Optimizing Single-Photon Avalanche Photodiodes for Dynamic Quantum Key Distribution Networks

Guan-Jie Fan-Yuan,[1,2,3,†] Jun Teng,[1,2,3,†] Shuang Wang,[1,2,3,*] Zhen-Qiang Yin,[1,2,3] Wei Chen,[1,2,3] De-Yong He,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China*

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

[3] *State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, People's Republic of China*

(Received 31 January 2020; accepted 14 April 2020; published 12 May 2020)

Quantum key distribution (QKD) networks can provide unconditional secure communications among many remote users. In real QKD networks, with the dynamic access and quit of nodes, qualities of various user links and the link lengths among different users, such as transmission loss, are different and changing. Customized optimization that aims at various channel environments offers a network performance benefit. In this paper, we propose including the detection efficiency, dark-count probability, and afterpulse rate of the single-photon avalanche photodiode (SPAD) into the parameter optimization by controlling its voltage and temperature to optimize the secure key rates in dynamic QKD networks. The result shows that our method improves the network adaptability to the variation and asymmetry of channel and profits the establishment of QKD networks in a complex channel environment. This method is suitable for arbitrary SPAD-based QKD system and network architecture.

DOI: 10.1103/PhysRevApplied.13.054027

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows authorized partners, Alice and Bob, to share a private key securely. Its security is unconditional and relies on the principles of quantum physics [3,4]. The implementations and protocols of QKD are various, such as BB84 [5–8], DPS [9–11], measurement-device-independent QKD (MDI QKD) [12–15] and twin-field QKD [16–21]. But they share a common characteristic that the number of communicating parties is limited to two. Therefore, QKD networks [22–28], which can provide QKD service for numerous users is a goal of practical QKD and a critical stage of the Quantum Internet [29].

The diversity of QKD protocol leads to a variety of network architecture. The physical topologies of reported QKD-network implementations include point-to-point network [23], mesh topology [25,26], daisy chain [27], star topology [24,28], etc. Certainly, constructing a network with hybrid architecture is a common practice. Whatever the architecture adopted, however, QKD networks cannot ensure that the channel losses between users are the same. The immediate cause is the diversity of the user location. The spatial distance between users is the main factor governing the channel loss. The users located in different places can initiate a network access request anytime [22]. Moreover, the channel loss also depends on the physical link. For example, in fiber-based networks, more routes and more redundancy can lead to a high channel loss. Besides, the channel loss of an established communication can change over time. Typically, both the motion of users in free-space communication and the dynamic switching of physical link in fiber-based communication are the causes. Due to the sensitivity of secure key rate to parameter optimization, the diversity and dynamics of channel losses require a customized optimization of each QKD instance in networks.

For single-channel protocols, such as the BB84 protocol, where Alice and Bob are connected by a single channel, the parameters that can be optimized include the intensities of weak coherent source and the probabilities of preparing the quantum state with various intensities and bases. The former is introduced by the decoy technique, and the latter is a consideration for the finite-size effect. Besides, in other protocols, such as the measurement-device-independent protocol, both Alice and Bob are transmitters and connected with an untrusted relay, Charlie. The losses of the two channels connected with Charlie can be different, which is called asymmetry [30,31]. The asymmetric

*wshuang@ustc.edu.cn

†These authors contributed equally to this work.

channel can nearly double the number of parameters that need optimization, but the types of parameters are still the intensity and probability.

Optimizing only the parameters of transmitters limits the improving of the secure key rate. The potential of optimizing the detector is neglected in previous works. Here we propose a method that optimizes the parameters of the single-photon avalanche photodiode (SPAD) [32], which is the mainstream of the single-photon detection in QKD, to obtain the optimal secure key rates at various channel losses. The dual-track approach that optimizes the detector as well as the transmitter can further improve the performance of QKD, whose significance can be further reinforced by the asymmetry and dynamic of network channels. Due to the uniform role of detection units, our method is not limited to the protocols and architectures of QKD networks.

In our design shown in Sec. II, the detection efficiency, dark-count probability, and afterpulse rate [33], as the parameters related to the generation of the secure key rate, are included in the optimization. However, the working principle of SPAD limits the independent modulation of these parameters. To overcome the undesired correlations among them, we propose modulating them by two independent parameters, the bias voltage and temperature of SPAD. We collect the data from a commercial detector [34] to map the relationship among three factors and two independent parameters. Then, the detector can be optimized by modulating the bias voltage and temperature. In Sec. III, we numerically simulate the secure key rate of BB84 protocol on different losses as an exemplification of asymmetric and dynamic channels. The optimal voltages and temperatures on different losses are obtained. The comparison between the secure key rates with and without SPAD optimization shows that the improvement of our approach is significant.

