Research Article Vol. 4, No. 9 / September 2017 / Optica 1016

Measurement-device-independent quantum key distribution robust against environmental disturbances

Chao Wang,[1,2,3] Zhen-Qiang Yin,[1,2,3,4] Shuang Wang,[1,2,3,5] Wei Chen,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1]Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei, Anhui 230026, China
[2]Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
[3]State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
[4]e-mail: yinzq@ustc.edu.cn
[5]e-mail: wshuang@ustc.edu.cn

Received 3 April 2017; revised 26 July 2017; accepted 27 July 2017 (Doc. ID 291983); published 24 August 2017

Measurement-device-independent quantum key distribution (MDI QKD) is a promising protocol for removing all detector side channel attacks. However, the variation of reference frames, e.g., polarization and phase reference, would be an acute threat to the performance of MDI systems. Here, based on polarization scrambling units, we demonstrate a reference-frame-independent MDI QKD scheme that is inherently stable against volatile channel conditions; therefore, the final secure key rate will be insensitive to the random disturbances of polarization and the drifts of phase reference. Thus, calibrations of the primary reference frames are intrinsically removed in our scheme, which essentially reduces potential vulnerabilities as well as the resource consumption of the whole system. In addition, a proof-of-principle experiment with an improved fluctuation analysis method is demonstrated to verify the feasibility and advantages of the proposed scheme.

OCIS codes: (270.0270) Quantum optics; (270.5568) Quantum cryptography; (060.0060) Fiber optics and optical communications; (060.5565) Quantum communications.

https://doi.org/10.1364/OPTICA.4.001016

1. INTRODUCTION

Quantum key distribution (QKD) [1], based on the fundamental principles of quantum physics instead of mathematical complexities, ensures the information-theoretic security of secret sharing among distant parties. Due to its promising future for practical use, QKD has attracted much attention in recent decades. Numerous efforts have been made to improve the practical security, applicability, and efficiency of QKD systems [2–12]. However, the practical security of real-life QKD applications is still questionable because of the realistic features of practical devices [13–17].

Measurement-device-independent QKD (MDI QKD), proposed to eliminate all possible detector side channel attacks, offers a great balance between practical security and usability [18,19]. In this protocol, the assumption of perfect and certified measurement is essentially removed, which is an important precondition of conventional QKD protocols. The MDI QKD protocol has been studied extensively since its emergence, and several MDI QKD experimental demonstrations as well as networks have been presented [20–28]. No matter which detailed coding scheme was deployed in these demonstrations, the spectrum, timing, and polarization mode as well as the coding reference frame of two independent sources needed to be rigorously calibrated to ensure efficient Bell-state measurement (BSM). In our previous work [26,29], we reported a MDI QKD protocol as well as a proof-of-principle experiment with no active coding reference (phase reference) calibration applied, which simplified the MDI QKD system and reduced the aligning expenses as well as the security risks for practical use. However, just like with other systems, the alignment process of polarization and timing states were still needed in our scheme [26].

Actually, to keep an identical spectrum for remote parties in MDI systems, we could simply use frequency-locked lasers whose center wavelengths remain consistent with a molecular absorption line [23,26,30]. Thus the spectrum indistinguishability of independent sources can be easily and effectively guaranteed. The timing synchronization in a QKD system can also be simply compensated with today's techniques, which will not cause dramatic system errors or decrease the final secure key rates [11,31].

Comparatively, the random birefringence evolution in optical fibers can be affected and accumulated by numerous ambient environmental disturbances such as temperature changes [32,33], mechanical stress [34,35], and electromagnetic interference [35]. Therefore, the final output polarization may change

rapidly in field optical networks, especially in complex and volatile channel conditions [32,33,36]. To ensure the indistinguishability between two polarization modes in the MDI QKD system, the most common solution is to use the polarization feedback system for automatic polarization stabilization [20,21,25,26]. These active compensation approaches, however, will either be time-consuming with faint laser pulses, which may have unreliable performance in unstable environments, or use auxiliary classical pulses, which will affect the performance of a system with wavelength-dependent fiber birefringence (wavelength-division multiplexing system) [37] or time polarization decorrelation between reference and quantum signals (time-division multiplexing system) [38], leading to unstable or even intermittent performance of a practical MDI QKD system in volatile environments. Moreover, the polarization calibration will increase the complexity of the system, which may compromise the practical security of MDI QKD. In addition, the polarization calibration processes make the MDI QKD network complicated and less practical, as frequent channel switching in practical MDI networks will certainly increase the consumption of time resources of the whole network, especially in volatile field environments.

To solve this problem, some novel schemes have been proposed to counteract the birefringence of the channel with conventional QKD protocols [5–7] as well as the plug-and-play MDI QKD protocol [27,39], with no additional polarization control applied in the system. However, in the plug-and-play MDI scheme, additional trustworthy assumptions about the single-mode source and the source-monitoring devices should be ensured to avoid source attacks [27,39]. Here, with stable frequency-locked lasers, we present a time-bin phase coding MDI QKD system that would intrinsically dispense with the calibration of both polarization disturbances and the phase reference drifts. The polarization-change-resisting property of the system makes it appropriate for complex channel conditions and multi-user network environments [26]. Additionally, eliminating the aligning of primary reference frames of the MDI QKD system will definitely simplify the realistic setup, reduce the resource consumption of the system, and prevent extra information leakage through these ancillary processes.

2. PROTOCOL AND SYSTEM

Our system is schematically shown in Fig. 1. Based on the reference-frame-independent (RFI) MDI QKD [3,26,29], we actively scramble the polarization of our time-bin phase coding quantum states, to protect against unpredictable channel disturbances. Correspondingly, the BSM on Charlie's side is also structurally improved for polarization stochastically varying photons, where incident pulses with the same polarization component are extracted for the BSM process, with Hong–Ou–Mandel (HOM)-type interference effectively guaranteed.

