Side-Channel Free Measurement-Device-Independent Quantum Key Distribution Based on Source Monitoring

Wen-Lin Wang, Xing-Yu Zhou, Ming-Shuo Sun, Chun-Hui Zhang, and Qin Wang

***Abstract*—Measurement-device-independent quantum key distribution (MDI-QKD) can remove all detector side-channel attacks. However, there are still some assumptions on source preparations in MDI-QKD protocols, which are too strict to achieve in real-life implementations. To remove those assumptions, here we construct a scheme on characterizing the source modulation errors with Hong-Ou-Mandel (HOM) interferences. Furthermore, we combine it with the decoy-state method and present the security analysis. Besides, finite data-size effects are taken into account as well. Simulation results verify the feasibility and practicability of this scheme. It thus seems a very promising candidate for constructing high-security network in the near future.**

***Index Terms*—Quantum key distribution, MDI-QKD, HOM interference.**

I. Introduction

TO ACHIEVE information-theoretic security is extremely difficult for classical cryptography, since its security relies on mathematical complexity and is threatened by advancement of computational power. In contrast, quantum key distribution (QKD) provides a way for two legitimate users, Alice and Bob, to share secret keys with unconditionally security, thanks to the laws of quantum physics. That is to say, the security of QKD does not rely on the computational power of an eavesdropper, Eve. Since the first BB84 QKD protocol was proposed by Bennett and Brassard [1] in 1884, significant theoretical and experimental progresses have been made in this field.

However, there still exist gaps, or so-called security loopholes, between the security proofs of QKD and its practical implementations. Device-independent quantum key distribution (DI-QKD) [2], [3] is inherently immune to all side-channel attacks, but its practicality is limited due to its high demand for detection efficiency and channel loss. As an alternative, MDI-QKD [4] eliminates all side-channels on the vulnerable detection side. However, the source side remains susceptible to modulation deviations and attacks. Side-channel attacks on the source system can be classified into two major types: active and passive. In an active attack, such as a Trojan horse attack, the eavesdropper sends a strong light source to the preparation side and attempts to obtain information about the settings from the reflected light. In passive attacks, the idea is to exploit imperfections within the signal generation stage to obtain information about high-dimensional parameters, which may reveal information about the secret keys.

In recent years, several studies have been conducted to improve security with source flaws, such as the loss-tolerant [5], [6], [7] and reference techniques [8], [9], [10]. Among these attempts, the loss-tolerant method only considers the state preparation errors in two-dimensional space. On the other hand, side channels caused by mode dependencies, e.g., classical pulse correlations [11] or distinguishable decoy states [12], need extra parameters to characterize the information leakage and have been solved in theory. However, those parameters are often very difficult to measure in experiments [13], leaving the high dimensional leakage hard to quantify in practice. Luckily, Duplinskiy et al. [14] proposed a new way of characterizing the passive side-channel information leakage by monitoring the HOM interference and implement it in BB84 protocol. Based on the work in [14], here we present a more practical decoy-state MDI-QKD protocol by taking modulation imperfections in decoy states into account, moreover, finite-size effects are also taken into account.

Our passage is arranged as follows: Section II is the introduction of 3-intensity MDI-QKD with source monitoring; Reconsidering of decoy-state method is shown in Section III; Section IV shows our simulation results and analysis. The passage end with conclusion.

II. MDI-QKD Protocol With Source Monitoring

In the following, we first briefly review the steps of the MDI-QKD protocol with 3-intensity decoy state method [15].

Preparation: Alice (Bob) independently sends a phase-randomized coherent state with intensities randomly chosen

Manuscript received 13 July 2023; revised 13 August 2023; accepted 18 August 2023. Date of publication 21 August 2023; date of current version 8 September 2023. This work was supported in part by the National Natural Science Foundation of China under Grants 12074194, 12104240, and 62101285, in part by the Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial key R&D Program under Grant BE2022071, in part by the Natural Science Foundation of Jiangsu Province under Grants BK20192001 and BK20210582, in part by the Natural Science Foundation of the Jiangsu Higher Education Institutions under Grant 21KJB140014, and in part by the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grant KYCX22_0954. *(Wen-Lin Wang, Xing-Yu Zhou, and Ming-Shuo Sun contributed equally to this work.) (Corresponding author: Qin Wang.)*

The authors are with the Institute of Quantum Information and Technology, Broadband Wireless Communication and Sensor Network Technology Key Lab of Ministry of Education, Telecommunication and Networks National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: 1221014028@njupt.edu.cn; xyz@njupt.edu.cn; 464787393@qq.com; chz@njupt.edu.cn; qinw@njupt.edu.cn).

