One-sided measurement-device-independent quantum key distribution

Wen-Fei Cao, Yi-Zheng Zhen, Yu-Lin Zheng, Li Li,‡ Zeng-Bing Chen,† Nai-Le Liu,§ and Kai Chen¶

Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,
University of Science and Technology of China, Hefei, Anhui 230026, People’s Republic of China
and CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics,
University of Science and Technology of China, Hefei, Anhui 230026, People’s Republic of China

(Dated: Jan 16, 2018)

Measurement-device-independent quantum key distribution (MDI-QKD) protocol was proposed to remove all the detector side channel attacks, while its security relies on the trusted encoding systems. Here we propose a one-sided MDI-QKD (1SMDI-QKD) protocol, which enjoys detection loophole-free advantage, and at the same time weakens the state preparation assumption in MDI-QKD. The 1SMDI-QKD can be regarded as a modified MDI-QKD, in which Bob’s encoding system is trusted, while Alice’s is uncharacterized. For the practical implementation, we also provide a scheme by utilizing coherent light source with an analytical two decoy state estimation method. Simulation with realistic experimental parameters shows that the protocol has a promising performance, and thus can be applied to practical QKD applications.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Mn, 03.65.Ud

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] enables two distant parties to produce random common secret key bits which can be used for secure communication. In theory, the unconditional security of QKD is guaranteed by the laws of quantum mechanics [4–6]. In the usual security proof of QKD, it is assumed that all the devices, both sources and measurement devices, are trusted or well-characterized. In a realistic setup, however, the imperfection of the practical devices leads to various kinds of side-channel attacks, including fake-state attack [7, 8], time-shift attack [9, 10], phase-remapping attack [11, 12], detector-blinding attack [13, 14], dead time attack [15], unambiguous state discrimination attack [16], etc. [17–22].

As a result, on the route of realizing applications of QKD, it is very crucial to bridge the gap between theoretical expectations and realistic setups. To connect theory with practice, several approaches have been proposed. A once-and-for-all solution is device-independent QKD (DI-QKD) [23–27], which allows all the devices (i.e., both sources and measurement devices) being untrusted. Based on the violation of Bell inequality, DI-QKD can defend against any possible eavesdropping. Although recently loophole-free Bell tests have been carried out [28, 29], the DI-QKD is still very difficult to be implemented. At the moment, what obstructs its practical application is not only the requirement of high detection efficiency but also the quite low secure key rate at feasible distances.

To make the realistic QKD applications more applicable, one has to make more assumptions on the characterization of devices. For such a purpose, one-sided device-independent QKD (1SDI-QKD) [30, 31] has been proposed, where the measurement device on one side is assumed to be trusted. The security of 1SDI-QKD is based on demonstration of EPR steering [32–35], in analogy to the demonstration of Bell inequality in DI-QKD. The 1SDI-QKD enjoys the advantage of a lower detection efficiency requirement than that of DI-QKD [30], since it is easier to realize a loophole-free EPR steering experiment [36–38] than a loophole-free Bell test. However, the detection efficiency requirement of 1SDI-QKD is still too high for a realistic QKD application, especially when the desired communication distance is long [30].

Based on the time-reversed entanglement-based QKD [39–41], the measurement-device-independent QKD (MDI-QKD) [42, 43] was proposed to close all kinds of detection side-channel attacks. The MDI-QKD is an attractive scheme for practical implementations because of its high security and long achievable distances. More recently, several MDI-QKD experiments have been successfully carried out [44–50]. A crucial assumption of MDI-QKD is that the state preparation device is nearly perfect, while such requirements might not be strictly satisfied in practice. For example, one’s encoding device may be manufactured by a untrusted third party.

Furthermore, several protocols have been proposed [51–55] to relax the assumptions on the encoding systems. By modifying the original MDI-QKD and assuming qubit sources, Yin et al. [51, 52] have proved that MDI-QKD can still be secure with uncharacterized encoding systems. In [53], MDI-QKD based on the CHSH inequality (CHSH-MDI-QKD) has been investigated, in which the state is prepared in the two-dimensional Hilbert space. In [54], the decoy state method was combined with the CHSH-MDI-QKD protocol to guarantee its security when using a weak coherent state source. In [55], a general technique that applies to any state preparation flaws in phase-randomized sources was proposed, which has been successfully carried out in experiments [56, 57]. With regard to the theoretical analysis of point-to-point quantum communications, the ideal optimal key rates with respect to different scenarios were discussed in Ref. [58], where all possible local operations and classical communications are taken into account.