II. METHOD

The parameter modulation of a QKD communication can be abstracted into an optimization problem. The objective function of the problem is the formula of the secure key rate, and the decision variables represent the system parameters related to the secure key rate. Therefore, the parameter optimization problem in previous works can be defined as

$$\begin{aligned} \max \quad & R(I,P,E_{\mathrm{nv}}) \\ \text{s.t.} \quad & I \geq 0 \\ & 0 \leq P \leq 1 \\ & \sum P = 1 \end{aligned} \tag{1}$$

where $I = \{\mu, \nu, \omega, \ldots\}$ is the set of intensities of weak coherent pulses, which depends on the particular scheme of decoy, $P = \{P_{\mu X}, P_{\mu Y}, \ldots, P_{\nu X}, P_{\nu Y}, \ldots\}$ is the set of the probabilities that preparing the pulse with particular intensity and basis, and E_{nv} is the set of the environment variable which includes the variables listed in Table I, and the parameters of detector. The restrictions represent the nature of the intensity and probability.

TABLE I. List of the experimental parameters used in numerical simulations. $N_Z = \sum_\alpha n_\alpha^Z$ is the total number of responses on Z basis. f_e is the error correction efficiency. $\varepsilon_{\mathrm{sec}}$ is the security parameters of finite key. $\varepsilon_{\mathrm{cor}}$ is the probability that a pair of nonidentical keys passes the error-verification step. $V_{\max}$ and e_{IC} are the optimal system visibility and its incompleteness in running system, they are used to depict the misalignment error.

N_Z	f_e	$\varepsilon_{\mathrm{sec}}$	$\varepsilon_{\mathrm{cor}}$	$V_{\max}$	e_{IC}
10^9	1.16	10^{-9}	10^{-15}	0.999	1%

Besides I and P, the secure key rate is directly dependent on the yield rate and error rate of single-photon states, which are also affected by the detection efficiency, dark-count probability, and afterpulse rate of SPAD. The detection efficiency and dark-count probability are the responsivity of a single-photon state and a vacuum state, respectively. The afterpulse rate is the average number of the afterpulses ignited by an avalanche of the light pulse and dark count. Therefore, in our method, the optimization problem is redefined as

$$\begin{aligned} \max \quad & R = f\,(I,P,\eta_d,p_d,p_a,E_{\mathrm{nv}}) \\ \text{s.t.} \quad & I \geq 0 \\ & 0 \leq P \leq 1 \\ & \sum P = 1 \\ & 0 \leq \eta_d \leq 1 \\ & 0 \leq p_d \leq 1 \\ & 0 \leq p_a \\ & g(\eta_d,p_d,p_a) = 0, \end{aligned} \tag{2}$$

where η_d is the detection efficiency, p_d is the dark-count probability, and p_a is the afterpulse rate.

The detection efficiency determines the number of valid counts, and the dark-count probability and the afterpulse rate introduce error counts. An ideal SPAD should have high detection efficiency, low dark-count probability, and low afterpulse rate. Unfortunately, it is a quantum version of "impossible trinity" [35] because of the working principle of SPAD. The correlation among the parameters is not yet clear and introduces the cooperative constraint, g, which is an obstacle to solve the optimization problem.

The working principle of SPAD is amplifying the electronic response to a single-photon absorption by avalanche gain [32,36,37]. Initially, the bias voltage, which is larger

than the breakdown voltage, reverses the SPAD to Geiger mode. When a photon arrives, the SPAD absorbs it and creates an electron-hole pair of electrical carriers. To detect the weak signal of single carriers, the carrier is charged by a high electric field and then ionizes extra carriers. As the process repeats in the electric field, the number of carriers increases exponentially. Finally, a strong enough signal is formed, which is called avalanche current. The breakdown current of biased diode generated by photon absorption and avalanche gain can be harnessed to detect the single photon. The detection efficiency is defined as the ratio of successful detections of avalanche current to photon incidences.

However, the primary dark current in SPAD can also ignite an avalanche as a seed carrier [38]. Such an undesirable response is called dark count. In addition, some defects can be formed in SPAD. The carriers of an avalanche can be trapped by defects and released in future detection. The release of trapped carriers can also ignite an avalanche after the previous avalanche, which is named afterpulse [38–40].

According to the physical principle of SPAD, the avalanche photodiode is reversed by a bias voltage to detect infrared single photons, which is known as Geiger mode operation. Therefore, the value of the bias voltage is critical to the performance of SPAD. Higher bias voltage increases the probability and intensity of avalanche and then brings higher detection efficiency. However, side effects are produced: the number of dark counts and afterpulses are also exacerbated by the rise of electric field intensity.

Besides, the breakdown voltage of SPAD shows a positive [41] correlation with the environmental temperature. As temperature increases, the avalanche is difficult to ignite due to the higher breakdown voltage, and both detection efficiency and dark-count probability are weakened. To ensure sufficient efficiency, the bias voltage is normally higher than it in the low temperature. Overall, under the influences of higher breakdown voltage and bias voltage, the dark-count probability is inflated when the detection efficiency remains unchanged. Hence, the SPAD is generally placed in a low-temperature environment to reduce the dark-count probability. However, the fact that the lifetime of trapped carriers is prolonged by lower temperature increases the afterpulse rate [39,40].