Digital Object Identifier 10.1109/JPHOT.2023.3307169

from a predetermined set with probability P_x (P_y), where $x, y \in \{\mu, \nu, o\}$. The phase-randomized weak coherent source follows the probability distribution of $\rho_x = \sum_{n=0}^{\infty} P_n^x |n\rangle\langle n| = \sum_{n=0}^{\infty} e^{-x} \frac{x^n}{n!} |n\rangle\langle n|$. In the following, Alice and Bob encode the polarization states to be $|H\rangle, |V\rangle, |D\rangle, |A\rangle$, where $|H\rangle$ and $|V\rangle$ are in the Z basis, and $|D\rangle$ and $|A\rangle$ are in the X basis, here $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$.

Measurement: For each time window, the untrusted party Charlie performs a Bell-state measurement on the received pulses from Alice and Bob. The successful outcome will be projected into $|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)$. Later on, Alice and Bob will exchange relevant information including the intensity or basis choices.

Key generation: In this step, Alice and Bob will carry out parameter estimation and calculate the final key rate as:

$$R = (P_{\mu z})^2 \left\{ (P_1^{\mu})^2 Y_{11}^{L,Z} [1 - H(e_{11}^{U,ph})] - f Q_{\mu\mu}^{Z} H(E_{\mu\mu}^{Z}) \right\}. \tag{1}$$

Here, $P_{\mu z}$ represents the probability of pulses prepared in the Z-basis with intensity μ for Alice or Bob, while P_1^{μ} indicates the probability of the WCS emitting a single-photon pulse with intensity μ. $Y_{11}^{L,Z}$ and $e_{11}^{U,ph}$ denote the lower bound of the single-photon yield and the upper bound of the single-photon error rate, respectively, and $Q_{\mu\mu}^{Z}$ and $E_{\mu\mu}^{Z}$ represent the average gain and the quantum bit error rate of the Z-basis. Additionally, f is the error correction efficiency factor, and $H(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ represents the binary entropy function.

It is well known that MDI-QKD can remove all side-channel attacks on the detector side. However, there may exist preparation flaws and side-channel leakage during the state encoding process due to device imperfections. In the following, we present an improved MDI-QKD scheme with a visibility testing module.

Fig. 1(a) shows the overall scheme and Fig. 1(b) shows the encoder module. In Fig. 1(a), phase-randomized weak coherent pulses (WCP) are sent into the encoder module and are prepared into different polarization states and intensities in either Alice or Bob's side. In Charlie's side, Bell-state projection measurements are carried out on the received photon-pair pulses from Alice and Bob. In Fig. 1(b), the encoder module mainly consists of one polarization modulator (Pol-M) and one intensity modulator (Decoy-IM). The beam-splitters (BSs) are placed separately before the Pol-M and after the Decoy-IM, each splitting part light and finally interfering at the V-Test module for security monitoring. Here we assume that the polarization state $|H\rangle$ prepared by the laser is a standard reference state, and the intensity of light passing through the down path of the beam splitter and attenuator is μ with the $|H\rangle$ polarization state. The light passing through the upper path will be modulated by a polarization modulator and an intensity modulator to prepare different intensities and encoding states. After that, a portion of it will be reflected on the beam splitter for HOM interference with the reference light. It is worth noting that the optical signal in the lower path is delayed by an integer number of periods using fiber, thereby guaranteeing that the pulses interfering at the beam splitter are phase-randomized, and OD enables convenient

