Source monitoring twin-field quantum key distribution assisted with Hong-Ou-Mandel interference

Ming-shuo Sun,* Wen-Lin Wang,* Xing-Yu Zhou, Chun-Hui Zhang, and Qin Wang†

Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; "Broadband Wireless Communication and Sensor Network Technology" Key Lab of Ministry of Education, NUPT, Nanjing 210003, China; and "Telecommunication and Networks" National Engineering Research Center, NUPT, Nanjing 210003, China

(Received 10 August 2023; accepted 20 October 2023; published 27 November 2023)

Twin-field quantum key distribution (TF-QKD) can change the channel-loss dependence of key rates from $O(\eta)$ to $O(\sqrt{\eta})$ and thus significantly increase the secure key rate compared with other existing quantum key distribution protocols. However, it does not take the source security into account in most present TF-QKD protocols. Here, we propose to employ the Hong-Ou-Mandel interference to characterize the source security, i.e., to use the interference visibility to quantify the information leakage from detectable side channels of sources. Furthermore, we establish a corresponding theoretical model and calculate the final key rate, by using the three-intensity decoy-state method and taking finite-data-size effects into account. Consequently, by employing our present scheme, the secure transmission distance can be longer than 100 km under current experimental conditions, significantly surpassing present device-independent QKD systems.

DOI: 10.1103/PhysRevResearch.5.043179

I. INTRODUCTION

Quantum key distribution (QKD) can provide secure and effective communications between two legitimate users, usually called Alice and Bob, since its security is based on the laws of quantum physics. Over the past forty years, significant progress has been made in this field.

For the Bennett-Brassard 1984 (BB84) protocol [1], many assumptions have been made on both sources and detection components in former security proofs. However, these assumptions are too demanding to achieve in practical QKD systems, which can lead to security loopholes. To bridge the gap between theory and practical implementations, numerous advanced methods and novel protocols have been proposed. The decoy-state method was put forward [2,3] to address photon-number-splitting attacks [4]. Furthermore, measurement-device-independent QKD (MDI-QKD) protocols were raised, showing exceptional resistance to side-channel attacks directed on the measurement part [5–7]. However, MDI-QKD is susceptible to finite-size effects [8], and the key rate is restricted by the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [9]. Recently, twin-field QKD (TF-QKD) [10] and related protocols [11–13], such as sending or not sending (SNS) TF-QKD, no phase postselecting TF-QKD, and phase matching TF-QKD, have been introduced. These protocols retain the advantages of MDI-QKD while at the same time being able to break the PLOB boundary without using quantum repeaters.

As an extension of MDI-QKD, TF-QKD has effectively solved the problem of information leakage from the measurement part. However, quantum attacks directed on the source part still pose a threat to practical TF-QKD systems [14–16]. For instance, in a Trojan horse attack (THA) [17], Eve sends a strong light to Alice (or Bob) and retrieves information about the system settings from the reflected light. Other attacks could exploit imperfections in the signal generation stage or high-dimensional parameters from the time or frequency domain [18]. Consequently, these potential information leakages may render the basic assumption of the decoy-state method inapplicable.

To address these threats, numerous approaches have been developed to ensure the security of the source. Nevertheless, these methods tend to concentrate on specific imperfections within the source component. For instance, loss-tolerant methods primarily solve state-preparation errors [14,18,19], while the virtual attenuation model addresses intensity fluctuations [20], and certain security analysis is directed against anti-Trojan-horse attacks [21]. Besides these methods, Hong-Ou-Mandel (HOM) interference is a standard method for characterization of light sources [22]. Its main idea lies in that the two indistinguishable single photons matched on a beam splitter always exit it in a pairwise manner. Recently, researchers proposed bounding passive-light-source side channels via HOM interferences [23,24], which seems as though it would b a very useful tool in analyzing the source security. However, the decoy-state method was not thoroughly discussed, and only the BB84 protocol was considered. Here, we give a practical decoy-state scheme for characterizing source imperfections and further extend it to the TF protocol.