Therefore, the conditions of high detection efficiency, low dark-count rate, and low afterpulse rate cannot be satisfied simultaneously. However, it enlightens us to the fact that although the detection efficiency, the afterpulse rate, and the dark-count probability are *dependent*, the optimal state can be obtained by modulating the bias voltage and the temperature *independently*. The availability of separate regulation to bias voltage and temperature avoids the optimization of dependent parameters and builds an explicit solution space for the search algorithm. Then, the optimization problem can be redefined as

$$\begin{aligned} \max \quad & R = f\,(I, P, V, T, E_{\mathrm{nv}}) \\ \text{s.t.} \quad & I \geq 0 \\ & 0 \leq P \leq 1 \\ & \sum P = 1 \\ & V_{\min} \leq V \leq V_{\max} \\ & T_{\min} \leq T \leq T_{\max}, \end{aligned} \tag{3}$$

where V is the bias voltage, T is the temperature of avalanche diode, and the subscripts of min and max are the lower bound and upper bound of tunable ranges, respectively, which depend on the peripheral circuit of SPAD, and the constraint g is removed.

To solve the problem, the mappings from performance factors to bias voltage and temperature need to be built. For reliability and practicability, we collect the data, as detailed in Appendix A, from a real commercial SPAD-based detector (WT-SPD-300, Qasky). Note that because the differences between SPADs are inevitable, the data are an example and each detector needs its own characterization. However, the collection can be performed quickly with an automated program. Therefore, the difference is not an obstacle.

Figure 1 shows the measured relations among detection efficiency, dark-count probability, afterpulse rate, bias voltage, and temperature. The data indicates the correspondence with the aforementioned analysis. In addition, the detector has four preset modes of detection deficiency, 10, 15, 20, and 25%, which are marked by red circles. The temperatures on these modes are $-40.88\,^{\circ}\mathrm{C}$ and the corresponding bias voltages are 65.06, 65.32, 65.68, 66.22 V, respectively. With this data, we can solve the optimization problem and verify if the optimization of detectors is helpful for dynamic QKD networks.

III. RESULTS

In this section, we present that the optimization of detectors is beneficial and discuss the results of the numerical simulation. To simulate the network environment, we numerically calculate the secure key rate on different channel losses with the data of Fig. 1, which is shown in Fig. 2. Here we use the one-decoy states protocol [42] and the characterizations of measurement unit [33,43] in all key rate calculations.

The yields and error yields are affected by the detection efficiency, the dark-count probability and the afterpulse rate, hence the data collected in Sec. II can help in simulating them. Then the gain and error rate of single-photon states can be estimated based on the yields and error yields and further be used to obtain the secure key rate. The

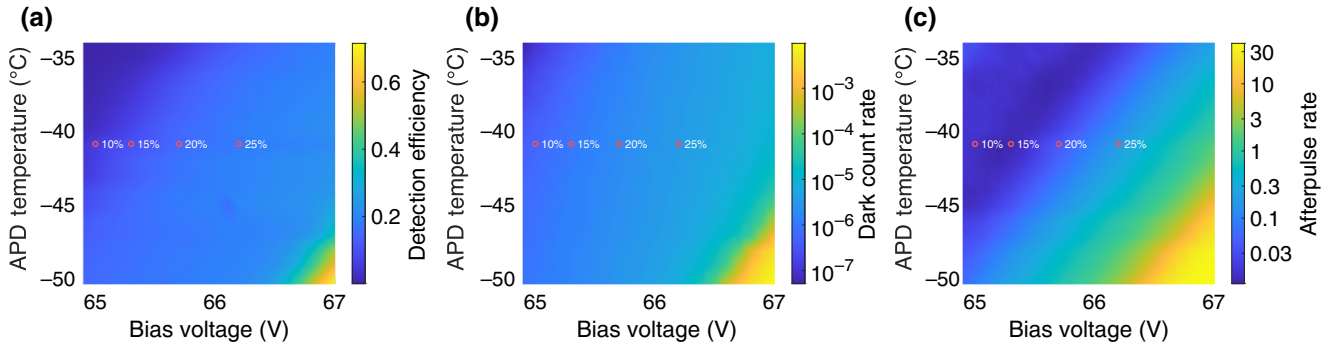

FIG. 1. (a) Detection efficiency, (b) dark-count probability, and (c) afterpulse rate as functions of bias voltage and temperature. The red circles mark four preset modes of a single-photon detector, which respectively, denote 10, 15, 20, and 25% of factory detection efficiencies. The ranges of bias voltage and temperature are 64.9 to 67 V and −34.07 to −54.33 °C, respectively. The step sizes of bias voltage and temperature are set as 0.1 V and 1 °C.

method of secure key rate calculation is described in detail in Appendix B.

Here, for comparison, the data of the detector are used in two distinct ways. One is the same as previous works, keeping the detection efficiency, the dark-count probability, and the afterpulse rate unchanged at different communication distances. The other is our optimization method, finding the optimal parameters for various communication distances by modulating the bias voltage and the temperature.

The secure key rates obtained by the two methods are shown in Fig. 2, which indicates the advantage of detector optimization. The solid line is the secure key rate using the optimization method, and the dashed lines are the results in preset modes of 10, 15, 20, and 25%, respectively.