Specifically, Alice and Bob own a frequency-locked laser whose central wavelength is locked to a molecular absorption line at 1542.38 nm, with a precision of 0.0001 nm, corresponding to an approximately 10 MHz accuracy in the spectrum domain. By comparison, pulses with a 2.5 ns temporal width and 1 MHz repetition rate can be generated through the pulse generation unit, equivalent to a frequency linewidth of approximately 400 MHz. Therefore, the high-precision wavelength locking intrinsically ensures the spectral consistency of two independent sources.

Thereafter, polarization scrambling units are used in each party to produce scrambled polarization states. Here we deploy an effective and low-cost scrambling scheme for uniformly distributed polarization states. First, a polarizing beam splitter (PBS) halves the 45° linearly polarized incident pulses into two orthogonal polarization modes with equal intensities. One arm is delayed, while the other is not, and the delay is precisely controlled so that the delayed pulse from one polarization mode will be combined with the other polarization mode of the next incident pulse. Since the global phase of each pulse has been actively randomized, the relative phase difference between two orthogonal modes is stochastically distributed, leading to randomly varying polarization states within a circle on the Poincaré sphere. Additionally, a fiber-squeezer-based polarization controller is used for the random alteration of the orientation of the circle on the Poincaré sphere. It should be stressed that because the coding message is irrelevant to the polarization states, the polarization scrambling of laser pulses in our scheme will not affect the security of the system.

Faraday–Michelson interferometers (FMIs) are used for the time-bin phase coding quantum state preparation, where the laser pulses are split into two adjacent pulses and the variable optical attenuators (VOAs) and the phase modulators (PMs) dominate the basis choice and the relative phase between two time bins, respectively. Therefore, the Z basis states ($|0\rangle$, $|1\rangle$), the X basis states ($|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$), and the Y basis states ($|+i\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$, $|-i\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$) can be arbitrarily prepared. The utilization of the FMI

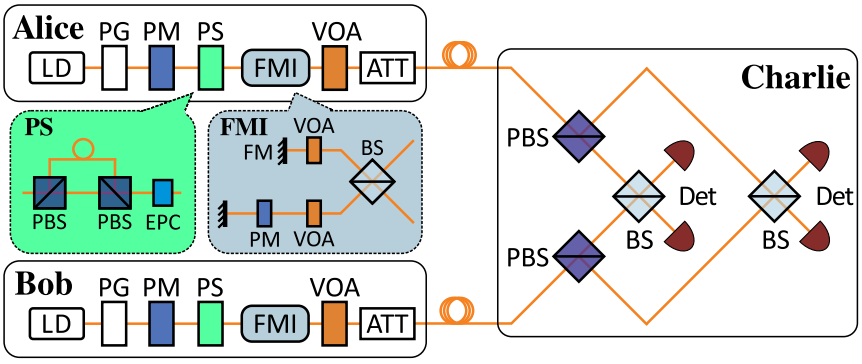

Fig. 1. Schematic diagram of our robust MDI QKD scheme. LD, laser diode; PM, phase modulator; PG, pulse generation unit; PS, polarization scrambling unit; EPC, electronic polarization controller; FMI, Faraday–Michelson interferometer; FM, Faraday mirror; VOA, variable optical attenuator; ATT, attenuator; BS, beam splitter; PBS, polarizing beam splitter; Det, detector.

essentially eliminates the polarization discrepancy between two divergent time bins. In addition, the reciprocating structure of the FMI improves the extinction ratio of VOAs and enhances the robustness performance of PMs against randomly polarized pulses. Afterward, decoy state technology is implemented by VOAs outside the FMI, and attenuators (ATTs) enable single-photon attenuation of the final states.

Then the modulated pulses are sent separately to the not trusted party, Charlie, through optical fibers. On Charlie's side, two PBSs are exploited to differentiate two orthogonal polarization modes. In each mode, photons from Alice and Bob are indistinguishable from each other in every aspect, and therefore the BSM can be effectively conducted regardless of the channel condition, while in original MDI system, the polarization discrepancies between incident pulses will certainly induce considerable system errors, and decrease the final secure key rate dramatically. It is clear that the alteration of the measurement will not diminish the system's security, due to the detector-attack-resistant nature of the MDI QKD protocol [18]. In our experiment, InGaAs/InP single-photon detectors (Qasky WT-SPD300) with a detection efficiency of 25% are used for the efficient BSM process, whose averaged dark count rate is approximately 8.2×10^{-6} per gate.

After the BSM process, Charlie shares the measurement results with Alice and Bob, who will then exchange their basis information and accordingly obtain the sifted keys. Here, data collected from the ZZ basis (Alice and Bob both send Z basis states) are used for key generation, and data collected from the xy basis ($x, y \in \{X, Y\}$, Alice sends x basis states and Bob sends y basis states) are used for the estimation of Eve's information [3,26,29]. Finally, Alice and Bob perform error reconciliation as well as privacy amplification to extract the final secret keys. The final secure key rate can then be given by [40–43]

$$R \geq P_{ZZ} P_{ZZ}^{\mu\mu} \{a_1'^Z b_1'^Z S_{ZZ}^{\mu\mu,11L}[1 - I_E^U] - f S_{ZZ}^{\mu\mu} H(E_{ZZ}^{\mu\mu})\}, \quad (1)$$

where P_{ZZ} is the probability that both Alice and Bob send the Z basis states and $P_{ZZ}^{\mu\mu}$ and $a_1'^Z (b_1'^Z)$ are, respectively, the signal state probability and the single-photon probability of the signal state when both the Z basis states are sent from Alice (Bob). $S_{ZZ}^{\mu\mu}$ ($S_{ZZ}^{\mu\mu,11L}$) and $E_{ZZ}^{\mu\mu}$ represent the yield (the lower bound of the single-photon yield) and error rate when Alice and Bob send signal states in the Z basis. Parameter $f = 1.16$ is the averaged error correction efficiency, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. x^L and x^U represent the estimated lower bound and upper bound of x, respectively.