* eidos@ustc.edu.cn
† zbchen@ustc.edu.cn
‡ nlliu@ustc.edu.cn
§ kaichen@ustc.edu.cn
In this paper, we propose a one-sided MDI-QKD (1SMDI-QKD) protocol, which enjoys the detection loophole-free advantage, and at the same time weakens the state preparation assumption in MDI-QKD. The 1SMDI-QKD can be regarded as a modified MDI-QKD, in which Bob’s encoding system is trusted, while Alice’s encoding system is uncharacterized. In the single-photon case, Alice’s encoding system is assumed to output a quantum state in a two-dimensional Hilbert space basis-independently. This is the assumption we made about Alice’s encoding system besides the common assumptions of the single-photon MDI-QKD case. For the practical implementation, we also propose a scheme by utilizing coherent light source with an analytically two decoy state estimation method. Besides, we provide a concise security analysis for both the single-photon case and the decoy-state case, using a virtual-photon qubit idea. Compared with the existing protocol [51–55], the security proof of our protocol is much more straightforward, and the data post-processing is easier to be applied for experimentists. Simulation with realistic experimental parameters also shows that our protocol has a promising performance, and thus can be applied to practical QKD applications. Without changing the experiment apparatus, one can achieve a higher security level with fewer assumptions about source device for the existing MDI-QKD experiments [44–50].

The paper is organized as follows. In Sec. II, we provide a short review on the 1SDI-QKD and a concrete security analysis. In Sec. III, we present a single-photon version of 1SMDI-QKD, derive the key rate formula with unconditional security, and make a discussion on the assumptions we used. In Sec. IV A, we present a decoy-state 1SMDI-QKD. In Sec. IV B, we derive the secure key rate for decoy-state 1SMDI-QKD. In Sec. IV C, we provide methods for estimating the parameters used in the key rate formula. In Sec. V, we show simulation results for the key rate by comparing between 1SMDI-QKD and MDI-QKD for, both cases of asymptotical and finite decoy states situations. Finally, we give a summary of this paper in Sec. VI.

II. ONE-SIDED DEVICE-INDEPENDENT QKD

A. Protocol description

In this subsection, we introduce the scheme for the non-post-selected version of 1SDI-QKD [30]. Following 1SDI-QKD, the non-post-selected version of the 1SDI-QKD protocol can be described as follows. Alice and Bob receive some quantum systems from an untrusted external source. Alice (Bob) can choose from two binary measurement operators, A1 and A2 (B1 and B2). Alice’s measurement device is untrusted, which is treated as a black box with two possible settings and two possible outputs each time. Bob’s measurement device is trusted, which is assumed to make projective measurements in some qubit subspace. After performing error correction and privacy amplification, they extract a secret common key string finally. The difference between the non-post-selected version of the 1SDI-QKD protocol and original 1SDI-QKD is that all the strings of classical bits Alice gets from measurements A1 are used for the key generation without post-selection.

B. Key rate for 1SDI-QKD

In this subsection we formulate the key rate for non-post-selected 1SDI-QKD. A post-selected version can also be found in Ref. [30]. We denote by A and B, the strings of classical bits Alice and Bob get from measurements Ai and Bi. From the N-bit strings A1 and B1, Alice and Bob can extract a secret key of length [59, 60],

\[ l \approx H_{\text{min}}^e(B_1|E) - H_{\text{max}}^e(A_1|B_1) \]  

where \( H_{\text{min}}^e(B_1|E) \) denotes the smooth entropy of B1 conditioned on Eve’s information E; \( H_{\text{max}}^e(A_1|B_1) \) denotes the smooth max entropy of B1 conditioned on A1. From the generalized uncertainty relation, one has

\[ H_{\text{min}}^e(B_1|E) \geq qN - H_{\text{max}}^e(A_2|B_2) \]

\[ H_{\text{max}}^e(A_1|B_1) \leq Nh(e_1) \]

\[ H_{\text{max}}^e(A_2|B_2) \leq Nh(e_2) \]  

where \( e_i \) is the bit error rate between \( A_i \) and \( B_i \), and \( q \) is a parameter to depict how distinct Bob’s two measurements are. For orthogonal qubit measurements, \( q = 1 \). Finally, one can achieve the key rate \( r = l/N \) for non-post-selected 1SDI-QKD as follows

\[ r \geq 1 - h(e_1) - h(e_2). \]  

III. SINGLE-PHOTON 1SMDI-QKD

In this section, we present a single-photon version of 1SMDI-QKD (see Fig. 1) in which single-photon sources are used by Alice and Bob. We leave a more practical setup using the weak coherent source state for implementation purposes in Sec. IV.