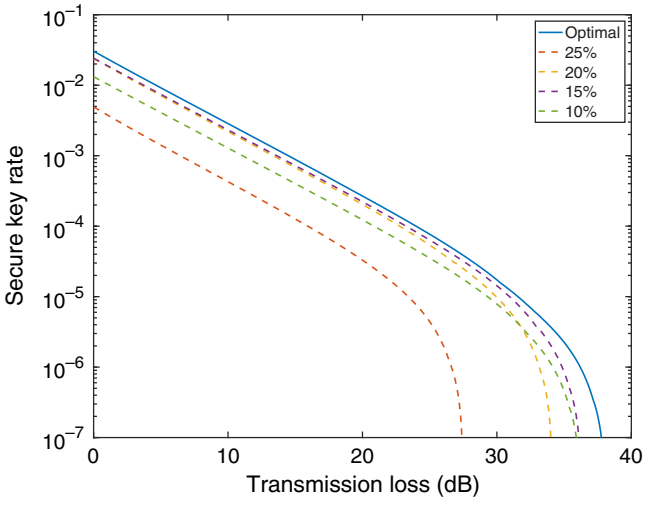

FIG. 2. Optimal secure key rates (per pulse) with and without detector optimization in logarithmic scale as functions of transmission loss, which are represented by solid and dashed lines, respectively.

This result proves the validity of our method. Figure 2 shows that the preset modes never become the optimal state on all transmission losses. Both secure key rate and maximum tolerable transmission loss on the optimal state are better than them on preset modes. Moreover, the secure key rate obtained in the highest detection efficiency is, however, the lowest result. Because the afterpulse rate in the mode of 25% is significantly higher than in other modes. The error rate introduced by afterpulses lower the secure key rate. Furthermore, the cross of yellow and green lines confirms our analysis. That is, the higher detection efficiency is more appropriate at a short distance, and the lower dark-count probability, and afterpulse rate are important at a long distance. The best is the mode of 15%, which represents the most balanced state in embedded modes. Therefore, in real QKD networks where the distances between users are various and changing, the detector optimization for specific communication links is effectual.

Furthermore, the optimal state is not changeless on different channel losses. For a clear explanation, the movement locus of optimal state among detection efficiency, dark-count probability and afterpulse rate are shown in Fig. 3. The result shows that the bias voltage and temperature decrease with the increase of transmission loss.

This conclusion bears out the analysis in Sec. II. In QKD networks, afterpulses, and dark counts introduce error responses and influence the longest distance of secure communication. Therefore, the bias voltage is reduced on high transmission losses to obtain low dark-count probability and afterpulse rate by sacrificing the detection efficiency.

Finally, the optimal values of detection efficiency, dark-count probability, and afterpulse rate on different losses are shown in Fig. 4. Comparing with detection efficiency, reducing the dark counts, and afterpulses for lower error yield is preferential as the transmission loss increases.

Although it seems counterintuitive that the afterpulse rate is increasing, the afterpulse is indeed weakened.

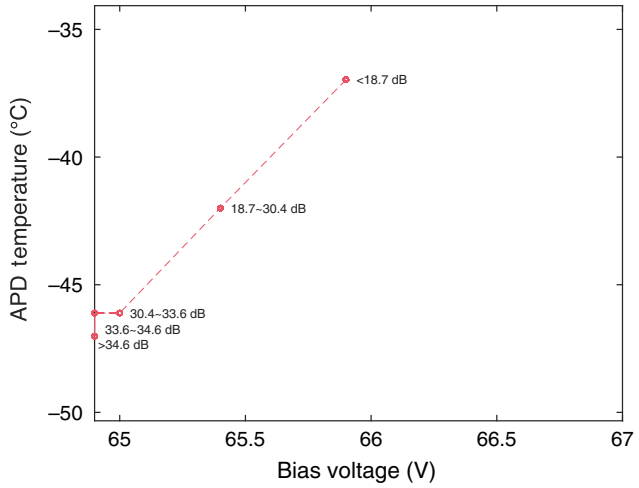

FIG. 3. Optimal state on different transmission losses.

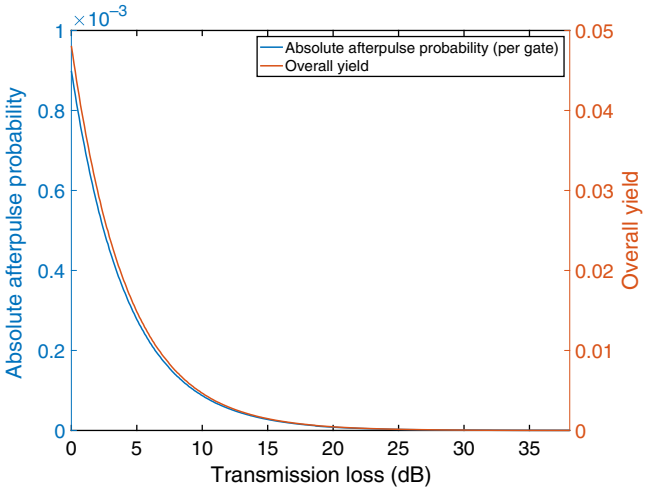

FIG. 5. Absolute probability of an afterpulse and the overall yield of the one-decoy method as functions of transmission loss.