Our work is arranged as follows: First, we briefly review the decoy-state TF-QKD protocol in Sec. II; next, the

*These authors contributed equally to this work.
†qinw@njupt.edu.cn

source monitoring theory is described in detail in Sec. III; subsequently, distinguishable decoy-state analysis is shown in Sec. IV; after that, simulation results are presented in Sec. V; and finally, conclusions are given in Sec. VI.

II. THREE-INTENSITY SNS TF-QKD

Here we use the SNS TF-QKD protocol as an example to illustrate our scheme due to its strong anti-interference ability against misalignment error, and its bit-error rate in the Z basis is not affected by channel phase drifts. However, our method is universal and applicable to other TF-QKD variant protocols as well. In the following, we briefly review the three-intensity decoy-state SNS TF-QKD protocol [11,25,26].

Step 1. Alice and Bob each independently send coherent states to Charlie along with a reference light and encoding phase δ_A (δ_B), all within a specified time window.

Step 2. For each time window, Alice (Bob) randomly chooses whether it is a signal window or a decoy window. If it is a decoy window, she (he) sends a decoy pulse $|\sqrt{x}e^{i\delta_A+i\gamma_A}\rangle$ ($|\sqrt{x}e^{i\delta_B+i\gamma_B}\rangle$) with the probability P_x and the intensity $x \in \{0,v\}$. If it is a signal window, she (he) sends a signal pulse $|\sqrt{\mu}e^{i\delta_A+i\gamma_A}\rangle$ ($|\sqrt{\mu}e^{i\delta_B+i\gamma_B}\rangle$) with the probability ε or not send a signal pulse (i.e., block the signal pulse) with the probability $1-\varepsilon$; μ is the intensity of the signal state. Regardless of which window Alice or Bob chooses, they always announce the global phases θ_A and θ_B after sending out the reference light. However, in reality, the presence of defects in devices or potential eavesdropping attacks may cause the prepared states to leak some encoding information, including high-dimensional side channels. Therefore it is important to optimize the system to minimize such vulnerabilities.

Step 3. Charlie performs phase compensation or estimation to eliminate the impact of the global phase θ_A (θ_B). He then announces the outcome of the measurement after all the pulses have been measured. The effective events are defined as follows: (a) Both Alice and Bob select a signal window, and only one detector clicks; and (b) both Alice and Bob select a decoy window, and only one detector clicks. Meanwhile, they use the same decoy state intensity, and their phases meet the postselection criteria [11].

Step 4. After the measurement and announcement, Alice and Bob carry out postprocessing processes and distill out the secure keys

$$R = (P_\mu P_{z|\mu})^2\{\varepsilon(1-\varepsilon)\mu e^{-\mu}Y_1[1-H(e_1)] - fS_zH(E_z)\}. \tag{1}$$

Here, Y_1 and e_1 refer to the yield and error rate of single-photon pulses, respectively. S_Z and E_Z are the average gain and quantum-bit error rate (QBER) of the Z basis. f is the error correction efficiency factor, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

III. FIDELITY-BASED SOURCE MONITORING

While SNS TF-QKD demonstrates excellent resistance against channel loss and side-channel attacks on the detection side, the security of the source component still cannot be guaranteed. As discussed in Sec. II, the preparation of a perfect state in practical applications is a challenging task.