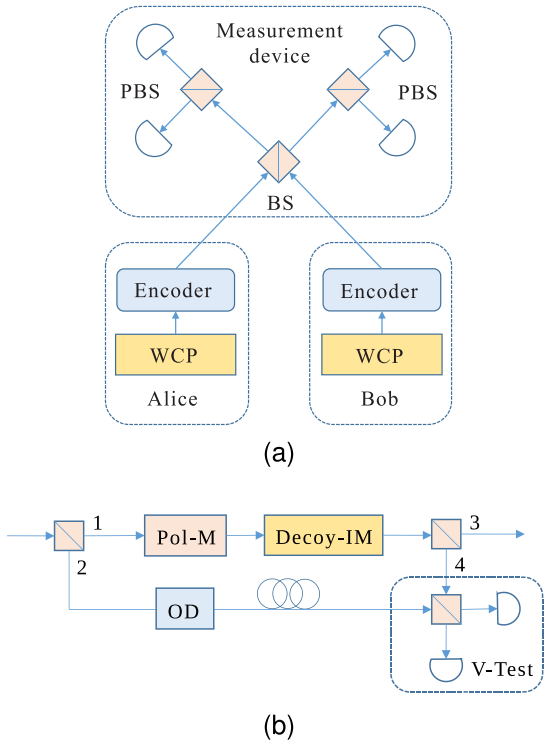

Fig. 1. (a) The schematic of MDI-QKD setup. WCP: weak coherent pulses; BS: beam-splitter; PBS: polarization beam-splitter; (b) The encoder module. Pol-M: polarization modulator; Decoy-IM: intensity modulator; OD: optical delay; V-Test: interference visibility test.

adjustment for achieving synchronized arrival time of two light paths.

We begin by expressing the source density matrices of the X or Z basis as a tensor product of actual density matrices and high-dimension freedom $\rho(\lambda)$, as follows:

$$\rho_x = \sum_{n=0}^{\infty} P_n^x |n\rangle \langle n| \otimes \rho(\lambda), \tag{2}$$

here, the photon number of each pulse follows a Poisson distribution denoted as P_n^x.

According to the definition of fidelity [16], [17], we can obtain that the HOM interference visibility of two states, V_{HOM} which has a relationship with their quantum fidelity as

$$F(\rho_x, \rho_y) = \sum_{n=0}^{\infty} \sqrt{P_n^x P_n^y} \gamma^{\frac{n}{2}}, \tag{3}$$

where $\gamma := \frac{V_{HOM}}{2}$ and γ is used to define the similarity between states ρ_x and ρ_y.

Next, the value called bases imbalance allows to quantify the differences between different density matrices [18], [19]:

$$\triangle = \frac{1 - F(X, Z)}{2}, \tag{4}$$

where $F(X, Z)$ is the fidelity between X basis and Z basis. However, we cannot obtain the value of bases imbalance instantly by (4). Based on Bures angles and triangle inequality [20], we can

conclude that:

$$arccosF(X,Z) \leq arccos \max_{i,j\in\{0,1\}} F(X_i,Z_j) + \sum_{B\in\{X,Z\}} arccos \max_{i\in\{0,1\}} F(B,B_i), \quad (5)$$

where X_i and Z_j $(i,j \in \{0,1\})$ respectively denote the auxiliary matrices [14] for each basis to calculate the fidelity between the bases, and B is used to represent the X basis or Z basis.

In the V-Test module, the state that arrives via the upper path is modulated by both polarization modulator and intensity modulator, with intensity of μ and v respectively, and can be polarized in one of four ways: $|H\rangle, |V\rangle, |D\rangle, |A\rangle$, resulting in a total of eight modulated states: $|H\rangle_\mu, |H\rangle_\nu, |V\rangle_\mu, |V\rangle_\nu, |D\rangle_\mu, |D\rangle_\nu, |A\rangle_\mu, |A\rangle_\nu$. Note that we do not consider the case where the pulse intensity is zero and its encoding. The state that arrives via the lower path has a reference intensity of μ and a polarization mode of $|H\rangle$. Within this module, there are eight possible cases for the HOM interference visibility measurement, denoted as V_M^k, and the corresponding expected values are denoted as V_E^k $(k \in \{1,2,\ldots,8\})$. We use the symbol V^k to represent the deviations between eight sets of measurements and expected HOM visibility. Considering that the maximum value of HOM visibility is 0.5 (i.e., the HOM visibility of two states with intensity μ and polarization $|H\rangle$), we use the following equation to express the deviations, and we denote the minimum value as V',

$$V' = \min_{k\in\{1,2,\ldots,8\}} V^k = \min_{k\in\{1,2,\ldots,8\}} \frac{V_E^k - \left|V_M^k - V_E^k\right|}{2V_E^k}. \quad (6)$$

In the special case when all fidelities equal the same minimum value F'corresponding to the worst visibility V'among all combinations in (3). Equation (5) simplifies to

$$1 - 2\triangle \geq \cos\left[2arccos\left(\frac{1+F'}{2}\right) + arccos\,(F')\right]. \quad (7)$$