Because the afterpulse depends not only on the afterpulse rate of detectors, but the intensity of laser pulses the detector received. Specifically, an afterpulse is likely to be ignited only if an initial avalanche occurred, then the higher the afterpulse rate is, the greater the probability of igniting an afterpulse. The detailed derivation of the afterpulse probability is shown in Eq. (B14). Therefore, an increase in the afterpulse rate on its own does not determine the absolute probability of an afterpulse. Even if the afterpulse rate increases, the absolute probability of an afterpulse may decrease if the yield also decreases, which can be caused by the lower intensity of emergent pulses, lower detection efficiency, and higher transmission loss.

Figure 5 shows that the increment of the transmission loss causes the absolute probability of an afterpulse to plummet. The red line indicates that the linear increase in the transmission loss leads to an exponential decrease in the yield, such insufficient prerequisite forces the afterpulse probability down (blue line) while the afterpulse rate remains the same magnitude as shown in Fig. 4. Therefore, the afterpulse effect is not enhanced.

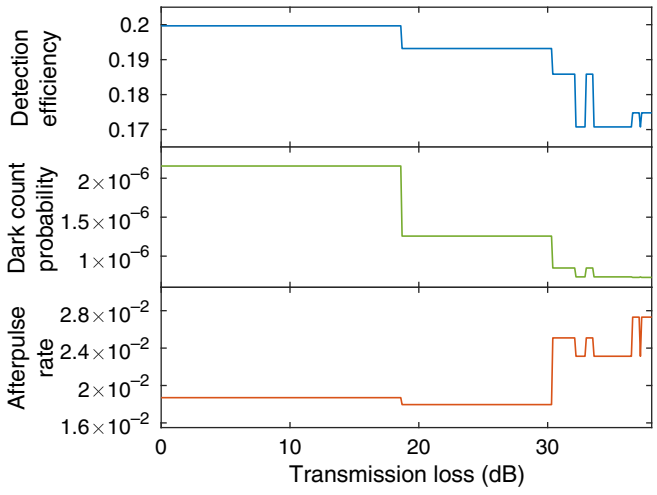

FIG. 4. Optimal detection efficiency, dark-count probability, and afterpulse rate as functions of transmission loss, which are represented by red, green, and blue lines, respectively.

IV. CONCLUSION

In conclusion, we propose a solution to the channel loss changing and asymmetry in QKD networks. It works because the sensitivity of QKD networks to dark counts and afterpulses changes with channel loss. By adjusting the bias voltage and temperature of SPAD, its detection efficiency, dark-count probability, and afterpulse rate can be maintained at optimal values. Our method can effectively improve the secure key rate and the longest secure communication distance.

Furthermore, other parameters that can affect the detection efficiency, dark-count probability, and afterpulse rate, such as dead time and threshold voltage, can also be a complement to the bias voltage and temperature. Because they, in essence, increase the available combinations of detection efficiency, dark-count probability, and afterpulse rate, which cannot worsen the optimal result. In theory, anything that expands the feasible set can benefit the optimization. Besides, with accurate modeling, the characterization of the relationship among parameters can be avoided. Here characterizing the detector is chosen for the reliability and practicability.

The network is a dynamic world, the change and asymmetry of channels are inevitable. Our method offers an initiative adaptation of QKD systems to the channel change and helps in building a QKD network in a fickle environment. Moreover, future QKD networks may be realized in hybrid topologies. Remarkably, our method is effective to

all types of QKD network based on the SPAD and can be a beneficial complementary to previous works.

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. 61622506, No. 61575183, No. 61627820, No. 61475148, and No. 61675189), and the Anhui Initiative in Quantum Information Technologies.

APPENDIX A: CHARACTERIZATION OF SPAD

In this work, to map the relations, we collect the data based on the scheme shown in Fig. 6. Specifically, the pulsed laser source (ID300, ID Quantique) and the single-photon detector (WT-SPD-300, Qasky) are triggered by clock signals of 1 and 50 MHz, respectively. The laser pulse is attenuated to a weak coherent pulse with the mean photon number (μ_t) of 0.1. The gate width and dead time of the detector are set at 1 and 50 ns. The ranges of bias voltage and temperature are 64.9 to 67 V and −34.07 to −54.33 °C, respectively, within the capabilities of device software function. These ranges are selected to contain four special states, 10, 15, 20, and 25% of factory detection efficiency, which are preset in the device as optional suggested modes. The step sizes of bias voltage and temperature are set as 0.1 V and 1 °C. Since the characters of each avalanche photodiode are not necessarily the same, the scan range and step size can be modified to specific situations.