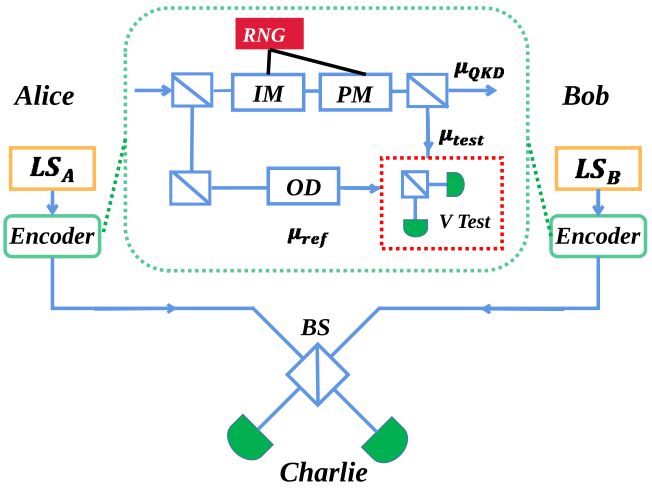

FIG. 1. Overall scheme of our source monitoring TF-QKD. LS, laser source; IM, intensity modulator; PM, phase modulator; RNG, random number generator; OD, optical delay; BS, beam splitter. The light emitted from LS_A (LS_B) will be split into two paths. One path as a reference light $\mu_{\rm ref}$ will not be modulated by any devices. The other light, which is modulated by the IM and PM, will be split into two paths. The pulses marked with $\mu_{\rm QKD}$ including decoy or signal states will be used to send out to Charlie and generate secure keys, and the pulses marked with $\mu_{\rm test}$ will be interfered with the pulses marked with $\mu_{\rm ref}$.

This is because any imperfections ξ, such as variations in wavelength, spectral differences, or electrical fields, must be taken into account, which can alter the density matrix of the source as

$$\rho_x = \sum P_n^x|n\rangle\langle n| \otimes \rho(\xi), \tag{2}$$

where P_n^x is the probability distribution of the n-photon pulse in the weak coherent source (WCS) with intensity x.

We have developed an alternative TF-QKD scheme to address certain issues by introducing an encoder module in the transmitter part, as shown in Fig. 1. The encoder module is enclosed within the dashed box. The scheme involves three participants: Alice, Bob, and Charlie. Alice and Bob each generate a phase-randomized pulse by using a laser source (LS). The pulses are then sent to the encoder module. The light pulse is split into two parts, as shown in the dashed box. One path is encoded by the intensity modulator and phase modulator. However, active modulation may introduce some leakage of high-dimensional information, which needs to be characterized. Due to the limitation of detectors, our method primarily focuses on detectable information. We can use the theory of HOM interference to describe the two light sources. Therefore we set up another path without any modulation as a reference light to create HOM interference with the modulated light in the visibility test (V Test) module. Moreover, an optical delay (OD) is inserted in one path to delay the arrival time of optical pulses with an integer number of periods, to guarantee that the pulses interfering at the beam splitter are phase randomized. As shown in Table I, the HOM visibility is typically worse than the ideal value of 0.5 for two identical WCS pulses [27]. Apart from the encoder part, the rest of our scheme is almost the same as the initial TF scheme [10].

TABLE I. Experimental HOM visibility results with phase-randomized WCPs.

	HOM visibility (%)
Woodward *et al.* [29]	47
Comandar *et al.* [30]	48.2
Wei *et al.* [31]	48.4
Comandar *et al.* [32] (with postselection)	49.9

The states prepared in the Z basis are recorded as ρ_{Z_i} $(i = 1, 2)$, corresponding to intensity $\mu, 0$. In the X basis, all the states are recorded as ρ_{X_i} $(i = 1, 2, 3)$ corresponding to intensity $\mu, \nu, 0$. At the visibility test module, all the prepared modes will be interfered with the reference light in Fig. 1, and we get a measured visibility of ρ_{K_i} and ρ_{L_j}, given as $V^M_{\rho_{K_i}\rho_{L_j}}$, where the high-dimensional degrees of freedom are taken into account. Here, K and L denote the basis. As legitimate users, Alice and Bob know the details of sending states. We could calculate a theoretical visibility $V^T_{\rho_{K_i}\rho_{L_j}}$ of the two known quantum states, i.e., without any modulation and high-dimension effects [28]:

$$V^T_{\rho_{K_i}\rho_{L_j}} = \frac{2\mu_{\rho_{K_i}}\mu_{\rho_{L_j}}}{\left(\mu_{\rho_{K_i}} + \mu_{\rho_{L_j}}\right)^2}, \tag{3}$$