A. Protocol description

The single-photon 1SMDI-QKD protocol runs as follows. Suppose that both Alice and Bob prepare single photons in the four BB84 states \((|0\rangle, |1\rangle, |\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle))\), where \( |0\rangle, |1\rangle \) are the eigenstates of \( \sigma_z \), and \( |\pm\rangle \) are the eigenstates of \( \sigma_x \) [61]. Alice’s encoding system is uncharacterized, i.e., it can be treated as a gray box which receives encoding information and outputs quantum state in two-dimensional Hilbert space (shown in Fig. 1). Alice and Bob send photons to the untrusted relay, Charlie, who performs a Bell state measurement (BSM) and projects the received pulses into one of the Bell states \((|\phi^\pm\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle), |\psi^\pm\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle))\). Then Charlie announces the BSM measurement results among a public classical channel. Afterward, Alice and Bob estimate the quantum phase error and quantum bit error rate (QBER).
They then perform error correction to get a correct key bits string and privacy amplification to remove the information obtained by any possible eavesdropper Eve. Finally, they obtain a correct and secure key bits string that can be used for later secure communication.

FIG. 1. Schematic diagram of 1SMDI-QKD. BSM denotes Bell state measurement; $A_i$ and $B_i$ $(i \in \{1,2\})$ denote the encoding basis of Alice and Bob. Alice and Bob prepare some quantum states and send them to an untrusted relay, Charlie, who is supposed to perform BSM and broadcast the results. Bob’s encoding system is trusted, while Alice’s is uncharacterized and assumed to output the quantum state in two-dimensional Hilbert space. The white box denotes the trusted device, the black box denotes the untrusted device, and the gray box denotes the uncharacterized device.

B. Key rate for single-photon 1SMDI-QKD

Similar to MDI-QKD, here we consider a virtual-photon qubit idea (see Fig. 2). Alice’s encoding system can be treated as a trusted EPR source with an untrusted projective measurement. Bob’s encoding system can be treated as a trusted EPR source with a trusted projective measurement. Using the time-reversed idea, we can perform the projective measurement on Alice’s and Bob’s side after the BSM is performed. Thus, we can treat the two EPR sources and the BSM in the middle as an untrusted EPR source which outputs qubits to Alice and Bob. This is exactly the 1SDI-QKD in which an EPR source outputs qubits to Alice and Bob. Therefore one can get the key rate for our 1SMDI-QKD directly from Eq. (3) for the non-post-selected 1SDI-QKD, which reads

$$r \geq 1 - h(e_1) - h(e_2)$$

(4)

where $e_1$ and $e_2$ is the bit error rate in the $Z$ and $X$ bases, respectively.

C. Discussions on the assumptions

An important assumption in our single-photon 1SMDI-QKD is that the dimension of Alice’s encoding system output is fixed. By taking an example of dimension two (i.e., qubit), we will prove that this assumption is necessary for security purposes. We will demonstrate that when the dimension of Alice’s encoding system output is not fixed, the protocol will be totally insecure. We prove this by constructing a specific attack scheme, in which Charlie can get all the information without introducing any error. Indeed, if the dimension of Alice’s encoding system is not fixed, it can encode the four BB84 states into four orthogonal states in four-dimensional Hilbert space (for instance, four Bell states). So Charlie can simply perform a four-dimensional projective measurement to distinguish the four orthogonal states. Then Charlie can perform a projective measurement on the photon sent by Bob according to the states sent by Alice. To be specific, when Alice sends state $|0\rangle$, Charlie performs the $Z$ basis projective measurement, and the measurement result is denoted by $M_z$. If $M_z = +$, then Charlie reports $|\phi^+\rangle$, $|\phi^-\rangle$ randomly with equal probability; if $M_z = –$, then Charlie reports $|\psi^+\rangle$, $|\psi^-\rangle$ randomly with equal probability. From Table I we can see that Charlie can simulate the same probability tables that can be obtained when genuine BB84 states sent by Alice and actual BSM performed by Charlie. Therefore, Alice and Bob cannot distinguish whether Alice’s encoding system sends genuine BB84 states or four orthogonal four-dimensional states. That is to say, Charlie can get all the information without introducing any error. Thus the security can’t be guaranteed. To remove this kind of attack, one must restrict that the dimen-
sion of Alice’s encoding system output is fixed. The qubit assumption is commonly made in various QKD protocols such as decoy-state BB84 [62–64] and MDI-QKD [42]. In fact an experimental method for verifying the qubit assumption can be easily implemented as proposed in Ref. [56]. To guarantee the qubit assumption, ones needs only to verify that Alice’s encoding system has the same mode except in the encoding degree of freedom. For example, Alice’s phase modulator should have the same timing, spectral, spatial, and polarization mode for different encoding phases in the phase-encoding system.