To measure the required data, a time-to-digital converter (quTAG, qutools) is started by a clock signal, which is the same as the trigger signal of the laser, and stopped by the response signals of the detector. Therefore, in each period of start, there is a time tag with a constant delay to the start signal according to pulse-emitting events. The count at such a time tag, denoted by C_{dd}, contains successful detection responses and dark counts. There are also other time tags created by the afterpulse responses and dark counts, whose count is denoted by C_{ad}, because the detector opens its gate at those time tags without incident pulse. Both C_{dd} and C_{ad} are cumulated in 30 s. In addition, the dark counts per second, C_d, can be obtained by counting the detector responses with the extinct laser source. Then, the detection efficiency, η_d, the dark-count probability, p_d, and the afterpulse rate, p_a, can be derived by the following relationships:

$$\begin{aligned}\eta_d &= \frac{\ln\left(1-\frac{C_{dd}}{30\times10^6}\right)}{-\mu_t(1-p_d)},\\ p_d &= \frac{C_d}{50\times10^6},\\ p_a &= \frac{C_{ad}-p_d\times30\times(50-1)\times10^6}{C_{dd}}.\end{aligned} \tag{A1}$$

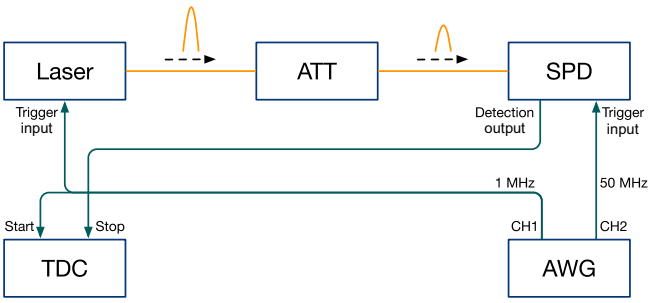

FIG. 6. Schematic diagram of data collection. Laser, short-pulse laser source; ATT, attenuator; SPD, single-photon detector; TDC, time-to-digital converter; AWG, arbitrary waveform generator.

APPENDIX B: CALCULATION OF SECURE KEY RATE

The total secure key rate R can be generated by X basis and Z basis.

$$R = \frac{l_X + l_Z}{N} \tag{B1}$$

$$\begin{aligned}l_\omega = {}& s_0^{\omega-}+s_1^{\omega-}[1-H_2(e_{1,p}^{\omega\ +})]\\ &-\lambda_{\mathrm{EC}}-6\log_2\frac{19}{\varepsilon_{\mathrm{sec}}}-\log_2\frac{2}{\varepsilon_{\mathrm{cor}}},\end{aligned} \tag{B2}$$

where s_0 is the number of vacuum events, s_1 is the number of single-photon events, $e_{1,p}$ is the phase error rate, the superscripts + and − represent upper and lower bounds, respectively, N is the total number of pulses (sent by Alice), $\omega \in \{X, Z\}$ represents a basis, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $\lambda_{\mathrm{EC}} = n^\omega f_e H_2(E_\omega)$ is the consumption of the information in error correction, f_e is the efficiency factor of the error-correction method used, $\varepsilon_{\mathrm{cor}}$ and $\varepsilon_{\mathrm{sec}}$ are secure parameters.

All needed parameters can be estimated by analytic formulas [42,44,45]. The analytic formulas of the one-decoy scheme, intensity $\alpha \in \{\mu, \nu\}$, which used in our simulation are given by

$$s_0^{\omega-} = \frac{\tau_0}{\mu-\nu}\left(\frac{\mu e^\nu n_\nu^{\omega-}}{P_\nu}-\frac{\nu e^\mu n_\mu^{\omega+}}{P_\mu}\right) \tag{B3}$$

$$\begin{aligned}s_1^{\omega-} = {}& \frac{\mu\tau_1}{\nu(\mu-\nu)}\\ &\left[\frac{e^\nu n_\nu^{\omega-}}{P_\nu}-\frac{\nu^2 e^\mu n_\mu^{\omega+}}{\mu^2 P_\mu}-\frac{\mu^2-\nu^2}{\mu^2}\frac{s_0^{\omega+}}{\tau_0}\right]\end{aligned} \tag{B4}$$

$$e_{1,p}^{\omega\ +} = \frac{v_1^{\overline{\omega}+}}{s_1^{\overline{\omega}-}} + \gamma\left(\varepsilon_{\sec}, \frac{v_1^{\overline{\omega}+}}{s_1^{\overline{\omega}-}}, s_1^{\overline{\omega}-}, s_1^{\omega-}\right), \tag{B5}$$

where

$$\tau_n = \sum_\alpha P_\alpha \frac{e^{-\alpha}\alpha^n}{n!}, \tag{B6}$$

$$s_0^{\omega+} = 2\left(\tau_0 m_\alpha^{\omega+} + \sqrt{\frac{\sum_\alpha n_\alpha^\omega}{2}\log\frac{19}{\varepsilon_{\sec}}}\right), \tag{B7}$$

$$v_1^{\omega+} = \frac{\tau_1}{\mu-\nu}\left(\frac{e^\mu m_\mu^{\omega+}}{P_\mu} - \frac{e^\nu m_\nu^{\omega-}}{P_\nu}\right), \tag{B8}$$

$$\gamma(a,b,c,d) = \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}}\sqrt{\log_2\left(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}\right)}. \tag{B9}$$

ω and $\overline{\omega}$ are different bases, i.e., $\omega = Z$ when $\overline{\omega} = X$ and vice versa. $n_\alpha^{\omega\pm}$ and $m_\alpha^{\omega\pm}$ are the upper bound and lower bound of the number of detections and bit error of basis ω and intensity α.