where $\mu_{\rho_{K_i}}$ is the intensity of the corresponding state. Next, we define the visibility after numerical normalization as $\widetilde{V}_{\rho_{K_i}\rho_{L_j}}$:

$$\widetilde{V}_{\rho_{K_i}\rho_{L_j}} = \frac{1}{2}\frac{V^T_{\rho_{K_i}\rho_{L_j}} - \left|V^M_{\rho_{K_i}\rho_{L_j}} - V^T_{\rho_{K_i}\rho_{L_j}}\right|}{V^T_{\rho_{K_i}\rho_{L_j}}}. \tag{4}$$

In the following, $\widetilde{V}_{\rho_{K_i}\rho_{L_j}}$ represents the HOM visibility in all calculations.

Imperfect preparation of different states can introduce vulnerabilities that could be exploited by Eve. Typically, the value used to quantify the vulnerability is denoted as the whole basis imbalance [33]:

$$\triangle = \frac{1 - F_{X,Z}}{2}, \tag{5}$$

where $F_{X,Z}$ is the fidelity between the Z and X bases.

In practical scenarios, it may not be possible to determine the basis imbalance instantaneously using Eq. (4). However, we can rely on the Bures angles [34] and the triangle inequality to make the following conclusion:

$$\begin{aligned}\arccos(F_{X,Z}) \leqslant \arccos(\max F_{\rho_{X_i}\rho_{Z_j}}) + \arccos(\max F_{\rho_X\rho_{X_i}}) \\ + \arccos(\max F_{\rho_Z\rho_{Z_j}}).\end{aligned} \tag{6}$$

Next, the definition of its fidelity is consistent with the original one as [24,35]

$$F_{\rho_x\rho_y} = \sum_n \sqrt{P^x_n P^y_n}\gamma^{\frac{n}{2}}. \tag{7}$$

Here, γ indicates the similarity between two states, ρ_x and ρ_y; $\gamma = 2\widetilde{V}_{\rho_x\rho_y}$. For simplicity, we assume that every pair of states has the same and worst visibility $\widetilde{V}' = \min_{i,j}\widetilde{V}_{\rho_{K_i}\rho_{L_j}}$. Substituting V' into Eq. (6), we could get the same and worst fidelity F'. Then, the basis imbalance can be estimated as

$$1 - 2\triangle \geqslant \cos\left(2\arccos\left(\frac{1+F'}{2}\right) + \arccos\left(F'\right)\right). \tag{8}$$

With the above basis imbalance, the phase-error rate of single-photon pulses can be calculated as [36]

$$\begin{aligned}e'_1 = e_1 + 4(1-\triangle')\triangle'(1-2e_1) \\ + 4(1-2\triangle')\sqrt{\triangle'(1-\triangle')e_1(1-e_1)}.\end{aligned} \tag{9}$$

Here, $\triangle' = \frac{\triangle}{Y_1}$.

IV. METHOD WITH DISTINGUISHABLE DECOY STATES

In the traditional decoy-state theory [2,3], it is often assumed that the only difference between decoy states and signal states lies in the pulse intensity, and for any given pulse, Eve is not able to distinguish it coming from decoy states or signal states. That is to say, the yield (or the error rate) of n-photon states is the same for both decoy pulses and signal pulses. However, in practical implementations, it may bring into side channels during intensity or phase modulations. As a result, the yield (or the error rate) of n-photon states may not be the same for decoy pulses and signal pulses, i.e.,

$$Y^\mu_n \neq Y^\nu_n, \quad e^\mu_n \neq e^\nu_n. \tag{10}$$

Therefore we need to do corrections on the decoy-state method by introducing another parameter, i.e., the trace distance, to quantify the difference between decoy states or signal states, where $D_{xy} = \frac{|\mathrm{Tr}(\rho_x - \rho_y)|}{2}$ [17,37]; then we have

$$\begin{aligned}\left|Y^\mu_n - Y^\nu_n\right| \leqslant D_{\mu\nu}, \\ \left|e^\mu_n Y^\mu_n - e^\nu_n Y^\nu_n\right| \leqslant D_{\mu\nu}.\end{aligned} \tag{11}$$