In our RFI MDI protocol [3,26,29], $I_E = (1 - E_{ZZ}^{11})H[(1+u)/2] + E_{ZZ}^{11} H[(1+v)/2]$ describes eavesdropper Eve's information, where $v = \sqrt{C/2 - (1 - E_{ZZ}^{11})^2 u^2}/E_{ZZ}^{11}$, $u = \min[\sqrt{C/2}/(1 - E_{ZZ}^{11}), 1]$, and

$$C = (1 - 2E_{XX}^{11})^2 + (1 - 2E_{XY}^{11})^2 + (1 - 2E_{YX}^{11})^2 + (1 - 2E_{YY}^{11})^2 \quad (2)$$

remains constant regardless of the exact value of the phase reference drift, and thus we can just ignore the phase compensation of the system.

3. RESULTS AND DISCUSSION

We first verify the system's performance by measuring the visibility of HOM interference on Charlie's side. Unlike the HOM interference with weak coherent states in the equivalent intensity case, the polarization of incident pulses in our scheme changes randomly each time, leading to a fluctuating pulse intensity as well as a different coincidence rate after the PBS. With the polarization scrambling process of our scheme, we can obtain a revised interference visibility of 0.4286 theoretically, which agrees well with our experimental result of 0.425.

To achieve a higher practical security with our robust MDI QKD system, we consider the statistical fluctuations of the finite-size pulses for real-world applications and provide a finite key analysis method for the decoy-state RFI MDI QKD.

Due to the limited number of total pulse pairs sent from Alice and Bob, the unavoidable fluctuations of the experimental observables will certainly influence the estimation of the yield and error rate in single-photon cases, and therefore directly affect the final secure key rate evaluation in Eq. (1). With either linear programming method or analytical equations, the conventional method for fluctuation analysis obtains the worst-case estimation of the single-photon yield as well as the single-photon error rate by simply treating the observables separately. This overly conservative approach exaggerates Eve's information, and calls for a relatively large amount of data to acquire an adequate final secure key rate. Here, by considering observables and statistical fluctuations jointly, we deploy several improved methods for fluctuation analysis in our system. Therefore, we can tightly estimate the single-photon yield as well as the single-photon error rate, and increase the evaluation accuracy of the final secure key rate of our RFI MDI scheme. Furthermore, we develop a universal analysis appropriate for fluctuating systems with an arbitrary number of observables, which may be useful not only in MDI QKD systems but also in other fields with measurement fluctuations. (See Appendices A and B for details).

Here we apply the large deviation theory, specifically, the Chernoff bound [44], for the fluctuation estimation in our experiment, with a fixed failure probability of $\epsilon = 10^{-10}$ and a total number of pulse pairs $N_t = 3.5 \times 10^{11}$. Finally, we obtain the secure key rates for transmission distances of 10 km and 20 km, which are presented in Table 1 and Fig. 2, where all parameters have been fully optimized [45].

In contrast, a performance simulation of our system with conventional fluctuation analysis [46] is also presented in Fig. 2, which treats the experimental observables separately and obtains much lower secure key rates compared to our improved methods.

Furthermore, to demonstrate the property of our polarization scrambling scheme against polarization disturbances, through numerical simulation we compare it with the polarization-controlled scheme from our earlier work with the RFI MDI QKD protocol [26], where the polarization departure of two incident photons will greatly diminish the performance of the HOM-type BSM process, and decrease the final secure key rate. To eliminate all other influences, we utilize single-photon sources, and study the asymptotic secure key rate in our simulation,

Table 1. Experimental Results of Our Robust MDI QKD Scheme[a]

Distance	μ_{ZZ}	$E_{ZZ}^{\mu\mu}$	C Value	I_E	Secure Key Rate
10 km	0.250	1.38%	0.746	0.711	2.229×10^{-7}
20 km	0.215	1.43%	0.646	0.752	6.327×10^{-9}

[a] μ_{ZZ}: Signal state intensity in the ZZ basis states.

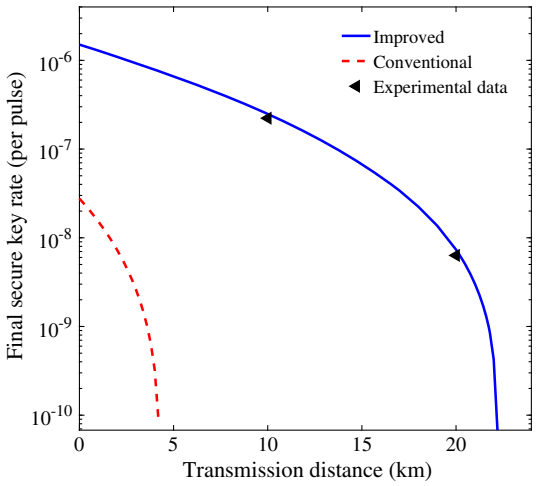

Fig. 2. Lower secure key rate bound of our robust RFI MDI QKD scheme. "Improved" represents the final key rate of the robust MDI QKD scheme with our improved fluctuation analysis, and "Conventional" is the final key rate of the robust MDI QKD scheme with conventional fluctuation analysis. The total number of pulse pairs sent from Alice and Bob is $N_t = 3.5 \times 10^{11}$, the failure probability is $\epsilon = 10^{-10}$, and all parameters have been optimized.

$$R \geq S_{ZZ}^{11}(1 - I_E - fH(E_{ZZ}^{11})), \tag{3}$$

where S_{ZZ}^{11} and E_{ZZ}^{11} represent the yield and error rate, respectively, when Alice and Bob send single photons in the Z basis states.