To simulate the effect of bases imbalance, we use a method mentioned in [18]. Considering the ability of Eve to use a lossless channel, the calculated bases imbalance is corrected as $\triangle'$.

$$\triangle' = \frac{\triangle}{Y_{11}^L}. \quad (8)$$

The relation between the upper bound of the single-photon error rate e_{11}^U and the phase error rate $e_{11}^{U,ph}$ is obtained as follows:

$$e_{11}^{U,ph} = e_{11}^U + 4(1-\triangle')\,\triangle'\,(1-2e_{11}^U) + 4(1-2\triangle')\sqrt{\triangle'(1-\triangle')e_{11}^U(1-e_{11}^U)}. \quad (9)$$

III. Decoy-State Method With Distinguishable Decoy States

In the classical theory of decoy-state method [21], we usually assume that the yield (or error rate) and the intensity of n-photon pulses are independent, so the yield and error rate of n-photon states at different intensities are always equal.

However, if Eve launches attacks on high-dimension freedom and obtains some prior information about the intensity of Alice's pulses, the assumption may no longer be valid, then we have:

$$Y_{nm}^\mu \neq Y_{nm}^\nu, \quad e_{nm}^\mu \neq e_{nm}^\nu. \quad (10)$$

According to the information obtained from the [22], it can be inferred that $D_{\mu\nu} \leq \sqrt{1-F(\rho_x,\rho_y)^2}$, where $D_{\mu\nu} = \frac{1}{2}Tr|\rho_x - \rho_y|$. The source imperfections can be characterized by the trace distance $D_{\mu\nu}$, which can be bounded by the following equations:

$$|Y_{nm}^\mu - Y_{nm}^\nu| \leq D_{\mu\nu} \leq \sqrt{1-F(\rho_x,\rho_y)^2},$$
$$|e_{nm}^\mu - e_{nm}^\nu| \leq D_{\mu\nu} \leq \sqrt{1-F(\rho_x,\rho_y)^2}. \quad (11)$$

By referring [12], we re-derive the lower bound of the yield and the upper bound of the error rate for single-photon pulses with distinguishable decoy states:

$$Y_{11}^L = \frac{\mu\left[e^{2\nu}\underline{Q}_{\nu\nu} - \frac{\nu^3}{\mu^3}e^{2\mu}\overline{Q}_{\mu\mu} + \frac{\nu^3-\mu^3}{\mu^3}\underline{Q}_{00} - D_{\mu\nu}(e^\nu-1)^2\right]}{\mu\nu^2-\nu^3}, \quad (12)$$

$$e_{11}^U = \frac{e^\nu\overline{E}_{\nu\nu} - e_0\underline{Q}_{00} + \nu D_{\mu\nu}}{\nu Y_{11}^L}, \quad (13)$$

here, we use Q_{xy} and E_{xy} to respectively denote the overall gain and quantum bit error rate. To account for the finite-key effect, we apply the Chernoff bound method as described in [23], and denote the upper and lower bounds of the variables in (12) and (13) with overlines and underlines. Specifically, for a variable X, $\underline{X} = X - \sigma_1 \leq X \leq X + \sigma_2 = \overline{X}$, where $\sigma_1 = \sqrt{2Xln(\frac{16}{\xi^4})}$ and $\sigma_2 = \sqrt{2Xln(\xi^{-\frac{3}{2}})}$. The failure probability of statistical fluctuation analysis ξ satisfies the following inequalities: $Pr(E[X] - X \geq \sigma_1) \leq \xi$ and $Pr(X - E[X] \geq \sigma_2) \leq \xi$.

TABLE I
List of Experimental Parameters Used in Numerical Simulations

P_d	e_0	e_d	η	f	ξ	N
10^{-9}	0.5	0.015	0.85	1.16	10^{-10}	10^{14}

IV. Simulations and Analysis

Based on the formulas presented in the previous section, we present simulation results in Fig. 2. Our simulations consider finite-key analysis and global optimization to obtain better practical performance. The system parameters we used are listed in Table I. Here, P_d denotes the dark count rate of detectors; e_0 is the error rate of the vacuum state; e_d is the misalignment error probability; η is the detection efficiency of detectors; f is the error correction efficiency; in addition, here we assume that the loss coefficient of the transmission fibers is 0.165 dB/km in our simulations. The parameters mentioned above are the primary characteristics of practical QKD systems, while the following parameters related to finite-key effect: ξ is the failure probability

