong) events from $N^{\omega}_{\mu_i\nu_j}$. The counting rate s^{ω}_{nm} is defined by the probability of a successful measurement event when Alice and Bob send pulses containing m and n photons, respectively. The error rate e^{ω}_{nm} is defined in a similar manner.

For a phase randomized WCS, the photon number distribution is [22]

$$a_n^{\mu_i} = e^{-\mu_i} \frac{\mu_i^n}{n!},\ b_m^{\nu_j} = e^{-\nu_j} \frac{\nu_j^m}{m!},\ n, m = 0, 1, 2, \ldots \tag{23}$$

The lower bound of counting rate of the single-photon pairs can be written as [15], [22]

$$s^{\omega}_{11} \geq \underline{s^{\omega}_{11}} = \frac{\hat{S}_+ - \hat{S}_-}{a_1^{\mu_1} b_1^{\nu_1} \tilde{a}_{12} \tilde{b}_{12}} \tag{24}$$

where

$$\tilde{a}_{12} = a_1^{\mu_1} a_2^{\mu_2} - a_1^{\mu_2} a_2^{\mu_1}, \tilde{b}_{12} = b_1^{\nu_1} b_2^{\nu_2} - b_1^{\nu_2} b_2^{\nu_1}$$
$$\hat{S}^{\omega}_{+} = g_{11} S^{\omega}_{\mu_1\nu_1} + g_{02} S^{\omega}_{\mu_0\nu_2} + g_{20} S^{\omega}_{\mu_2\nu_0} + g_{00} S^{\omega}_{\mu_0\nu_0}$$
$$\hat{S}^{\omega}_{-} = g_{12} S^{\omega}_{\mu_1\nu_2} + g_{21} S^{\omega}_{\mu_2\nu_1} + g_{01} S^{\omega}_{\mu_0\nu_1} + g_{10} S^{\omega}_{\mu_1\nu_0} \tag{25}$$

and

$$g_{11} = a_1^{\mu_1} a_2^{\mu_2} b_1^{\nu_1} b_2^{\nu_2} - a_1^{\mu_2} a_2^{\mu_1} b_1^{\nu_2} b_2^{\nu_1}$$
$$g_{12} = b_1^{\nu_1} b_2^{\nu_1} \tilde{a}_{12}, g_{21} = a_1^{\mu_1} a_2^{\mu_1} \tilde{b}_{12}$$
$$g_{02} = a_0^{\mu_1} g_{12}, g_{20} = b_0^{\nu_1} g_{21}$$
$$g_{00} = a_0^{\mu_1} b_0^{\nu_1} g_{11} - a_0^{\mu_1} b_0^{\nu_2} g_{12} - a_0^{\mu_2} b_0^{\nu_1} g_{21}$$
$$g_{01} = a_0^{\mu_1} g_{11} - a_0^{\mu_2} g_{21}, g_{10} = b_0^{\nu_1} g_{11} - b_0^{\nu_2} g_{12}. \tag{26}$$

Then, the upper bound of error rate is given by [22]

$$e^{\omega}_{11} \leq \overline{e^{\omega}_{11}} = \frac{\frac{m^{\omega}_{\mu_1\nu_1}}{N^{\omega}_{\mu_1\nu_1}} - a_0^{\mu_1} \frac{m^{\omega}_{\mu_0\nu_1}}{N^{\omega}_{\mu_0\nu_1}} - b_0^{\nu_1} \frac{m^{\omega}_{\mu_1\nu_0}}{N^{\omega}_{\mu_1\nu_0}} + a_0^{\mu_1} b_0^{\nu_1} \frac{m^{\omega}_{\mu_0\nu_0}}{N^{\omega}_{\mu_0\nu_0}}}{a_1^{\mu_1} b_1^{\nu_1} \underline{s^{\omega}_{11}}}. \tag{27}$$

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, 1984, pp. 175–179, doi: 10.48550/arXiv.2003.06557.

[2] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photon.*, vol. 8, no. 8, pp. 595–604, 2014, doi: 10.1038/nphoton.2014.149.

[3] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, 2006, Art. no. 022313, doi: 10.1103/PhysRevA.74.022313.

[4] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, 2008, Art. no. 042333, doi: 10.1103/PhysRevA.78.042333.

[5] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, 2000, Art. no. 1330, doi: 10.1103/PhysRevLett.85.1330.

[6] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, 2012, Art. no. 130503, doi: 10.1103/PhysRevLett.108.130503.

[7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, 2007, Art. no. 230501, doi: 10.1103/PhysRevLett.98.230501.

[8] E. Biham, B. Huttner, and T. Mor, "Quantum cryptographic network based on quantum memories," *Phys. Rev. A*, vol. 54, pp. 2651–2658, 1996, doi: 10.1103/PhysRevA.54.2651.

[9] H. Inamori, "Security of practical time-reversed EPR quantum key distribution," *Algorithmica*, vol. 34, pp. 340–365, 2002, doi: 10.1007/s00453-002-0983-4.

[10] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Phys. Rev. Lett.*, vol. 91, 2003, Art. no. 057901, doi: 10.1103/PhysRevLett.91.057901.

[11] X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” *Phys. Rev. Lett.*, vol. 94, 2005, Art. no. 230503, doi: 10.1103/PhysRevLett.94.230503.