With polarization intensity deviations of 10%, 20%, and 30%, we obtain the final secure key rates, as shown in Fig. 3, where the RFI MDI QKD system can obtain higher secure key rates with our polarization scrambling scheme than those of the polarization tracking scheme in volatile channel conditions.

4. CONCLUDING REMARKS

In summary, we proposed and realized a robust time-bin phase-coding RFI MDI QKD scheme that is tolerant to complex field environments. The dramatic environmental changes may cause violently varying polarization states of the quantum signal, which can be quite common in real-life scenarios. The intrinsic synchronization elimination of both the polarization and coding phase reference frame of our scheme makes the system inherently capable of extreme channel conditions, and maximally lessens the system's dependency on external auxiliary equipment and processes, further strengthening the overall security of MDI QKD.

Also, we presented a fluctuation analysis method for RFI MDI QKD. With the use of several improved methods and the retightened constraints, we can tightly bound the single-photon yield as well as the single-photon error yield in every basis. The enhanced method for a secure key rate for the system reduces the demands for a large number of sending photon pairs from Alice and Bob, leading to a more practical finite-size key analysis for RFI MDI QKD.

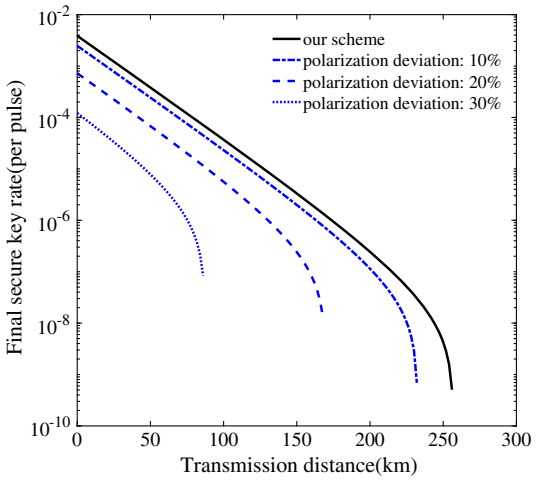

Fig. 3. Simulation comparison of the secure key rates of our polarization scrambling scheme and the polarization tracking scheme with a polarization intensity deviation of 10%, 20%, and 30%.

The positive results of the proof-of-concept experiment demonstrate the feasibility of our scheme, and its performance can be further enhanced with a higher working frequency and detection efficiency of the system. The structural stability against complex channel conditions and the inherent RFI property of our robust MDI QKD reveal its prospective application in real-life quantum communication links.

APPENDIX A: FINITE-KEY ANALYSIS

In our RFI MDI QKD protocol, Alice (Bob) randomly chooses a quantum state preparing base $\omega \in \{Z, X, Y, o\}$ with a probability p_ω, where o represents the vacuum state. Alice (Bob) then prepares her (his) state with an intensity l (r), $l, r \in \{\mu_\omega, \nu_\omega, o\}$ and $\mu_\omega > \nu_\omega > o$, where μ_ω and ν_ω are the signal state and the decoy state, respectively, in X, Y, Z. With a phase-randomized weak coherent source, the state can therefore be described in photon number states:

$$\begin{aligned} \rho_{\mu A}^{\omega} &= \sum_k a_k'^{\omega} |k\rangle\langle k|, \qquad \rho_{\mu B}^{\omega} = \sum_k b_k'^{\omega} |k\rangle\langle k|, \\ \rho_{\nu A}^{\omega} &= \sum_k a_k^{\omega} |k\rangle\langle k|, \qquad \rho_{\nu B}^{\omega} = \sum_k b_k^{\omega} |k\rangle\langle k|, \\ \rho_{oA} &= \rho_{oB} = |0\rangle\langle 0|. \end{aligned} \tag{A1}$$

Due to the symmetry of the X, Y basis in Eq. (2), we treat the parameters of the X, Y basis equivalently for simplicity. Accordingly, $p_X = p_Y$, $\mu_X = \mu_Y$, and $\nu_X = \nu_Y$, and thus $a_k'^X = a_k'^Y$, $b_k^X = b_k^Y$.

The lower bound and upper bound of the single-photon yield and the error yield can be tightly estimated by explicit formulas with a three-intensity decoy-state method [42,43,47,48]:

$$\begin{aligned} m^{11L} &\geq \frac{[a_1' b_2' M^{\nu\nu} + a_1 b_2 a_0' M^{o\mu} + a_1 b_2 a_0' M^{\mu o}] - [a_1 b_2 M^{\mu\mu} + a_1 b_2 a_0' b_0' M^{oo}] - a_1' b_2' [a_0 M^{o\nu} + b_0 M^{\nu o} - a_0 b_0 M^{oo}]}{a_1 a_1' (b_1 b_2' - b_1' b_2)}, \\ m^{11U} &\leq \frac{M^{\nu\nu} - [a_0 M^{o\nu} + b_0 M^{\nu o} - a_0 b_0 M^{oo}]}{a_1 b_1}, \end{aligned} \tag{A2}$$

where M^{lr}, $M \in \{S, T\}$, and $l, r \in \{\mu, \nu, o\}$ represent the gain (S) and the error count gain (T) when Alice and Bob send l, r intensity states, respectively. And $E^{11L(U)} = T^{11L(U)}/S^{11U(L)}$ indicates the lower or upper bound of the single-photon error rate.