In order to deal with the statistical fluctuation, according to the counterfactual protocol proposed by Ref. [45], the counts and errors can be bounded by Hoeffding's inequality.

$$\begin{aligned} n_\alpha^{\omega\pm} &= n_\alpha^\omega \pm \sqrt{\frac{n^\omega}{2}\ln\frac{19}{\varepsilon_{\sec}}}, \\ m_\alpha^{\omega\pm} &= m_\alpha^\omega \pm \sqrt{\frac{m^\omega}{2}\ln\frac{19}{\varepsilon_{\sec}}} \end{aligned} \tag{B10}$$

In the numerical simulation, n_α^ω and m_α^ω can be derived by

$$\begin{aligned} n_\alpha^\omega &= NP_\alpha P_\omega P_\omega Q_\alpha^\omega, \\ m_\alpha^\omega &= NP_\alpha P_\omega P_\omega E_\alpha^\omega Q_\alpha^\omega, \end{aligned} \tag{B11}$$

where $P_\alpha, P_\omega, Q_\alpha^\omega, E_\alpha^\omega Q_\alpha^\omega$ are the ratio of α state, the selecting probability ω basis, the gain of α state in ω basis, and the QBER of α state in ω basis, respectively.

The gain and QBER can be obtained by

$$\begin{aligned} Q_\mu &= p_\mu^a(1-p_\mu^b) + (1-p_\mu^a)p_\mu^b + p_\mu^a p_\mu^b, \\ E_\mu Q_\mu &= (1-p_\mu^a)p_\mu^b + \frac{1}{2}p_\mu^a p_\mu^b, \end{aligned} \tag{B12}$$

where the p_μ^a and p_μ^b are the response probability of detector a and b, respectively, in a dual-detector system.

Furthermore, the p_μ^a and p_μ^b are given by

$$\begin{aligned} p_\mu^a &= 1 - e^{-\mu\eta(1-\eta_l)}(1-Y_0)(1-P_{ap}), \\ p_\mu^b &= 1 - e^{-\mu\eta\eta_l}(1-Y_0)(1-P_{ap}), \end{aligned} \tag{B13}$$

where μ is the intensity of the coherent source, η is the overall transmission of the channel, η_l is the light leak ratio, Y_0 is the background counting rate, P_{ap} is the afterpulse probability.

The relationship between Y_0 and p_d depends on the scheme of detection. For example, Y_0 is equal to p_d and $2p_d(1-p_d)$ for the single-detector scheme and the dual-detector scheme, respectively.

The η_l is defined by the optimal visibility, $V_{\max}$, and the incompleteness of optimal visibility, e_{IC}, which characterizes the misalingment error in Ref. [43].

$$\begin{aligned} \eta_l &= \frac{1-V}{2}, \\ V &= (1-e_{IC})V_{\max}. \end{aligned} \tag{B14}$$

The afterpulse probability can be obtained by the analysis proposed in Ref. [33].

$$\begin{aligned} P_{ap} &= \frac{p_a}{1-p_a}\hat{Q}^d \\ \hat{Q}^d &= \sum_{\alpha=\mu,\nu,\ldots} P_\alpha \widetilde{Q_\alpha} \\ \widetilde{Q_\alpha} &= (P_X^2 + P_Z^2)\left\{1 - \frac{1}{2}[e^{-\alpha\eta(1-\eta_l)} + e^{-\alpha\eta\eta_l}](1-Y_0)\right\} \\ &\quad + 2P_X P_Z\left[1 - e^{-(\alpha\eta/2)}(1-Y_0)\right], \end{aligned} \tag{B15}$$

where p_a is the overall afterpulse rate, P_α and $\widetilde{Q_\alpha}$ are the selecting probability and response probability of the state of intensity α respectively, P_X and P_Z are the probabilities of selecting basis (X or Z) in preparation and measurement. Note that Eqs. (B14) require that $p_a < 1$. If $p_a \geq 1$, P_{ap} is set to 1.

In our numerical simulation, the full parameter optimization is employed. The values of these parameters are listed in Table I.

[1] C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems & Signal Processing* (IEEE, Bangalore, 1984), p. 175.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings* (IEEE, Chicago, 2004), p. 136.

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

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

[6] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M. J. Li *et al.*, Secure Quantum Key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[7] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W. S. Tam, A. Plews, A. W. Sharp, Z. L. Yuan, and A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica **4**, 163 (2017).

[8] S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, J. Yin, Q. Shen, Y. Cao, Z. P. Li *et al.*, Satellite-to-ground quantum key distribution, Nature **549**, 43 (2017).

[9] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature **509**, 475 (2014).

[10] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, Nat. Photonics **9**, 827 (2015).

[11] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, Nat. Photonics **9**, 832 (2015).

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

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

[14] H. L. Yin, T. Y. Chen, Z. W. Yu, H. Liu, L. X. You, Y. H. Zhou, S. J. Chen, Y. Q. Mao, M. Q. Huang, W. J. Zhang *et al.*, Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[15] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, W. W. S. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).

[16] 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).