[12] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Phys. Rev. Lett.*, vol. 94, 2005, Art. no. 230504, doi: 10.1103/PhysRevLett.94.230504.

[13] X. Ma and M. Razavi, “Alternative schemes for measurement-device-independent quantum key distribution,” *Phys. Rev. A*, vol. 86, 2012, Art. no. 062319, doi: 10.1103/PhysRevA.86.062319.

[14] X. Ma, C.-H. F. Fung, and M. Razavi, “Statistical fluctuation analysis for measurement-device-independent quantum key distribution,” *Phys. Rev. A*, vol. 86, 2012, Art. no. 052305, doi: 10.1103/PhysRevA.86.052305.

[15] S. H. Sun, M. Gao, C. Y. Li, and L. M. Liang, “Practical decoy-state measurement-device-independent quantum key distribution,” *Phys. Rev. A*, vol. 87, 2013, Art. no. 052329, doi: 10.1103/PhysRevA.87.052329.

[16] X.-B. Wang, “Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors,” *Phys. Rev. A*, vol. 87, 2013, Art. no. 012320, doi: 10.1103/PhysRevA.87.012320.

[17] T. Song, Q. Wen, F. Guo, and X. Tan, “Finite-key analysis for measurement-device-independent quantum key distribution,” *Phys. Rev. A*, vol. 86, 2012, Art. no. 022332, doi: 10.1103/PhysRevA.86.022332.

[18] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, “Finite-key analysis for measurement-device-independent quantum key distribution,” *Nature Commun.*, vol. 5, 2014, Art. no. 3732, doi: 10.1038/ncomms4732.

[19] C. Zhou et al., “Biased decoy-state measurement-device-independent quantum key distribution with finite resources,” *Phys. Rev. A*, vol. 91, 2015, Art. no. 022313, doi: 10.1103/PhysRevA.91.022313.

[20] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, “Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method,” *Phys. Rev. A*, vol. 91, 2015, Art. no. 032318, doi: 10.1103/PhysRevA.91.032318.

[21] Y. Zhou, Z. Yu, and X. Wang, “Making the decoy-state measurement-device-independent quantum key distribution practically useful,” *Phys. Rev. A*, vol. 93, 2016, Art. no. 042324, doi: 10.1103/PhysRevA.93.042324.

[22] X.-L. Hu, C. Jiang, Z.-W. Yu, and X.-B. Wang, “Practical long-distance measurement-device-independent quantum key distribution by four-intensity protocol,” *Adv. Quantum Technol.*, vol. 4, 2021, Art. no. 2100069, doi: 10.1002/qute.202100069.

[23] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks,” *Phys. Rev. Lett.*, vol. 111, 2013, Art. no. 130501, doi: 10.1103/PhysRevLett.111.130501.

[24] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, “Modeling a measurement-device-independent quantum key distribution system,” *Opt. Exp.*, vol. 22, pp. 12716–12736, 2014, doi: 10.1364/OE.22.012716.

[25] S. Pirandola et al., “High-rate measurement-device-independent quantum cryptography,” *Nature Photon.*, vol. 9, pp. 397–402, 2015, doi: 10.1038/nphoton.2015.83.

[26] H.-L. Yin et al., “Measurement-device-independent quantum key distribution over a 404 km optical fiber,” *Phys. Rev. Lett.*, vol. 117, 2016, Art. no. 190501, doi: 10.1103/PhysRevLett.117.190501.

[27] 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*, vol. 4, pp. 1016–1023, 2017, doi: 10.1364/OPTICA.4.001016.

[28] H. Liu et al., “Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels,” *Phys. Rev. Lett.*, vol. 122, 2019, Art. no. 160501, doi: 10.1103/PhysRevLett.122.160501.

[29] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, “Continuous-variable measurement-device-independent quantum key distribution,” *Phys. Rev. A*, vol. 89, 2014, Art. no. 052301, doi: 10.1103/PhysRevA.89.052301.

[30] C. K. Hong, Z. Y. Ou, and L. Mandel, “Measurement of subpicosecond time intervals between two photons by interference,” *Phys. Rev. Lett.*, vol. 59, 1987, Art. no. 2044, doi: 10.1103/PhysRevLett.59.2044.

[31] A. M. Brańczyk, “Hong-Ou-Mandel interference,” 2017. *arXiv: 1711.00080v1*, doi: 10.48550/arXiv.1711.00080.

[32] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, 2005, Art. no. 012326, doi: 10.1103/PhysRevA.72.012326.

[33] H. Kim, O. Kwon, and H. S. Moon, “Time-resolved two-photon interference of weak coherent pulses,” *Appl. Phys. Lett.*, vol. 118, 2021, Art. no. 244001, doi: 10.1063/5.0049746.

[34] J. Herrmann and B. Wilhelmi, “Principle of ultrashort optical pulse generation: Mode synchronization technology,” in *Lasers For Ultrashort Light Pulses*, Tokyo, Japan: Kyoritsu-Pub., 1991, pp. 75–80.

[35] P. Zeng, H. Zhou, W. Wu, and X. Ma, “Mode-pairing quantum key distribution,” *Nature Commun*, vol. 13, 2022, Art. no. 3903, doi: 10.1038/s41467-022-31534-7.