However, if we take the finite-key-size effect into account, the gathered information S^{lr} and T^{lr}, as well as the evaluated single-photon yield and error yield, would probably be misjudged due to the statistical fluctuation of the finite number of pulses in a practical situation. By applying the Chernoff bound method [44], we can estimate the fluctuation variation range of the observed total gain S^{lr} (or error gain T^{lr}) with probability $1 - 2\epsilon$:

$$\langle S^{lr}\rangle = S^{lr}(1+\delta^{lr}), \qquad -\frac{\Delta}{\sqrt{N^{lr}S^{lr}}} \le \delta^{lr} \le \frac{\hat{\Delta}}{\sqrt{N^{lr}S^{lr}}}, \tag{A3}$$

where $\Delta = f(\epsilon^{3/2})$, $\hat{\Delta} = f(\epsilon^{4}/16)$, and $f(x) = \sqrt{2\ln(x^{-1})}$. N^{lr} represents the total number of pulses that are sent from Alice and Bob with the sources l and r.

Instead of implementing the worst-case fluctuation analysis in our calculation, we use several tricky methods to improve the overall performance of our system [47,48].

(1) We treat the same observables as an integrated whole in related calculations [48]. For example, the lower bound of the single-photon yield and the upper bound of the single-photon error rate can be obtained by the explicit formulas in Eq. (A2). Considering the error rate must be 50% when either of the two parties send the vacuum state, we denote $[a_0 S^{o\nu} + b_0 S^{\nu o} - a_0 b_0 S^{oo}]$ by $\mathcal{H}$, and find out that this is contained in the estimations of both quantities. Therefore, we do not have to evaluate the bounds of the single-photon yield and single-photon error rate separately and exaggerate the ability of Eve.

(2) Statistical fluctuations of different observables can be treated jointly, because the error analysis also works for several parameters as a whole [47]. For instance, from Eq. (A3), we have the fluctuations δ^{lr} and $\delta^{l'r'}$ that satisfy the relations $|N^{lr}S^{lr}\delta^{lr}| \le \Delta\sqrt{N^{lr}S^{lr}}$ and $|N^{l'r'}S^{l'r'}\delta^{l'r'}| \le \Delta\sqrt{N^{l'r'}S^{l'r'}}$. When we group them together, the larger number of total successful events also follows the fluctuation nature, leading to an additional constraint

$$|N^{lr}S^{lr}\delta^{lr} + N^{l'r'}S^{l'r'}\delta^{l'r'}| \le \Delta\sqrt{N^{lr}S^{lr} + N^{l'r'}S^{l'r'}}. \tag{A4}$$

Similarly, we can obtain all the constraints when all possible observables are taken into consideration,

$$\left|\sum_{lr\in\mathcal{J}} N^{lr}S^{lr}\delta^{lr}\right| \le \Delta\sqrt{\sum_{lr\in\mathcal{J}} N^{lr}S^{lr}}, \tag{A5}$$

and $\mathcal{J} \subseteq \{oo, o\nu, o\mu, \nu o, \nu\nu, \nu\mu, \mu o, \mu\nu, \mu\mu\}$ indicates the arbitrary nonempty subset of all possible observables in any basis. These additional joint constraints obviously tighten the range of the data fluctuation, and further enhance the system's performance.

(3) The single-photon yields in different bases are supposed to share the same value [48]. In our protocol, we use the same estimated values of the lower bound and upper bound of the single-photon yield for the calculation in all bases, to further improve the final secure key rate:

$$\begin{aligned}\langle S^{11}\rangle_L &= \max\{\langle S^{11}_{ZZ}\rangle_L, \langle S^{11}_{XX}\rangle_L, \langle S^{11}_{\mathrm{avg}}\rangle_L\},\\ \langle S^{11}\rangle_U &= \min\{\langle S^{11}_{ZZ}\rangle_U, \langle S^{11}_{XX}\rangle_U, \langle S^{11}_{\mathrm{avg}}\rangle_U\}.\end{aligned} \tag{A6}$$

Then, $\langle S^{11}_{\mathrm{avg}}\rangle$ is the averaged single-photon yield of all the bases:

$$\begin{aligned}\langle S^{11}_{\mathrm{avg}}\rangle = &\frac{1}{p_{\mathrm{tot}}}\sum_{l,r} P_{ZZ}P^{lr}_{ZZ}a_1^{Z_l}b_1^{Z_r}\langle S^{11}_{ZZ}\rangle\\ &+\frac{1}{p_{\mathrm{tot}}}\sum_{l,r} P_{XX}P^{lr}_{XX}a_1^{X_l}b_1^{X_r}\langle S^{11}_{XX}\rangle\\ &+\frac{1}{p_{\mathrm{tot}}}\sum_{l,r} P_{YY}P^{lr}_{YY}a_1^{Y_l}b_1^{Y_r}\langle S^{11}_{YY}\rangle\\ &+\frac{1}{p_{\mathrm{tot}}}\sum_{l,r} P_{XY}P^{lr}_{XY}a_1^{X_l}b_1^{Y_r}\langle S^{11}_{XY}\rangle\\ &+\frac{1}{p_{\mathrm{tot}}}\sum_{l,r} P_{YX}P^{lr}_{YX}a_1^{Y_l}b_1^{X_r}\langle S^{11}_{YX}\rangle, \quad l,r\in\{\mu,\nu\},\end{aligned} \tag{A7}$$

where

$$\begin{aligned}p_{\mathrm{tot}} = &\sum_{l,r} P_{ZZ}P^{lr}_{ZZ}a_1^{Z_l}b_1^{Z_r} + \sum_{l,r} P_{XX}P^{lr}_{XX}a_1^{X_l}b_1^{X_r}\\ &+\sum_{l,r} P_{YY}P^{lr}_{YY}a_1^{Y_l}b_1^{Y_r} + \sum_{l,r} P_{XY}P^{lr}_{XY}a_1^{X_l}b_1^{Y_r}\\ &+\sum_{l,r} P_{YX}P^{lr}_{YX}a_1^{Y_l}b_1^{X_r}\end{aligned} \tag{A8}$$

is the total probability of single-photon states from both Alice and Bob, P_{ij}, $i,j \in \{Z, X, Y\}$ represents the probability that Alice chooses the i basis states and Bob chooses the j basis states simultaneously. P^{lr}_{ij}, $(l, r \in \{\mu, \nu\})$ is the probability that Alice sends l intensity in the i basis states and Bob sends r intensity in the j basis states, and $a_1^{i_l}$ ($b_1^{j_r}$) indicates the single-photon possibility, which can be inferred from Eq. (A1).