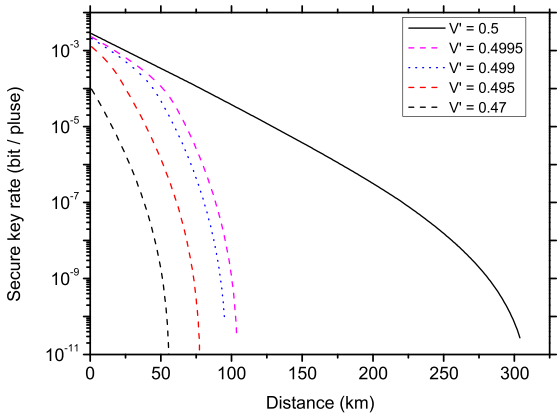

Fig. 2. Optimal secure key rate versus the communication distance in presence of states preparation flaws. Each color in the graph corresponds to a different HOM visibility value. The solid line corresponds to the perfect source scenario, while the dashed lines correspond to scenarios where V' equals 0.47, 0.495 and 0.4995. The dotted line is used to indicate the case where the HOM visibility is 0.499, which is a relatively high level of interference visibility that can be achieved in current experimental articles.

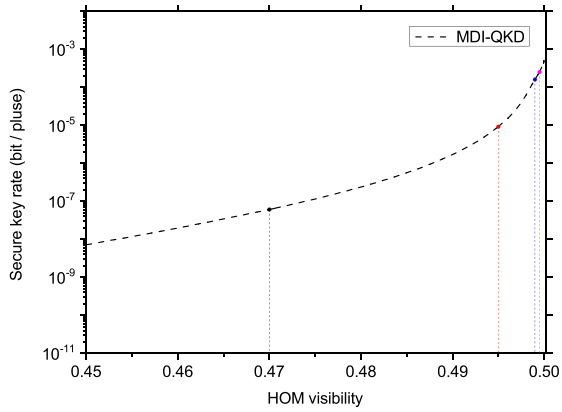

Fig. 3. Relationship between the optimal secure key rate and the HOM visibility at 40 km. Different colored markers on the curve correspond to the V' values used in Fig. 2, from left to right.

of statistical fluctuation analysis; N denotes the total number of signals (weak coherent pulses) sent by Alice and Bob.

As show in Fig. 2, both the key rate and the transmission distance will rapidly decline their values with the decreasing of the HOM visibility, e.g., the transmission distance decreases to a third of the distance when V' changing from 0.5 to 0.4995. For experiments conducted under favorable conditions, e.g., with a HOM visibility of 0.499 [24] (indicated by the dotted line), the simulation results indicate that our approach can still achieve 95 km transmission distance with a high security. Even for experiments conducted under normal experimental conditions [25], [26], [27], [28], e.g., with a HOM visibility of 0.47, our approach can still achieve transmission distances over 50 km. Overall, our present proposed scheme can exhibit superior performance compared with present DI-QKD while maintaining a comparable level of security.

In order to demonstrate the influence of HOM visibility on the secure key rate more clearly, we also calculate the key rate corresponding to different HOM visibilities at 40 km as shown in Fig. 3. It can be observed that the secure key rate rapidly decreases as the interference visibility diminishes, and subsequently exhibits a gradual decline before approaching a plateau. In spite of this, for as low as $V' = 0.45$, the keys are still available. In general, this method has proven effective at achieving secure transmission over long distances and under challenging experimental conditions, demonstrating promising performance and ensuring high security.