An uncharacterized encoding system can be treated as a perfect EPR source with an untrusted measurement, which implies that the qubit state from Alice’s encoding system is basis independent. To check the basis-independent assumption in experiment, one needs to test the fidelity between the states sent out by Alice ρA⊗ρB and ρA⊗ρB, where either the X or Z basis is used. If the fidelity is close to unity, one can accept the basis-independent assumption, and vice versa. Considering that most errors come from the inaccuracy or uncharacterized polarization modulator in the realistic experiment, the basis independent is satisfied in most cases.

### IV. DECOY-STATE 1SMDI-QKD

Since the single-photon source is difficult to realize in a real experiment mainly due to high cost, the weak coherent state is widely used in quantum information processing tasks. However, the nonzero probability of multiphoton pulses in the weak coherent pulses may cause the photon-number-splitting (PNS) attack [65, 66]. Hence, the decoy-state method [62–64] is employed to defeat the multiphoton events in the weak coherent states. In the decoy-state 1SMDI-QKD, one naturally assumes that the single-photon portion of the coherent pulses is basis-independent qubit. In this section, we will present the decoy-state 1SMDI-QKD using the coherent light as the source, derive the secure key rate for decoy-state 1SMDI-QKD, and provide practical methods for estimating the parameters.

#### A. Protocol description

The basic setup of the decoy-state 1SMDI-QKD using polarization encoding is illustrated in Fig. 3. The decoy-state 1SMDI-QKD protocol runs as follows. Suppose that both Alice and Bob prepare random BB84 states with phase randomized weak coherent pulses (WCPs), in combination with decoy states. They send the pulses to the untrusted relay, Charlie, who performs the Bell state measurement (BSM) that projects the received states into a Bell state. Then Charlie announces his BSM measurement results among a public classical channel. Afterward, Alice and Bob estimate the gain and QBER of single-photon contributions using the decoy state method [63, 64]. Finally, they generate a correct and secure key bits string after performing error correction and privacy amplification.

![Fig. 3. Basic setup of a decoy-state 1SMDI-QKD protocol. WCP denotes the weak coherent pulse, PM denotes the polarization modulator, IM denotes the intensity modulator, BS denotes beam splitter, PBS denotes polarization beam splitter, and D1, D2, D3, and D4 denote single-photon detectors. Alice and Bob prepare WCPs in a different BB84 polarization state randomly, then send them to Charlie to perform the Bell state measurement. A click in D1 or D4, or in D2 and D3, indicates a projection into the Bell state |ψ−⟩ = (|HV⟩ − |VH⟩)/√2, and a click in D1 and D2, or in D3 and D4 indicates a projection into the Bell state |ψ+⟩ = (|HV⟩ + |VH⟩)/√2. The black, white, and dashed boxes denote the untrusted, trusted, and uncharacterized parts, respectively.]

#### B. Key rate for decoy-state 1SMDI-QKD

In this subsection, we present a concise security analysis and derive the key rate for decoy-state 1SMDI-QKD. Since we have proven the security of single-photon 1SMDI-QKD, here we extend it to the coherent light source situation following the idea of GLLP methods [67].

From the information theory, the key rate is lower bounded by [6]

\[
R = I(A : B) - χ(B : E),
\]

(5)

where I(A : B) denotes the mutual information between Alice and Bob, and χ(B : E) denotes the possible information of Eve. The first term I(A : B) quantifies the amount of classical information between Alice and Bob after error correction. The second term χ(B : E) estimates Eve’s knowledge on the raw key, which will be reduced to an arbitrarily small amount after privacy amplification.