With the explicit formulas in Eq. (A2), many more constraints can be additionally implemented to restrict the range of S^{11}_{avg}, and may lead to a tighter bound of the single-photon yield estimation of the system. In [47], Yu *et al.* presented an explicit formula to analytically calculate the statistical fluctuation, which provided us simple and efficient access to the boundary estimation of the observables. However, the previous work has been proved valid only if the number of variables $K \le 4$, which is not applicable in our situation. Here, we prove that the result also works under general conditions (K can be any arbitrary integer), which include multi-parameter conditions such as RFI MDI QKD. Details of the proof can be seen in Appendix B.

From the evaluated value of the single-photon yield in Eq. (A6), we then have the lower bound and the upper bound of the single-photon yield in each basis [49]:

$$\langle S^{11}_{BC}\rangle_L = \langle S^{11}\rangle_L(1-\delta_{BC,L}), \langle S^{11}_{BC}\rangle_U = \langle S^{11}\rangle_U(1+\delta_{BC,U}), \tag{A9}$$

where $BC \in \{ZZ, XX, YY, XY, YX\}$ means the basis choice, $\delta_{BC,L} = \sqrt{-2\ln\epsilon}/\sqrt{N^{11}_{BC}\langle S^{11}\rangle_L}$, and $\delta_{BC,U} = \sqrt{-2\ln\epsilon}/\sqrt{N^{11}_{BC}\langle S^{11}\rangle_U}$.

Also, we can estimate the lower bound as well as the upper bound of the single-photon error yield in each basis $\langle T^{11}_{BC}\rangle$, with fluctuation analysis taken into consideration. The single-photon error rate can therefore be obtained through

$$\langle E^{11}_{BC}\rangle_L = \frac{\langle T^{11}_{BC}\rangle_L}{\langle S^{11}_{BC}\rangle_U}, \langle E^{11}_{BC}\rangle_U = \frac{\langle T^{11}_{BC}\rangle_U}{\langle S^{11}_{BC}\rangle_L}. \tag{A10}$$

Thus we can estimate the upper bound of Eve's information from the C value in Eq. (1), as well as finding the lower bound of the final secure key rate with Eq. (2).

APPENDIX B: PROOF OF THE EXPLICIT FLUCTUATION FORMULA UNDER GENERAL CONDITIONS

Considering a K- variable linear function $f(x_k)=\sum_{k=1}^{K}\alpha_k x_k$ with x_k $(k=1,2,\ldots K)$, our aim is to find the maximum value of $f(x_k)$ with linear constraints

$$\left|\sum_{k\in\mathcal{K}}\beta_k x_k\right|\le n_\epsilon\sqrt{\sum_{k\in\mathcal{K}}\beta_k},\qquad \mathcal{K}\subseteq\{1,2,3,\ldots,K\},\tag{B1}$$

where α_k,β_k are all positive coefficients. It is obvious that the fluctuation analysis with joint treatment of different observables can be written in this form.

Similar to [47], the maximum value of $f(x_k)$ is

$$\begin{aligned}f_{\max}&=f(\tilde{x}_k^*)=\mathcal{F}(K,n_\epsilon,V_\alpha,V_\beta)\\&=n_\epsilon\sum_{n=1}^{K}(\tilde{\gamma}_n-\tilde{\gamma}_{n-1})\sqrt{\sum_{k=n}^{K}\tilde{\beta}_k},\end{aligned}\tag{B2}$$

and the corresponding variables $\tilde{x}_k^*$ are

$$\tilde{x}_k^*=\frac{n_\epsilon}{\tilde{\beta}_k}\left(\sqrt{\sum_{n=k}^{K}\tilde{\beta}_n}-\sqrt{\sum_{n=k+1}^{K}\tilde{\beta}_n}\right),\tag{B3}$$

where $k=1,2,3,\ldots,K$. $V_\alpha=[\alpha_1,\alpha_2,\ldots,\alpha_K]$, $V_\beta=[\beta_1,\beta_2,\ldots,\beta_K]$, $\gamma=\alpha/\beta=[\alpha_1/\beta_1,\alpha_2/\beta_2,\ldots,\alpha_K/\beta_K]$, and $\gamma_0=0$. $\tilde{\gamma}$ represents the sorted form of γ in ascending order, and $\tilde{\alpha}_k$, $\tilde{\beta}_k$, and $\tilde{x}_k$ are accordingly also rearranged to satisfy $\tilde{\gamma}_k=\tilde{\alpha}_k/\tilde{\beta}_k$ $(k=1,2,\ldots,K)$.

Therefore, the minimum value of $f(x_k)$ can be written as

$$f_{\min}=-f_{\max}=-\mathcal{F}(K,n_\epsilon,V_\alpha,V_\beta).\tag{B4}$$

Now the principle problem is proving the maximum value $f_{\max}$ is reachable, that is, the variables in Eq. (B3) meet all the constraint conditions [Eq. (B1)], where the total number of variables K can be any arbitrary integer. For simplicity, we rewrite the problem and the constraints as

$$x_k=\begin{cases}\sqrt{\beta_K} & (k=K),\\ \sqrt{\sum_{n=k}^{K}\beta_k}-\sqrt{\sum_{n=k+1}^{K}\beta_k} & (k<K),\end{cases}\tag{B5}$$

and

$$\sum_{k\in\mathcal{K}}x_k\le\sqrt{\sum_{k\in\mathcal{K}}\beta_k},\tag{B6}$$

for $\forall\ \mathcal{K}\subseteq\{1,2,\ldots,K\}$.