To build up the relationship between the trace distance and the fidelity, i.e., the fidelity is HOM-relevant in Eq. (6), we use the following inequality [38]:

$$1 - F_{\rho_\mu\rho_\nu} \leqslant D_{\mu\nu} \leqslant \sqrt{1 - F^2_{\rho_\mu\rho_\nu}}. \tag{12}$$

We can obtain the relationship between the yield (or the error rate) of n-photon states and fidelity:

$$\begin{aligned}\left|Y^\mu_n - Y^\nu_n\right| \leqslant \sqrt{1 - F^2_{\rho_\mu\rho_\nu}}, \\ \left|e^\mu_n Y^\mu_n - e^\nu_n Y^\nu_n\right| \leqslant \sqrt{1 - F^2_{\rho_\mu\rho_\nu}}.\end{aligned} \tag{13}$$

With the above, we can rederive the lower bound of Y_1 and upper bound of e_1:

$$\begin{aligned}Y^L_1 = \left[P^2_\mu \underline{Q}_\nu - P^2_\nu \overline{Q}_\mu - \overline{Q_{\mathrm{vac}}}\left(P^2_\mu P^0_\nu - P^2_\nu P^0_\mu\right)\right. \\ \left. - \sqrt{1 - F^2_{\rho_\mu\rho_\nu}}\left(P^2_\nu(1 - e^{-\mu}) + P^2_\mu(1 - e^{-\nu})\right)\right] \\ \div \left(P^2_\mu P^1_\nu - P^1_\mu P^2_\nu\right),\end{aligned} \tag{14}$$

TABLE II. List of experimental parameters used in numerical simulations. Here, P_d denotes the dark count rate of detectors, e_0 is the error rate of the vacuum count and is often set as 0.5 [42], e_d is the misalignment-error probability of the optical system, η is the detection efficiency of detectors, f is the error correction inefficiency, ξ is the failure probability of statistical fluctuation analysis, and N is the data size.

e_d	P_d	η	ξ	f	N
0.015	10^{-7}	0.5	10^{-10}	1.16	10^{12}

$$e_1^U = \frac{e^{\nu}\overline{\mathrm{QE}_{\nu}} - e_0\underline{Q_{\mathrm{vac}}} + \nu\sqrt{1 - F^2_{\rho_\mu\rho_\nu}}}{\nu Y_1^L}, \tag{15}$$

where Q_x and QE_x denote the gain and QBER, respectively, of light pulses with intensity x. The overline and the underline represent the upper bound and the lower bound, respectively, of the measurable variables when taking statistical fluctuations into account. Here we apply the Chernoff bound method for calculations. For a variable X, $\underline{X} = X - \sigma_1 \leqslant X \leqslant X + \sigma_2 = \overline{X}$, where $\sigma_1 = \sqrt{2X\ln(16/\xi^4)}$ and $\sigma_2 = \sqrt{2X\ln(\xi^{-\frac{3}{2}})}$. Here, ξ satisfies the following: $\Pr(E[X] - X \geqslant \sigma_1) \leqslant \xi$ and $\Pr(X - E[X] \geqslant \sigma_2) \leqslant \xi$[39].

V. SIMULATION RESULTS

In this section, we will carry out numerical simulations by using practical experimental parameters. In our simulations, for simplicity, we assume that Charlie lies in the middle between Alice and Bob. The parameters we used are listed in Table II. Furthermore, we apply the optimization algorithm (local search algorithm) to optimize all the system parameters [40,41] including μ, ν, ε, P_μ, P_ν, and $P_{z|u}$.