V. Conclusion

We have constructed a scheme to improve the security of MDI-QKD systems by monitoring the HOM interference visibility of the source. Moreover, we have established a relationship between the HOM interference visibility and the key rate through formulaic derivations. Besides, to further improve the security, we also reconsidered the distinguishability of the signal and the decoy states and estimate the yield and the error rate of the single-photon pulses. After carrying out full parameter optimization and finite-key analysis, we have demonstrated that, although the secure key rate of the present scheme is quite sensitive to the HOM interference visibility, it can still exhibit secure transmission distances over 50 km with current technology. Most importantly, it can show much better performance compared with present DI-QKD systems [3] while keep similar security. Ref. [13] experimentally characterizes various source flaws through five distinct parameters. In contrast, our approach employs a single parameter to characterize the overall source imperfections, thus avoiding potential undetected side channels and unannounced attacks, resulting in enhanced security. In addition, here we only use the MDI-QKD protocol for illustration, in fact, this method can also be applied to other protocols such as TF-QKD or Mode-Pairing MDI-QKD [29]. Therefore, our present work may provide valuable references for developing high-performance and high security quantum communications in the near future.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, 1984, pp. 175–179.
[2] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phy. Rev. Lett.*, vol. 98, 2007, Art. no. 230501.
[3] U. Vazirani and T. Vidick, "Fully device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 113, 2014, Art. no. 140501.
[4] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, 2012, Art. no. 130503.
[5] K. Tamaki, M. Curty, G. Kat, H.-K. Lo, and K. Azuma, "Loss-tolerant quantum cryptography with imperfect sources," *Phys. Rev. A*, vol. 90, 2014, Art. no. 052314.
[6] F. Xu, S. Sajeed, S. Kaiser, Z. Tang, and H. K. Lo, "Experimental quantum key distribution with source flaws," *Phys. Rev. A*, vol. 92, 2015, Art. no. 032305.
[7] M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," *npj Quantum Inf.*, vol. 5, 2019, Art. no. 62.
[8] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, "Quantum key distribution with correlated sources," *Sci. Adv.*, vol. 6, 2020, Art. no. eaaz4487.
[9] Á. M. Navarrete, M. Pereira, and K. Curty Tamaki, "Practical quantum key distribution that is secure against side channels," *Phys. Rev. Appl.*, vol. 15, 2021, Art. no. 034072.

[10] H. J. Ding, X. Y. Zhou, C. H. Zhang, J. Li, and Q. Wang, "Measurement-device-independent quantum key distribution with insecure sources," *Opt. Lett.*, vol. 47, pp. 665–668, 2022.
[11] V. Zapatero, Á. K. N. Tamaki, and M. Curty, "Security of quantum key distribution with intensity correlations," *Quantum*, vol. 5, 2021, Art. no. 602.
[12] A. Huang, S. H. Sun, Z. Liu, and V. Makarov, "Quantum key distribution with distinguishable decoy states," *Phys. Rev. A*, vol. 98, 2018, Art. no. 012330.
[13] G. Jie et al., "Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources," *Sci. Bull.*, vol. 67, pp. 2167–2175, 2022.
[14] A. Duplinskiy and D. Sych, "Bounding passive light-source side channels in quantum key distribution via Hong-Ou-Mandel interference," *Phys. Rev. A*, vol. 104, 2021, Art. no. 012601.
[15] X. B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," *Phys. Rev. A*, vol. 87, 2013, Art. no. 012320.
[16] A. Uhlmann, "The transition probability in the state space of a*-algebra," *Rep. Math. Phys.*, vol. 9, pp. 273–279, 1976.
[17] R. Jozsa, "Fidelity for mixed quantum states," *J. Mod. Opt.*, vol. 41, pp. 2315–2323, 1994.
[18] 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*, vol. 5, 2015, Art. no. 031030.
[19] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, 2009, Art. no. 045018.
[20] Z. Ma, F. L. Zhang, and J. L. Chen, "Fidelity induced distance measures for quantum states," *Phys. Lett. A*, vol. 373, pp. 3407–3409, 2009.
[21] X. B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phy. Rev. Lett.*, vol. 94, 2005, Art. no. 230503.
[22] A. Gilchrist, N. K. Langford, and M. A. Nielsen, "Distance measures to compare real and ideal quantum processes," *Phys. Rev. A*, vol. 71, 2005, Art. no. 062310.
[23] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and Hoi-Kwong Lo, "Finite-key analysis for measurement-device-independent quantum key distribution," *Nature Commun.*, vol. 5, 2005, Art. no. 062310.
[24] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, Z. Yuan, and A. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," *Opt. Exp.*, vol. 24, pp. 17849–17859, 2016.
[25] 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*, vol. 88, 2013, Art. no. 052303.
[26] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, 2013, Art. no. 130501.
[27] 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.*, vol. 112, 2014, Art. no. 190503.
[28] X. Y. Zhou, H. J. Ding, C. H. Zhang, J. Li, C. M. Zhang, and Q. Wang, " Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources," *Opt. Lett.*, vol. 45, pp. 4176–4179, 2020.
[29] P. Zeng, H. Y. Zhou, W. J. Wu, and X. F. Ma, "Mode-pairing quantum key distribution," *Nature Commun.*, vol. 13, 2022, Art. no. 3903.