Denote by Ai and Bi the random bits of Alice and Bob post-selected based on a successful Bell measurement along Ai and Bi bases for i = 1, 2. The A1, B1 denotes the Z basis, A2, B2 denotes the X basis, and A3, B3 denotes the H basis.
denotes the $X$ basis when BB84 states are used. Here we assume that the final key is extracted from the data measured in the $Z$ basis. The mutual information between $A_1$ and $B_1$, considering the information leaked in the error-correction process is given by

$$I(A_1 : B_1) = 1 - f \cdot H(E_{\mu\nu}^{ZZ}),$$  

(6)

where $E_{\mu\nu}^{ZZ}$ denotes the QBER with intensities $\mu$ and $\nu$ when Alice and Bob both use the $Z$ basis, $\mu(\nu)$ is the mean photon number of Alice’s (Bob’s) signal state, and $f > 1$ is the error correction inefficiency for the error correction process. Denote by $Q_{\mu\nu}^{ZZ}$ the overall gain with intensities $\mu$ and $\nu$ when Alice and Bob both use the $Z$ basis, then the mutual information between Alice and Bob is given by

$$I(A : B) = Q_{\mu\nu}^{ZZ} \cdot (1 - f \cdot H(E_{\mu\nu}^{ZZ})),$$  

(7)

Following the idea of GLLP methods [67], all the possible information of Eve can be divided into tagged and untagged portions, in which the tagged portion comes from the multi-photon pulses, while the untagged portion comes from the single-photon pulses. So the information of Eve can be written as

$$\chi'(B : E) = \chi'(B : E) + \chi''(B : E),$$

$$\chi'(B : E) = Q_{\mu\nu}^{ZZ} - Q_{11}^{ZZ},$$

$$\chi''(B : E) = Q_{11}^{ZZ} \cdot H(e_{11}^{XX}),$$  

(8)

where the superscripts $t$ and $u$ denote tagged and untagged portions, respectively, $Q_{11}^{ZZ}$ denotes the overall gain in the $Z$ basis, and $e_{11}^{XX}$ denotes the bit error rate of the $X$ basis when Alice and Bob sends a single photon.

Finally, we derive the lower bound of the secure key rate as follows

$$R = Q_{11}^{ZZ} (1 - H(e_{11}^{XX})) - Q_{\mu\nu}^{ZZ} \cdot f \cdot H(E_{\mu\nu}^{ZZ}).$$  

(9)

In a realistic experiment, $Q_{\mu\nu}^{ZZ}$ and $E_{\mu\nu}^{ZZ}$ can be directly obtained from the experimental measurements results, while $Q_{11}^{ZZ}$ and $e_{11}^{XX}$ can be estimated by the decoy method, which will be illustrated in the next subsection.

**C. Parameter estimation**

For simulation purposes, we evaluate the overall gain and QBER when Alice and Bob prepare phase-randomized WCPs. The overall gain and QBER, in the situation without eavesdropping, are the same as MDI-QKD, and can be written as follows [68]:

$$Q_{\mu\nu}^{XX} = 2 \sqrt{2} (1 + 2\sqrt{2} - 4y_{00}(x_0) + y_{01}(2x_1)), $$

$$E_{\mu\nu}^{XX}Q_{\mu\nu}^{XX} = e_0 Q_{\mu\nu} - 2(e_0 - e_d)y^2(1 - 2x_1),$$  

(10)

and

$$Q_{\mu\nu}^{ZZ} = Q_{\mu}^{C} + Q_{\nu}^{E},$$

$$E_{\mu\nu}^{ZZ}Q_{\mu\nu}^{ZZ} = e_d Q_{\mu}^{C} + (1 - e_d)Q_{\nu}^{E},$$  

(11)

where

$$Q_{\mu}^{C} = 2(1 - p_d)e^{\frac{-u}{2}} - x(1 - (1 - p_d)e^{-\frac{u}{2}}),$$

$$Q_{\nu}^{E} = 2p_d (1 - p_d)e^{\frac{-u}{2}} - y(1 - (1 - p_d)e^{-\frac{u}{2}}).$$  

(12)

In the above equations, $Q_{\mu}^{C}$, $Q_{\nu}^{E}$ denote the gains from the correct and false BSM results, respectively. $I_0(\cdot)$ is the first kind modified Bessel function, $e_d$ represents the misalignment error probability, $p_d$ is the background count rate, $e_0 = 1/2$, $\omega = \mu(\nu) + \nu(\mu)$, $x = \frac{(\mu(\nu) - \nu(\mu))}{2\mu\nu}$, $y = (1 - p_d)e^{-\omega/4}$, and $n_1 = n_0 = n_d = 10^{-4} \cdot 20$ is the total efficiency (both channel transmittance efficiency and detection efficiency $n_1$ included) for Alice and Bob, respectively.