In Fig. 2, the solid curve represents the scenario where HOM visibility is perfect at 0.5. The other curves indicate different degrees of imperfection in $\widetilde{V}$, ranging from 0.05 to 10^{-4}. When comparing the theoretical limit of visibility at 50%, i.e., $\delta = 0$, with the best experimental visibility of 49.9% shown in Table I, i.e., $\delta = 10^{-3}$, it becomes apparent that imperfections in visibility have a significant impact on both the secure key rate and the transmission distance. However, it is reassuring to note that even with visibility as low as 45 or 49.9%, our scheme is still capable of transmitting keys over distances of 100 or 150 km, respectively, even when faced with potential threats from source imperfections. Figure 3 shows the key rate at 50 km for different HOM visibilities, revealing their inner relation. The secure key rate increases rapidly when HOM visibility is larger than 0.495, indicating that a slight increase in HOM visibility results in a significant increase in key rate. Conversely, the increase in key rate becomes comparatively stable for HOM visibility less than 0.48. This demonstrates our high tolerance for the current low HOM visibility, allowing us to achieve a reasonably high key rate.

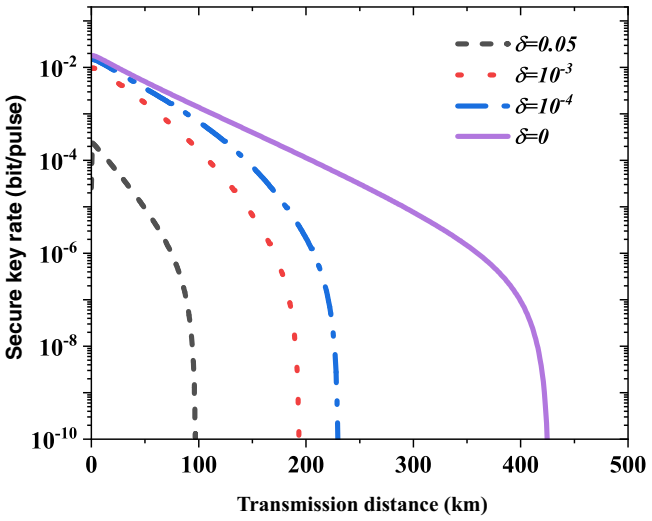

FIG. 2. The optimal key rate vs the transmission distance with different values of the imperfection of visibility. Here, $\delta = |0.5 - \widetilde{V}|$.

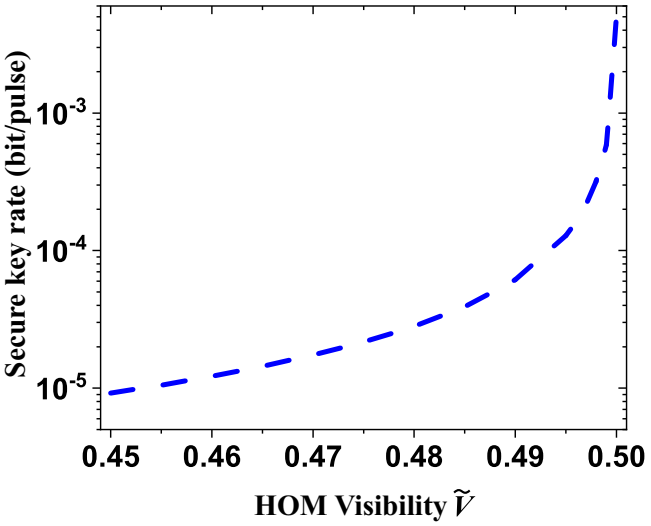

FIG. 3. The optimal key rate vs different visibilities at 50 km.

VI. CONCLUSIONS

In conclusion, we present an alternative approach to detectable side-channel free TF-QKD by examining the relationship between HOM interference and the state fidelity of sources. Compared with prior studies on source security [43,44], here we characterize all the imperfections of light sources only via the HOM visibility. In this way, we can avoid some side channels and unannounced attacks and thus increase the system security. Moreover, we take distinguishable decoy states into account—i.e., the distinguishability is also HOM-relevant—and provide the corresponding security analysis.