We assume an n-variable arbitrary subset $\mathcal{K}_1=\{u_1,u_2,\ldots,u_n\}$, where $1\le n\le K$ and $u_i\in\{1,2,3,\ldots,K\}$. By complementing the set, we obtain the $(K-n)$-variable subset $\mathcal{K}_2=\{v_1,v_2,\ldots,v_{K-n}\}$ that satisfies

$$\mathcal{K}_2\cup\mathcal{K}_1=\{1,2,\ldots,K\}.\tag{B7}$$

Due to its arbitrariness, we assume subset $\mathcal{K}_2=\{v_k\}$ follows ascending order, that is, $v_1<v_2<\ldots<v_{K-n}$.

From the constraints, we have

$$x_1+x_2+x_3+\ldots+x_{K-1}+x_K=\sqrt{\beta_1+\beta_2+\ldots+\beta_K},\tag{B8}$$

and we need to show that when $\mathcal{K}_2=\{x_{v_1},x_{v_1},\ldots,x_{v_{K-n}}\}$ are all subtracted, the constraints are still valid for $\mathcal{K}_1=\{x_{u_1},x_{u_1},\ldots,x_{u_n}\}$.

(1) When only x_{v_1} is subtracted, we can rewrite Eq. (B8) as

$$\begin{aligned}&x_1+\ldots+x_{v_1-1}+x_{v_1+1}+\ldots+x_K=\sqrt{\beta_1+\beta_2+\ldots+\beta_K}\\&-\left(\sqrt{\beta_{v_1}+\beta_{v_1+1}+\ldots+\beta_K}-\sqrt{\beta_{v_1+1}+\beta_{v_1+2}+\ldots+\beta_K}\right)\\&\le\sqrt{\beta_1+\beta_2+\ldots+\beta_{v_1-1}+\beta_{v_1+1}+\ldots+\beta_K}.\end{aligned}\tag{B9}$$

This can be easily proven after a little transformation as well as taking the squares of the two sides twice.

(2) We assume that the relation is satisfied when $\{x_{v_1},x_{v_2},\ldots,x_{v_i}\}$ are subtracted, that is,

$$\begin{aligned}&x_1+x_2+\ldots+x_{v_1-1}+x_{v_1+1}+\ldots+x_{v_i-1}+x_{v_i+1}+\ldots+x_K\\&\le\sqrt{\beta_1+\beta_2+\ldots+\beta_{v_1-1}+\beta_{v_1+1}+\ldots+\beta_{v_i-1}+\beta_{v_i+1}+\ldots+\beta_K}.\end{aligned}\tag{B10}$$

The key point here is that if we subtract $x_{v_{i+1}}$ on both sides additionally, the relation would still be met.

Let us define the following:

$$\begin{aligned}P_{v_{i+1}}&=\beta_{v_{i+1}+1}+\beta_{v_{i+1}+2}+\ldots+\beta_K,\\P'_{v_{i+1}}&=\beta_1+\beta_2+\ldots+\beta_{v_1-1}+\beta_{v_1+1}+\ldots+\beta_{v_i-1}\\&\quad+\beta_{v_i+1}+\ldots+\beta_{v_{i+1}-1}.\end{aligned}\tag{B11}$$

From *Lemma 1* in [47], we can easily obtain

$$\begin{aligned}&\sqrt{P'_{v_{i+1}}+\beta_{v_{i+1}}+P_{v_{i+1}}}+\sqrt{P_{v_{i+1}}}\\&\le\sqrt{\beta_{v_{i+1}}+P_{v_{i+1}}}+\sqrt{P'_{v_{i+1}}+P_{v_{i+1}}},\end{aligned}\tag{B12}$$

and thus we have

$$\begin{aligned}&\sqrt{P'_{v_{i+1}}+\beta_{v_{i+1}}+P_{v_{i+1}}}-\left(\sqrt{\beta_{v_{i+1}}+P_{v_{i+1}}}-\sqrt{P_{v_{i+1}}}\right)\\&\le\sqrt{P'_{v_{i+1}}+P_{v_{i+1}}}\end{aligned}\tag{B13}$$

and

$$\begin{aligned}&\sqrt{\beta_1+\beta_2+\ldots+\beta_{v_1-1}+\beta_{v_1+1}+\ldots+\beta_{v_i-1}+\beta_{v_i+1}+\ldots+\beta_{v_{i+1}-1}+\beta_{v_{i+1}}+\beta_{v_{i+1}+1}+\ldots+\beta_K}\\&-\left(\sqrt{\beta_{v_{i+1}}+\beta_{v_{i+1}+1}+\ldots+\beta_K}-\sqrt{\beta_{v_{i+1}+1}+\beta_{v_{i+1}+2}+\ldots+\beta_K}\right)\\&\le\sqrt{\beta_1+\ldots+\beta_{v_{i+1}-1}+\beta_{v_{i+1}+1}+\ldots+\beta_K}.\end{aligned}\tag{B14}$$

Hence, the constraints are still satisfied when arbitrary $\{x_{v_1}, x_{v_2}, \ldots, x_{v_i}\}$ are subtracted, which also means the constraints are valid for all $\mathcal{K} \subseteq \{1, 2, \ldots, K\}$ in Eq. (B6). Therefore, all the $\{\tilde{x}_k^*\}$ values as well as the maximum value of $f(x)$ ($f_{\max}$) in Eqs. (B2) and (B3) are reachable within the limiting conditions and can be directly used in the fluctuation analysis with any number of variables.