Without Eve’s intervention, the yield in $Z$ basis $Y_{11}^{ZZ}$ and bit error rate with single-photon states in $X$ basis $e_{11}^{XX}$ are given as follows:

$$Q_{11}^{ZZ} = \sqrt{\nu(\mu) - \nu(\mu)Y_{11}^{ZZ}}, $$

$$Y_{11}^{ZZ} = Y_{11}^{XY} = (1 - p_d)^2 \left( \frac{\eta_0 \nu_{0\mu}}{2} + (2\eta_{a} + 2\nu_{b} - 3\eta_{a} \eta_{b})p_d + 4(1 - \eta_{a})(1 - \eta_{b})p_d^2 \right),$$

$$e_{11}^{XX} = e_{01}^{YY} - (e_0 - e_d)(1 - p_d)^2 \frac{\eta_0 \nu_{0\mu}}{2}. $$  

(13)

In a practical experiment, the length of the raw key and the number of decoy states are finite. Here, we consider a vacuum + weak-decoy-state method to obtain $Q_{11}^{ZZ}$ and $e_{11}^{XX}$. In general, Alice and Bob can use $\mu_0$, $\nu_0$, $\mu_1$, $\nu_1$ as the decoy state, and $\mu_2$, $\nu_2$ as the signal state, in which $\mu_2 > \mu_1 > \nu_1 > \mu_0 = \nu_0 = 0$. The lower bound of $Y_{11}^{ZZ}$, $Y_{11}^{XX}$ and the upper bound of $e_{11}^{XX}$ are given as follows [69]:

$$Y_{11}^{L} = \frac{1}{\mu \eta_{\mu}^{2} / (\mu_{1} - \mu_{2})_{\mu_{2}}} \left( \frac{\mu_{2}^{2}}{e_{01}^{YY}Q_{\mu_{2}\mu_{2}} + Q_{00} - e_{01}^{YY}Q_{\mu_{2}\mu_{2}} - e_{01}^{YY}Q_{00}}{2} \right),$$

(14)

$$e_{11}^{XX} = \left( \mu_{1} \nu_{1} / (Q_{00}^{XX} + e_{01}^{YY}Q_{\mu_{2}\mu_{2}} + e_{01}^{YY}Q_{00}) \right),$$

(15)

in which Eq. (14) is applicable to the $Z$ and $X$ bases.

We add a trustworthiness parameter $\eta_1$ to depict the trustworthiness of Alice’s source abstractly. This parameter results from the imperfect preparation of states on Alice’s side. The $\eta_1$ denotes the probability of Alice’s encoding system outputting the exact BB84 states. For the case Alice doesn’t send the right state, we assume that 50% error is introduced in terms of the worst case. We note that the assumption of 50% error is equivalent to the assumption of white noise on Alice’s encoding device. Considering the trustworthiness of Alice’s source, the gains and QBERs used for simulation can be written as

$$Q_{\mu\nu}^{ZZ} = Q_{\mu\nu}^{ZZ} \cdot \eta_1, $$

$$Q_{11}^{ZZ} = Q_{11}^{ZZ} \cdot \eta_1, $$

$$e_{11}^{XX} = e_{11}^{XX} \cdot \eta_1, $$

$$e_{11}^{XX} = e_{11}^{XX} \cdot \eta_1. $$  

(16)
V. SIMULATION RESULTS

We consider a setup of our proposal with practical experimental parameters from Ref. [47], which are listed in Table II. We assume that all detectors have the same dark count rates and the same detection efficiencies. For simplicity, we only consider the asymptotic data case. One can extend the analysis to the finite-data case by following the procedures in Refs. [70, 71].