Simulation results show that, even under current experimental conditions, our scheme is capable of transmitting secure keys over 100 km, which is a much larger distance than that for current device-independent QKD [45–47] or passive schemes [48,49]. In fact, there is still much room for improvement in our present work. We conclude with two possible directions: One is to depress the influence of the loss-

dependent security mode by implementing some loss-tolerant methods [14,18,19] or reference techniques [21,50,51]; the other direction is to utilize state-of-the-art decoy-state methods for parameter estimations [52,53].

ACKNOWLEDGMENTS

We gratefully acknowledge the National Natural Science Foundation of China (Grants No. 12074194, No. 12104240, and No. 62101285), Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial Key R&D Program (Grant No. BE2022071), Natural Science Foundation of Jiangsu Province (Grants No. BK20192001 and No. BK20210582), Natural Science Foundation of the Jiangsu Higher Education Institutions (Grant No. 21KJB140014), and Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX220954).

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society, Washington, DC, 1984), pp. 175–179.

[2] X. B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[3] H. K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[4] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[5] X. B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors, Phys. Rev. A **87**, 012320 (2013).

[6] H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[7] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[8] 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).

[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[10] 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 (London) **557**, 400 (2018).

[11] 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).

[12] C. Cui, Z. Q. Yin, R. Wang, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Twin-field quantum key distribution without phase post-selection, Phys. Rev. Appl. **11**, 034053 (2019).

[13] X. F. Ma, P. Zeng, and H. Y. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).

[14] K. Tamaki, M. Curty, G. Kato, H. K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[15] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H. K. Lo, Experimental quantum key distribution with source flaws, Phys. Rev. A **92**, 032305 (2015).

[16] X. B. Wang, X. L. Hu, and Z. W. Yu, Practical long-distance side-channel-free quantum key distribution, Phys. Rev. Appl. **12**, 054034 (2019).

[17] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

[18] M. Pereira, M. Curty, and K. Tamaki, Quantum key distribution with flawed and leaky sources, npj Quantum Inf. **5**, 62 (2019).

[19] Y. F. Lu, Y. Wang, M. S. Jiang, X.-X. Zhang, F. Liu, H.-W. Li, C. Zhou, S.-B. Tang, J.-Y. Wang, and W.-S. Bao, Sending or not-sending twin-field quantum key distribution with flawed and leaky sources, Entropy **23**, 1103 (2021).

[20] C. Jiang, Z. W. Yu, X. L. Hu, and X. B. Wang, Robust twin-field quantum key distribution through sending or not sending, Natl. Sci. Rev. **10**, nwac186 (2023).

[21] H. J. Ding, J. Y. Liu, X.-Y. Zhou, C.-H. Zhang, J. Li, and Q. Wang, Improved finite-key security analysis of measurement-device-independent quantum key distribution against a Trojan-horse attack, Phys. Rev. Appl. **19**, 044022 (2023).

[22] C. K. Hong, Z. Y. Ou, and L. Mandel, Measurement of subpicosecond time intervals between two photons by interference, Phys. Rev. Lett. **59**, 2044 (1987).

[23] P. Merodio, A. Kalitsov, M. Chshiev, and J. Velev, Interference of short optical pulses from independent gain-switched laser diodes for quantum secure communications, Phys. Rev. Appl. **5**, 064006 (2016).

[24] A. Duplinskiy and D. Sych, Bounding passive light-source side channels in quantum key distribution via Hong-Ou-Mandel interference, Phys. Rev. A **104**, 012601 (2021).

[25] C. Jiang, Z. W. Yu, X. L. Hu, and X. B. Wang, Unconditional security of sending or not sending twin-field quantum key distribution with finite pulses, Phys. Rev. Appl. **12**, 024061 (2019).

[26] H. Xu, Z. W. Yu, C. Jiang, X. L. Hu and X. B. Wang, Sending-or-not-sending twin-field quantum key distribution: breaking the direct transmission key rate, Phys. Rev. A **101**, 042330 (2020).