Funding. National Key R&D Program of China (2016YFA0302600); National Natural Science Foundation of China (NSFC) (61622506, 61475148, 61575183); Strategic Priority Research Program (B) of the Chinese Academy of Sciences (CAS) (XDB01030100).

Acknowledgment. The authors would like to thank Y.-H. Zhou, X.-B. Wang, Y.-C. Wu, N.-H. Wang, and W. Liao for helpful discussions and comments.

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, 1984), pp. 175–179.
2. A. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
3. A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," Phys. Rev. A **82**, 012304 (2010).
4. T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," Nature **509**, 475–478 (2014).
5. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play systems for quantum cryptography," Appl. Phys. Lett. **70**, 793–795 (1997).
6. X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, "Faraday–Michelson system for quantum cryptography," Opt. Lett. **30**, 2632–2634 (2005).
7. Z. F. Han, X. F. Mo, Y. Z. Gui, and G. C. Guo, "Stability of phase-modulated quantum key distribution systems," Appl. Phys. Lett. **86**, 221103 (2005).
8. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
9. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
10. S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, G. C. Guo, and Z. F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. **37**, 1008–1010 (2012).
11. 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, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**, 21739–21756 (2014).
12. 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**, 832–836 (2015).
13. C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," Phys. Rev. A **75**, 032314 (2007).
14. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," Quantum Inf. Comput. **7**, 073–082 (2007).
15. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686–689 (2010).
16. H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, "Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources," Phys. Rev. A **84**, 062308 (2011).
17. J. Z. Huang, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, and Z. F. Han, "Effect of intensity modulator extinction on practical quantum key distribution system," Eur. Phys. J. D **66**, 159 (2012).
18. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
19. S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," Phys. Rev. Lett. **108**, 130502 (2012).
20. 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. **111**, 130501 (2013).
21. T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," Phys. Rev. A **88**, 052303 (2013).
22. Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett. **111**, 130502 (2013).
23. Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," Phys. Rev. Lett. **112**, 190503 (2014).
24. L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nat. Photonics **10**, 312–315 (2016).
25. Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Phys. Rev. X **6**, 011024 (2016).
26. 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).
27. G.-Z. Tang, S.-H. Sun, F. Xu, H. Chen, C.-Y. Li, and L.-M. Liang, "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution," Phys. Rev. A **94**, 032326 (2016).
28. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**, 190501 (2016).
29. Z. Q. Yin, S. Wang, W. Chen, H. W. Li, G. C. Guo, and Z. F. Han, "Reference-free-independent quantum key distribution immune to detector side channel attacks," Quantum Inf. Process. **13**, 1237–1244 (2014).
30. C. Wang, S. Wang, Z.-Q. Yin, W. Chen, H.-W. Li, C.-M. Zhang, Y.-Y. Ding, G.-C. Guo, and Z.-F. Han, "Experimental measurement-device-independent quantum key distribution with uncharacterized encoding," Opt. Lett. **41**, 5596–5599 (2016).
31. A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "High speed prototype quantum key distribution system and long term field trial," Opt. Express **23**, 7583–7592 (2015).
32. C. D. Angelis, A. Galtarossa, G. Gianello, F. Matera, and M. Schiano, "Time evolution of polarization mode dispersion in long terrestrial links," J. Lightwave Technol. **10**, 552–555 (1992).
33. D. S. Waddy, P. Lu, L. Chen, and X. Bao, "Fast state of polarization changes in aerial fiber under different climatic conditions," IEEE Photon. Technol. Lett. **13**, 1035–1037 (2001).
34. Y. Namihira, Y. Horiuchi, S. Ryu, K. Mochizuki, and H. Wakabayashi, "Dynamic polarization fluctuation characteristics of optical fiber submarine cables under various environmental conditions," J. Lightwave Technol. **6**, 728–738 (1988).
35. J. Wuttke, P. M. Krummrich, and J. Rosch, "Polarization oscillations in aerial fiber caused by wind and power-line current," IEEE Photon. Technol. Lett. **15**, 882–884 (2003).
36. K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," Opt. Express **21**, 31395–31401 (2013).

37. J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, "Stable quantum key distribution with active polarization control based on time-division multiplexing," New J. Phys. **11**, 065004 (2009).
38. N. J. Muga, M. F. S. Ferreira, and A. N. Pinto, "QBER estimation in QKD systems with polarization encoding," J. Lightwave Technol. **29**, 355–361 (2011).
39. F. Xu, "Measurement-device-independent quantum communication with an untrusted source," Phys. Rev. A **92**, 012333 (2015).
40. X. Ma, C.-H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," Phys. Rev. A **86**, 052305 (2012).
41. F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Practical aspects of measurement-device-independent quantum key distribution," New J. Phys. **15**, 113007 (2013).
42. X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," Phys. Rev. A **87**, 012320 (2013).
43. Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, "Three-intensity decoy-state method for measurement-device-independent quantum key distribution," Phys. Rev. A **88**, 062339 (2013).
44. 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," Nat. Commun. **5**, 3732 (2014).
45. F. Xu, H. Xu, and H.-K. Lo, "Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution," Phys. Rev. A **89**, 052333 (2014).
46. C.-M. Zhang, J.-R. Zhu, and Q. Wang, "Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution," Phys. Rev. A **95**, 032309 (2017).
47. 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 **91**, 032318 (2015).
48. Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," Phys. Rev. A **93**, 042324 (2016).
49. Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, "Reexamination of decoy-state quantum key distribution with biased bases," Phys. Rev. A **93**, 032307 (2016).