[17] C. H. Cui, Z. Q. Yin, R. Wang, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Twin-Field Quantum Key Distribution Without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[18] X. F. Ma, P. Zeng, and H. Y. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[19] X. B. Wang, Z. W. Yu, and X. L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[20] S. Wang, D. Y. He, Z. Q. Yin, F. Y. Lu, C. H. Cui, W. Chen, Z. Zhou, G. C. Guo, and Z. F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-Of-Principle Quantum Key Distribution System, Phys. Rev. X **9**, 021046 (2019).

[21] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

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

[23] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes *et al.*, The SECOQC quantum key distribution network in vienna, New J. Phys. **11**, 075001 (2009).

[24] S. Wang, W. Chen, Z. Q. Yin, Y. Zhang, T. Zhang, H. W. Li, F. X. Xu, Z. Zhou, Y. Yang, D. J. Huang *et al.*, Field test of wavelength-saving quantum key distribution network, Opt. Lett. **35**, 2454 (2014).

[25] T. Y. Chen, J. Wang, H. Liang, W. Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W. Q. Cai, L. Ju *et al.*, Metropolitan all-pass and inter-city quantum communication network, Opt. Express **18**, 27217 (2010).

[26] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[27] S. Wang, W. Chen, Z. Q. Yin, H. W. Li, D. Y. He, Y. H. Li, Z. Zhou, X. T. Song, F. Y. Li, D. Wang *et al.*, Field and long-term demonstration of a wide area quantum key distribution network, Opt. Express **18**, 21739 (2014).

[28] Y. L. Tang, H. L. Yin, Q. Zhao, H. Liu, X. X. Sun, M. Q. Huang, W. J. Zhang, S. J. Chen, L. Zhang, L. X. You *et al.*, Measurement-Device-Independent Quantum Key Distribution Over Untrustful Metropolitan Network, Phys. Rev. X **6**, 011024 (2016).

[29] Stephanie Wehner, David Elkouss, and Ronald Hanson, Quantum internet: A vision for the road ahead, Science **362**, eaam9288 (2018).

[30] W. Y. Wang, F. H. Xu, and H. K. Lo, Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks, Phys. Rev. X **9**, 041012 (2019).

[31] H. Liu, W. Y. Wang, K. J. Wei, X. T. Fang, L. Li, N. L. Liu, H. Liang, S. J. Zhang, W. J. Zhang, H. Li *et al.*, Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum key Distribution Over Asymmetric Channels, Phys. Rev. Lett. **122**, 160501 (2019).

[32] J. Zhang, M. A. Itzler, H. Zbinden, and J. W. Pan, Advances in InGaAs/InP single-photon detector systems for quantum communication, Light: Sci. Appl. **4**, e286 (2015).

[33] G. J. Fan-Yuan, C. Wang, S. Wang, Z. Q. Yin, H. Liu, W. Chen, D. Y. He, Z. F. Han, and G. C. Guo, Afterpulse Analysis for Quantum Key Distribution, Phys. Rev. Appl. **10**, 064032 (2018).

[34] Qasky, Infrared single photon detector, accessed March 31, 2020. http://www.qasky.com/en/info.asp?base_id=2&second_id=2004

[35] James M. Boughton, On the origins of the fleming-mundell model, IMF Staff Papers **50**, 1 (2002).

[36] R. H. Hadfield, Single-photon detectors for optical quantum information applications, Nat. Photonics **3**, 696 (2009).

[37] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, Invited review article: Single-photon sources and detectors, Rev. Sci. Instrum. **82**, 071101 (2011).

[38] Y. Kang, H. X. Lu, Y. H. Lo, D. S. Bethune, and W. P. Risk, Dark count probability and quantum efficiency of avalanche photodiodes for single-photon detection, Appl. Phys. Lett. **83**, 2955 (2003).

[39] K. E. Jensen, P. I. Hopman, E. K. Duerr, E. A. Dauler, J. P. Donnelly, S. H. Groves, L. J. Mahoney, K. A. McIntosh, K. M. Molvar, A Napoleone *et al.*, Afterpulsing in geiger-mode avalanche photodiodes for 1.06 μm wavelength, Appl. Phys. Lett. **88**, 133503 (2006).

[40] F. X. Wang, W. Chen, Y. P. Li, D. Y. He, C. Wang, Y. G. Han, S. Wang, Z. Q. Yin, and Z. F. Han, Non-markovian property of afterpulsing effect in single-photon avalanche detector, J. Lightwave Technol. **34**, 3610 (2016).

[41] D. Bronzi, F. Villa, S. Bellisai, B. Markovic, S. Tisa, A. Tosi, F. Zappa, S. Weyers, D. Durini, W. Brockherde, and U. Paschen, in *2012 Proceedings of the European Solid-State Device Research Conference (ESSDERC)* (IEEE, Bordeaux, France, 2012), p. 230.

[42] Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden, Finite-key analysis for the 1-decoy state QKD protocol, Appl. Phys. Lett. **112**, 171104 (2018).

[43] Guan-Jie Fan-Yuan, Shuang Wang, Zhen-Qiang Yin, Wei Chen, De-Yong He, Zheng-Fu Han, and Guang-Can Guo, Modeling Alignment Error in Quantum Key Distribution Based on a Weak Coherent Source, Phys. Rev. Appl. **12**, 064044 (2019).

[44] X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

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