TABLE II. List of experimental parameters used for simulation. $\eta_d$ is the detection efficiency; $\varepsilon_d$ is the misalignment-error probability of the system; $p_d$ is the dark count rate of the detector; $f$ is error correction efficiency; $\alpha$ is the intrinsic loss coefficient of the standard telecom fiber channel.

| $\eta_d$ | $\varepsilon_d$ | $p_d$ | $f$ | $\alpha$ (dB/km) |
|----------|-----------------|------|-----|------------------|
| 40%      | 1.5%            | $3 \times 10^{-6}$ | 1.16 | 0.2               |

FIG. 4. (Color online) Lower bound on the secret key rate $R$ versus communication distance between Alice and Bob. The experimental parameters used are listed in Table II. The solid line denotes the asymptotic case, and the dashed line denotes the two decoy states case. The different color corresponds to different $\eta_d$. In particular, the red line denotes $\eta_d = 1$, i.e., the MDI-QKD protocol. The intensities of the signal state used by Alice and Bob are optimized for the asymptotic case, and are $0.45, 0.3, 0.1, 0.05$, for $\eta_d = 1, 0.95, 0.9, 0.85$, respectively. The intensity of the decoy states are fixed at $0.01$ and $0$.

The secure key rates of the 1SMDI-QKD in the asymptotic case and two decoy states case with different source efficiencies $\eta_d$ are shown in Fig. 4. The simulation results of the MDI-QKD protocol are also illustrated with the red curve in the figure for comparison. We can find that the secure key rate and largest secure communication length of 1SMDI-QKD are slightly lower than that of MDI-QKD, both in the asymptotical case and finite decoy states case. Moreover, the secure key rate and the largest secure communication distance decrease when the source efficiency $\eta_d$ decreases. This makes sense since 1SMDI-QKD requires fewer security assumptions than MDI-QKD. The lower largest secure communication distance is the price to pay in order to make Alice’s device more uncharacterized. The simulation results show that 1SMDI-QKD can tolerate high-loss and low trustworthiness of Alice’s encoding system.

VI. CONCLUSION

In summary, we have provided a 1SMDI protocol, which enjoys the detection loophole-free advantage, and at the same time weakens the state preparation assumption in MDI-QKD. For the practical implementation, we also provide a scheme by utilizing coherent light source with an analytical decoy state method. The simulation results show that our protocol has a promising performance, and thus can be applied to real-life QKD applications. Besides, our proposal can be implemented with standard linear optical elements with low detection efficiency over a high-loss channel. Therefore, it is unnecessary to modify the existing MDI-QKD experiment apparatus, except to guarantee that Alice’s encoding states are in two-dimensional Hilbert space. With the merit of lower requirement, we believe that our proposal is a significant improvement for MDI-QKD under the more realistic situation and paves the way towards the implementations of fully DI-QKD.

ACKNOWLEDGMENTS

We thank Valerio Scarani for valuable discussion, in particular for bringing to our attention and valuable help for the matters of Sec. III C. We also thank Howard M. Wiseman, Feihu Xu, Xiong-Feng Ma, Xiang-Bin Wang, Fei Gao, Tian-Yin Wang, Qiong-Yi He, Jing-Ling Chen, Si-Xia Yu, Zhen-Sheng Yuan, Sheng-Jun Wu, Qiang Zhang, Yu-Ao Chen, Teng-Yun Chen, Jun Zhang and Xiao-Hui Bao for very valuable and enlightening discussions. This work has been supported by the Chinese Academy of Science, the National Fundamental Research Program, and the National Natural Science Foundation of China (Grants No. 11575174, No. 11374287, No. 61125502, and No. 11574297).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
[3] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. 8, 595 (2014).
[4] H.-K. Lo and H. F. Chau, Science 283, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[58] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. 8, 15043 (2017).
[59] M. Tomamichel and R. Renner, Phys. Rev. Lett. 106, 110506 (2011).
[60] J. M. Renes and R. Renner, IEEE Transactions on Information Theory 58, 1985 (2012).
[61] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computer System and Signal Processing (IEEE, New York, 1984) p. 175.
[62] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[63] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
[64] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
[65] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A 51, 1863 (1995).
[66] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).
[67] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).
[68] X. Ma and M. Razavi, Phys. Rev. A 86, 062319 (2012).
[69] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. 15, 113007 (2013).
[70] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. 5, 3732 (2014).
[71] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A 89, 052333 (2014).