[27] J. G. Rarity, P. R. Tapster, and R. Loudon, Non-classical interference between independent sources, J. Opt. B: Quantum Semiclassical Opt. **7**, S171 (2005).

[28] C. Wang, F. X. Wang, H. Chen, S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, G.-C. Guo, and Z.-F. Han, Realistic device imperfections affect the performance of Hong-Ou-Mandel interference with weak coherent states, J. Lightwave Technol. **35**, 4996 (2017).

[29] R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraïso, M. Lucamarini, Z. L. Yuan, and A. J. Shields, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Inf. **7**, 58 (2021).

[30] L. 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 (2016).

[31] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W. J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T. Y. Chen, S. K. Liao, C. Z. Peng, F. Xu, and J. W. Pan, High-speed measurement-device-independent quantum key distribution with integrated silicon photonics, Phys. Rev. X **10**, 031030 (2020).

[32] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, Z. Yuan, and A. Shields, Near perfect mode overlap between independently seeded, gain-switched lasers, Opt. Express **24**, 17849 (2016).

[33] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).

[34] Z. Ma, F. L. Zhang, and J. L. Chen, Fidelity induced distance measures for quantum states, Phys. Lett. A **373**, 3407 (2009).

[35] R. Jozsa, Fidelity for mixed quantum states, J. Mod. Opt. **41**, 2315 (1994).

[36] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Practical security bounds against the Trojan-horse attack in quantum key distribution, Phys. Rev. X **5**, 031030 (2015).

[37] A. Huang, S. H. Sun, Z. Liu, and V. Makarov, Quantum key distribution with distinguishable decoy states, Phys. Rev. A **98**, 012330 (2018).

[38] A. Gilchrist, N. K. Langford and M. A. Nielsen, Distance measures to compare real and ideal quantum processes, Phys. Rev. A **71**, 062310 (2005).

[39] M. Curty, F. H. 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).

[40] 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).

[41] Z. W. Yu, X. L. Hu, C. Jiang, H. Xu, and X. B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, Sci. Rep. **9**, 3080 (2019).

[42] J. C. Chapman, C. C. W. Lim, and P. G. Kwiat, Hyperentangled time-bin and polarization quantum key distribution, Phys. Rev. Appl. **18**, 044027 (2022).

[43] Y. Chen, C. F. Huang, Z. H. Chen, W. He, C. X. Zhang, S. H. Sun, and K. J. Wei, Experimental study of secure quantum key distribution with source and detection imperfections, Phys. Rev. A **106**, 022614 (2022).

[44] S. H. Sun and F. H. Xu, Security of quantum key distribution with source and detection imperfections, New J. Phys. **23**, 023011 (2021).

[45] W. Zhang, T. Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, A device-independent quantum key distribution system for distant users, Nature (London) **607**, 687 (2022).

[46] W. Z. Liu, Y. Z. Zhang, Y. Z. Zhen, M. H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J. W. Pan, Toward a photonic demonstration of device-independent quantum key distribution, Phys. Rev. Lett. **129**, 050502 (2022).

[47] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Experimental quantum key distribution certified by Bell's theorem, Nature (London) **607**, 682 (2022).

[48] F. Y. Lu, Z. H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Experimental demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110802 (2023).

[49] C. Hu, W. Wang, K. S. Chan, Z. Yuan, and H. K. Lo, Proof of principle demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110801 (2023).

[50] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, eaaz4487 (2020).

[51] Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, Practical quantum key distribution that is secure against side channels, Phys. Rev. Appl. **15**, 034072 (2021).

[52] J. Y. Liu, X. Ma, H. J. Ding, C. H. Zhang, X. Y. Zhou, and Q. Wang, Experimental demonstration of five-intensity measurement-device-independent quantum key distribution over 442 km, Phys. Rev. A **108**, 022605 (2023).

[53] C. Jiang, Z. W. Yu, X. L. Hu, and X. B. Wang, Higher key rate of measurement-device-independent quantum key distribution through joint data processing, Phys. Rev. A **103**, 012402 (2021).